D. B. Zagier

Zetafunktionen und quadratische Körper

Eine Einführung in die höhere Zahlentheorie

Mit 8 Abbildungen

Springer-Verlag
Berlin Heidelberg New York 1981

Don Bernard Zagier

Sonderforschungsbereich „Theoretische Mathematik"
Beringstraße 4
5300 Bonn

ISBN 3-540-10603-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-10603-0 Springer-Verlag New York Heidelberg Berlin

CIP-Kurztitelaufnahme der Deutschen Bibliothek

Zagier, Don Bernard:
Zetafunktionen und quadratische Körper: e. Einf. in d. höhere Zahlentheorie /
Don B. Zagier. – Berlin; Heidelberg; New York: Springer, 1981.
(Hochschultext)
ISBN 3-540-10603-0 (Berlin, Heidelberg, New York)
ISBN 0-387-10603-0 (New York, Heidelberg, Berlin)

Printed in Germany

Druck und Bindearbeiten: Beltz Offsetdruck, Hemsbach/Bergstr.
2141/3140-543210

To my father

Vorwort

Das Ziel dieses Buchs ist, die Theorie der binären quadratischen Formen, die im letzten Jahrhundert in ihren algebraischen Aspekten von Gauß und in ihren analytischen Aspekten von Dirichlet entwickelt wurde, darzustellen. Diese Theorie, die früher zur normalen Ausbildung in der Mathematik gehörte, wird heute den Studenten oft nur als Beispiel für die moderne algebraische Zahlentheorie, analytische Zahlentheorie oder Klassenkörpertheorie präsentiert. Da sie aber eine große Schönheit besitzt und außerdem elementar zugänglich ist, halte ich es für zweckmäßiger, sie umgekehrt als Einführung in die genannten Gebiete zu benutzen, die ja historisch aus ihr hervorgegangen sind.

Da das Buch eine Einführung sein soll, sind die Voraussetzngen minimal gehalten, und zwar:

- aus der Algebra die Grundbegriffe über Gruppen und Ringe und der Struktursatz für endlich erzeugte abelsche Gruppen;
- aus der komplexen Funktionentheorie eigentlich nur die Begriffe "holomorphe Funktion", "meromorphe Funktion", "Residuum" und "analytische Fortsetzung" (der Cauchysche Integralsatz wird nie benutzt);
- aus der Zahlentheorie etwa der Inhalt einer elementaren einsemestrigen Vorlesung, insbesondere Kongruenzen, Legendre-Symbol, quadratische Reziprozität.

Das Buch basiert auf Vorlesungen in Bonn (SS 1975) und Harvard (WS 1977) und ist als Vorläufer eines umfassenderen Buches auf Englisch gedacht. Hanspeter Kraft, David Kramer und Winfried Kohnen, die Teile des Manuskripts gelesen und ausführlich kommentiert haben, möchte ich hier herzlich danken; vor allem gilt mein Dank Silke Suter für ihre Unterstützung bei dem ganzen Unternehmen und für ihre Hilfe bei sprachlichen und darstellerischen Schwierigkeiten.

Konventionen und Bezeichnungen: Wir bezeichnen mit $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ die Mengen der ganzen, natürlichen (also strikt positiven ganzen), rationalen, reellen und komplexen Zahlen. Die Kardinalität einer Menge C wird mit $|C|$ oder $\#C$ bezeichnet. Für $x \in \mathbb{R}$ ist $[x]$ die größte ganze Zahl $n \leq x$. Sind f und g Funktionen einer Veränderlichen x,

die nach a strebt (häufig $a = 0$ oder ∞), so bedeuten die Symbole $f = O(g)$, $f = o(g)$ bzw. $f \sim g$, daß für $x \to a$ das Verhältnis $f(x)/g(x)$ beschränkt bleibt, nach 0 strebt bzw. nach 1 strebt. Die n-te Formel von §m wird innerhalb des Paragraphen als (n), in anderen Paragraphen als (m.n) zitiert.

Inhaltsverzeichnis

Teil I. Dirichletsche Reihen

§1 Dirichletsche Reihen: analytische Theorie

Wir wollen in diesem und dem nächsten Paragraphen die elementarsten Eigenschaften von Dirichletschen Reihen angeben, die in der analytischen Zahlentheorie eine so grundlegende Rolle spielen wie die Potenzreihen in der Funktionentheorie.

In der Theorie der Potenzreihen nimmt man die *Potenzfunktionen* $z \mapsto z^n$ $(n \in \mathbb{N})$ als die zugrundeliegenden Funktionen und versucht, beliebige Funktionen als unendliche Linearkombinationen dieser speziellen Funktionen darzustellen. Bei Dirichletschen Reihen nehmen wir statt dessen die *Exponentialfunktionen* $z \to e^{-\lambda z}$ $(\lambda \in \mathbb{R})$ als Bausteine; da aber $\mathbb{R}$ nicht abzählbar ist, müssen wir uns auf eine Folge $\{z \to e^{-\lambda_n z}\}_{n \in \mathbb{N}}$ beschränken, wobei λ_n reelle Zahlen sind, von denen wir annehmen, daß

$$\lambda_1 < \lambda_2 < \dots , \qquad \lambda_n \to \infty . \tag{1}$$

Schließlich bemerken wir, daß es sich in der Theorie der Dirichletschen Reihen eingebürgert hat, die komplexe Veränderliche mit s (statt wie in der Funktionentheorie mit z) und ihren Real- bzw. Imaginärteil mit σ bzw. t (statt mit x bzw. y) zu bezeichnen. Wir haben also die folgende

Definition: Eine *Dirichletsche Reihe* ist eine Reihe

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n s} , \tag{2}$$

wobei die λ_n reelle Zahlen sind, die (1) genügen, die a_n beliebige komplexe Zahlen sind, und $s = \sigma + it$ eine komplexe Zahl ist.

Beispiel 1: $\lambda_n = n$. Das ist sicherlich die naheliegendste Wahl für die Folge (1), führt aber zu keiner neuen Theorie, weil die Substi-

tution $z = e^{-s}$ die Reihe (2) in die Gestalt $\sum a_n z^n$ bringt, so daß die Theorie der Dirichletschen Reihen in diesem Fall identisch ist mit der gewöhnlichen Funktionentheorie.

Beispiel 2: $\lambda_n = \log n$. Mit dieser Wahl der Exponentenmenge läßt sich die Reihe (2) schöner schreiben als

$$(3) \qquad \sum_{n=1}^{\infty} a_n n^{-s} .$$

Dieser Fall ist der für die analytische Zahlentheorie relevante. Eine Reihe der Gestalt (3) heißt *gewöhnliche* Dirichletsche Reihe.

Wann und wo konvergiert eine Dirichletsche Reihe? Für Potenzreihen $\sum a_n z^n$ wissen wir, daß es eine nichtnegative reelle Zahl R gibt (Konvergenzradius), so daß $\sum a_n z^n$ für alle z mit $|z| < R$ und für kein z mit $|z| > R$ konvergiert (wobei man $R = 0$ oder $R = \infty$ setzt für Reihen, die nirgendwo bzw. überall konvergieren). Für den Fall $\lambda_n = n$ des ersten Beispiels läßt sich dieses Ergebnis mit Hilfe der dort angegebenen Transformation $z = e^{-s}$ sofort auf die Veränderliche s übertragen; mit $\sigma_0 = \log(1/R)$ finden wir dann nämlich, daß die Reihe (2) für alle s mit $\sigma > \sigma_0$ und für kein s mit $\sigma < \sigma_0$ konvergiert (während man über das Verhalten auf der Geraden $\sigma = \sigma_0$, die dem Konvergenzkreis $|z| = R$ der Potenzreihe entspricht, allgemein nichts aussagen kann). Wir werden jetzt sehen, daß dieses Beispiel für das Konvergenzverhalten von Dirichletschen Reihen typisch ist.

SATZ 1: *Ist die Reihe (2) für $s = s_0$ konvergent, so konvergiert sie auch für alle s mit $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, und zwar gleichmäßig auf kompakten Mengen. Somit existiert eine reelle Zahl σ_0, so daß die Reihe (2) für alle s mit $\sigma > \sigma_0$ konvergiert und für alle s mit $\sigma < \sigma_0$ divergiert* (falls (2) überall konvergent bzw. divergent ist, setzen wir σ_0 gleich $-\infty$ bzw. ∞). *Die in dem Gebiet $\sigma > \sigma_0$ durch*

$$(4) \qquad f(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

definierte Funktion von s ist dort holomorph; die Ableitungen von $f(s)$ sind gegeben durch

$$(5) \qquad f^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \lambda_n^k a_n e^{-\lambda_n s} ,$$

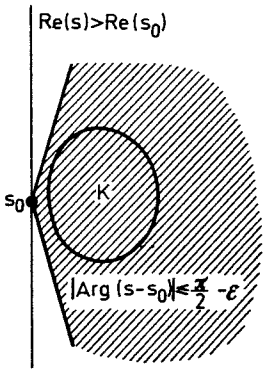
wobei die rechts stehende Dirichletsche Reihe auch für $\sigma > \sigma_0$ konvergiert.

Die Zahl σ_0 heißt *Konvergenzabszisse* der Dirichletschen Reihe (2).

Beweis: Wir brauchen nur die erste Aussage zu beweisen, da die Existenz von einem σ_0 mit den angegebenen Eigenschaften dann klar ist und die Holomorphie von (4) sowie die Zulässigkeit der der Formel (5) zugrundeliegenden gliedweisen Differentiation wegen des bekannten Weierstraßschen Satzes aus der gleichmäßigen Konvergenz folgen. Wir werden sogar mehr beweisen, nämlich, daß die Reihe in jedem Gebiet

$$(6) \qquad |\arg(s - s_0)| \leq \frac{\pi}{2} - \varepsilon < \frac{\pi}{2}$$

gleichmäßig konvergiert; das ist stärker als die Aussage des Satzes, da jede in $\{s \mid \sigma > \sigma_0\}$ enthaltene kompakte Menge K in einem Winkel



der Gestalt (6) liegt (s. Abb.).

Wir führen die Bezeichnungen

$$(7) \qquad A(N) = \sum_{n=1}^{N} a_n , \quad A(M,N) = \sum_{n=M}^{N} a_n , \quad A(M,M-1) = 0$$

ein, die in diesem Paragraphen mehrmals benutzt werden. O.B.d.A. können wir $s_0 = 0$ voraussetzen (indem wir s durch $s + s_0$, a_n durch $a_n e^{-\lambda_n s_0}$ ersetzen); dann ist $\sum a_n$ konvergent und es gibt zu vorgegebenem $\varepsilon > 0$ ein N_0, so daß $|A(M,N)| \leq \varepsilon$ für alle $N > M \geq N_0$. Dann gilt für $N > M \geq N_0$

$$\sum_{M}^{N} a_n e^{-\lambda_n s} = \sum_{M}^{N} [A(M,n) - A(M,n-1)] e^{-\lambda_n s}$$

$$= A(M,M)e^{-\lambda_M s} - A(M,M)e^{-\lambda_{M+1}s} + A(M,M+1)e^{-\lambda_{M+1}s}$$

$$- \dots + A(M,N-1)e^{-\lambda_{N-1}s} - A(M,N-1)e^{-\lambda_N s}$$

$$+ A(M,N)e^{-\lambda_N s}$$

$$= \sum_M^{N-1} A(M,n)\left[e^{-\lambda_n s} - e^{-\lambda_{n+1}s}\right] + A(M,N)e^{-\lambda_N s}$$

(dieser Trick ist das sogenannte Abelsche Summationsverfahren). Es ist

$$\left|e^{-\lambda_n s} - e^{-\lambda_{n+1}s}\right| = \left|s\int_{\lambda_n}^{\lambda_{n+1}} e^{-su}du\right| \le |s|\int_{\lambda_n}^{\lambda_{n+1}} \left|e^{-su}\right|du$$

$$= |s|\int_{\lambda_n}^{\lambda_{n+1}} e^{-\sigma u}\,du = \frac{|s|}{\sigma}\left(e^{-\lambda_n\sigma} - e^{-\lambda_{n+1}\sigma}\right)$$

und die Größe $\frac{|s|}{\sigma}$ ist in dem Bereich (6) (mit $s_0 = 0$) durch eine Konstante C beschränkt; somit ist für $\sigma > 0$

$$\left|\sum_M^N a_n e^{-\lambda_n s}\right| \le \sum_M^{N-1} |A(M,n)|\left|e^{-\lambda_n s} - e^{-\lambda_{n+1}s}\right|$$

$$+ |A(M,N)|\left|e^{-\lambda_N s}\right|$$

$$\le C\varepsilon \sum_M^{N-1}\left(e^{-\lambda_n\sigma} - e^{-\lambda_{n+1}\sigma}\right) + \varepsilon e^{-\lambda_N\sigma}$$

$$\le C\varepsilon e^{-\lambda_M\sigma} + \varepsilon e^{-\lambda_N\sigma} < (C+1)e^{-\lambda_{N_0}\sigma}\varepsilon\,,$$

woraus die gleichmäßige Konvergenz von (2) in diesem Bereich folgt.

Wie kann man die Konvergenzabszisse einer Dirichletschen Reihe bestimmen? Wir wollen eine Formel für σ_0 in Abhängigkeit von den Koeffizienten a_n angeben, analog zur Formel $R = \liminf |a_n|^{-1/n}$ für den Konvergenzradius einer Potenzreihe $\sum a_n z^n$. Diese wird durch den folgenden Satz geliefert.

SATZ 2: *Sei* $\sum a_n e^{-\lambda_n s}$ *eine Dirichletsche Reihe mit* $\sum a_n$ *divergent. Dann ist die Konvergenzabszisse* σ_0 *durch*

$$\sigma_0 = \limsup_{N\to\infty} \frac{\log|A(N)|}{\lambda_N} \tag{8}$$

gegeben, wo $A(N)$ *die in (7) definierte Koeffizientensumme ist.*

(Bemerkung: Falls $\sum a_n$ konvergiert, gilt der Satz noch, wenn wir $A(N)$ durch $\sum_N^\infty a_n$ ersetzen; übrigens kann man durch Verschiebung immer erreichen, daß $\sigma_0 > 0$ und somit $\sum a_n$ divergent ist.)

Beweis: Wir beweisen der Einfachheit halber nur den von uns benötigten Fall von gewöhnlichen Dirichletschen Reihen: $\lambda_N = \log N$; wir müssen also zeigen, daß

$$\sigma_0 = \gamma := \limsup_{N\to\infty} \frac{\log|A(N)|}{\log N} = \inf\{\alpha \mid A(N) = O(N^\alpha)\}\,. \tag{9}$$

(Die Gleichung $A(N) = O(N^\alpha)$ bedeutet: es gibt eine Zahl $B > 0$ mit $|A(N)| \le BN^\alpha$ für alle N.)

Sei $\sigma > \sigma_0$. Dann ist $\sum a_n n^{-\sigma}$ konvergent, also $\left|\sum_1^N a_n n^{-\sigma}\right| < C$ für alle N und geeignetes C. Mit Hilfe der Abelschen partiellen Summation (wie im Beweis von Satz 1) erhalten wir

$$|A(N)| = \left|\sum_{n=1}^N (a_n n^{-\sigma})n^\sigma\right|$$

$$= \left|\sum_{n=1}^{N-1}\left(\sum_{m=1}^n a_m m^{-\sigma}\right)\left(n^\sigma - (n+1)^\sigma\right) + \left(\sum_{n=1}^N a_n n^{-\sigma}\right)N^\sigma\right|$$

$$\le \sum_{n=1}^{N-1}\left|\sum_{m=1}^n a_m m^{-\sigma}\right|\left((n+1)^\sigma - n^\sigma\right) + \left|\sum_{n=1}^N a_n n^{-\sigma}\right|N^\sigma$$

$$< C\sum_{n=1}^{N-1}\left((n+1)^\sigma - n^\sigma\right) + CN^\sigma < 2CN^\sigma\,,$$

also $\gamma \le \sigma$, und da dies für alle σ mit $\sigma > \sigma_0$ gilt, ist $\gamma \le \sigma_0$.

Sei umgekehrt $\sigma > \gamma$. Dann finden wir wieder mit partieller Summation

$$\sum_{n=1}^N a_n n^{-\sigma} = \sum_{n=1}^{N-1} A(n)\left(n^{-\sigma} - (n+1)^{-\sigma}\right) + A(N)N^{-\sigma}\,. \tag{10}$$

Wir wählen α mit $\gamma < \alpha < \sigma$ und ein C mit $|A(N)| \le CN^\alpha$ für alle N. Dann ist

$$|A(n)\left(n^{-\sigma} - (n+1)^{-\sigma}\right)| \le Cn^\alpha\left(n^{-\sigma} - (n+1)^{-\sigma}\right)$$

$$= C\sigma n^\alpha \int_n^{n+1} x^{-\sigma-1}\,dx < C\sigma n^{\alpha-\sigma-1}$$

und $|A(N)N^{-\sigma}| \le CN^{\alpha-\sigma} \to 0$; da $\sum_{n=1}^\infty n^{\alpha-\sigma-1}$ konvergiert, hat die rechte Seite von (10) einen endlichen Limes, wenn N nach ∞ geht, also $\sigma \ge \sigma_0$ und (da dies für jedes $\sigma > \gamma$ gilt) $\gamma \ge \sigma_0$.

Beispiele: a) Sei

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots \tag{11}$$

(das ist die berühmte Riemannsche Zetafunktion, die wir in §4 studieren werden). Hier ist $a_n = 1$, $A(N) = N$, also $\sigma_0 = \gamma = 1$; die Reihe (11) konvergiert für $\sigma > 1$.

b) Sei

$$\psi(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \dots . \tag{12}$$

Hier ist $a_n = (-1)^{n-1}$, $A(N)$ gleich 1 oder 0 je nachdem N ungerade oder gerade ist, also $\sigma_0 = \gamma = 0$; die Reihe (12) konvergiert also für $\sigma > 0$ und definiert in dieser Halbebene eine analytische Funktion. Für $\sigma > 1$ gilt aber offensichtlich

$$\psi(s) = \zeta(s) - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \dots\right) = (1 - 2^{1-s})\,\zeta(s) , \tag{13}$$

so daß wir eine Methode erhalten, $\zeta(s)$ in die Halbebene $\sigma > 0$ meromorph fortzusetzen, mit Polen höchstens in den Punkten $s = 1$, $1 \pm \frac{2\pi i}{\log 2}$, $1 \pm \frac{4\pi i}{\log 2}$ usw., wo der Faktor $(1-2^{1-s})$ verschwindet.

Diese Beispiele zeigen einen großen Unterschied zwischen der Theorie der (gewöhnlichen) Dirichletschen Reihen und der der Potenzreihen. Aus der Formel $R = \liminf |a_n|^{-1/n}$ folgt, daß die Potenzreihen $\sum a_n z^n$ und $\sum |a_n| z^n$ gleichen Konvergenzradius haben; außer auf dem Konvergenzradius $|z| = R$ selbst ist die Reihe also überall, wo sie überhaupt konvergiert, absolut konvergent. Dagegen ist die Dirichletsche Reihe (12) für $\sigma > 0$, die entsprechende Reihe mit Pluszeichen (nämlich (11)) aber erst für $\sigma > 1$ konvergent. Dies ist in einem gewissen Sinne ein extremer Fall, da man aus (9) leicht folgenden Satz erhalten kann:

SATZ 3: *Sei* $\sum a_n n^{-s}$ *eine Dirichletsche Reihe mit Konvergenzabszisse* σ_0 *und sei* σ_1 $(\geq \sigma_0)$ *die Konvergenabszisse von* $\sum |a_n| n^{-s}$. *Dann ist*

$$\sigma_1 \leq \sigma_0 + 1 .$$

Bemerkung: Dieser Satz ist nur für gewöhnliche Dirichletsche Reihen gültig: z.B. ist die Reihe $\sum_{n=2}^{\infty} \frac{(-1)^n}{\sqrt{n}} (\log n)^{-s}$ für alle s konvergent, aber für kein s absolut konvergent.

Es gibt einen noch viel wichtigeren Unterschied zwischen Dirichletschen Reihen und den uns geläufigeren Potenzreihen. Bei Potenzreihen kann man den Konvergenzradius nicht nur in Abhängigkeit von den Koeffizienten, sondern auch durch das Verhalten der durch die Reihe definierten analytischen Funktion bestimmen, nämlich als den Absolutbetrag der kleinsten Singularität: stellt die Reihe $\sum a_n z^n$ eine Funktion dar, die sich in $|z| < r$ holomorph fortsetzen läßt, so ist sie auch in diesem Bereich konvergent. Für Dirichletsche Reihen stimmt das nicht - die Funktion $\psi(s)$, die für $\sigma > 0$ durch (12) gegeben wird, läßt sich auf die ganze komplexe Ebene holomorph fortsetzen (dies folgt aus (13), da wir in §4 die Funktion $\zeta(s)$ auf $\mathbb{C} - \{1\}$ fortsetzen werden), aber die Reihe (12) ist nur für $\sigma > 0$ konvergent. Nur in einem Spezialfall können wir auf die Existenz einer Singularität schließen:

SATZ 4 (Landau): *Sei* $\sum_{n=1}^{\infty} a_n n^{-s}$ *eine gewöhnliche Dirichletsche Reihe mit Konvergenzabszisse* σ_0 *und nichtnegativen reellen Koeffizienten. Dann hat die durch*

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s} \qquad (\sigma > \sigma_0)$$

definierte Funktion an der Stelle $s = \sigma_0$ *eine Singularität.*

Beweis: O.B.d.A. sei $\sigma_0 = 0$. Nehmen wir an, die Funktion $f(s)$ wäre bei $s = 0$ holomorph. Dann würde sie auch in einer Kreisscheibe $|s| < \varepsilon$ holomorph sein und folglich um $s = 1$ eine Taylor-Entwicklung haben mit Konvergenzradius > 1, also wäre für geeignetes $\delta > 0$ die Reihe $\sum_{k=0}^{\infty} \frac{(-1-\delta)^k}{k!} f^{(k)}(1)$ konvergent (und gleich $f(-\delta)$). Aber nach (5) ist

$$\sum_{k=0}^{\infty} \frac{(-1-\delta)^k}{k!} f^{(k)}(1) = \sum_{k=0}^{\infty} \frac{(1+\delta)^k}{k!} \sum_{n=1}^{\infty} \frac{(\log n)^k a_n}{n}$$

$$= \sum_{n=1}^{\infty} \frac{a_n}{n} \sum_{k=0}^{\infty} \frac{(1+\delta)^k (\log n)^k}{k!}$$

(die Vertauschung ist zulässig, da die konvergente Reihe wegen $a_n \geq 0$ auch absolut konvergent ist)

$$= \sum_{n=1}^{\infty} \frac{a_n}{n} e^{(1+\delta)\log n} = \sum_{n=1}^{\infty} a_n n^{\delta}$$

also wäre $\sum a_n n^{\delta}$ im Widerspruch zur Annahme $\sigma_0 = 0$ konvergent.

Wir schließen mit einem einfachen Satz über die Eindeutigkeit der Koeffizienten einer Dirichletschen Reihe.

SATZ 5: *Seien* $\sum a_n e^{-\lambda_n s}$ *und* $\sum b_n e^{-\lambda_n s}$ *zwei Dirichletsche Reihen, die in einem offenen Gebiet in* $\mathbb{C}$ *konvergieren und dort die gleiche Funktion definieren. Dann ist* $a_n = b_n$ *für alle* n.

Beweis: Nehmen wir an, dies sei nicht der Fall, und sei m der kleinste Index mit $a_m \neq b_m$. Dann gilt für σ genügend groß

$$0 = e^{\lambda_m \sigma}\Big(\sum_{n=1}^{\infty} a_n e^{-\lambda_n \sigma} - \sum_{n=1}^{\infty} b_n e^{-\lambda_n \sigma}\Big)$$

$$= a_m - b_m + \sum_{n=m+1}^{\infty} (a_n - b_n)\, e^{-(\lambda_n - \lambda_m)\sigma} .$$

In der Reihe hat jedes Glied für $\sigma \to \infty$ den Limes 0 (da $\lambda_n - \lambda_m > 0$) und die gleichmäßige Konvergenz impliziert, daß dann auch die Summe mit wachsendem σ nach 0 strebt, im Widerspruch zu $a_m \neq b_m$.

Aufgaben:

1. An welcher Stelle wurde im Beweis von Satz 2 die Annahme "$\sum a_n$ divergiert" benutzt?

2. Man zeige ohne Benutzung von (9), daß die Reihe (12) die Konvergenzabszisse $\sigma_0 = 0$ hat, indem man die Konvergenz für s reell, $s > 0$ direkt nachweist und Satz 1 anwendet (daß $\sigma_0 \geq 0$ ist, ist trivial).

3. Man beweise Satz 3.

4. Man zeige (entweder mit Satz 2 oder so wie in Aufgabe 2), daß die Reihe

$$1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \ldots = (1-3^{1-s})\zeta(s)$$

für $\sigma > 0$ konvergiert, und schließe daraus, daß $\zeta(s)$ eine meromorphe Fortsetzung nach $\sigma > 0$ hat mit Polen höchstens bei $s = 1$, $s = 1 \pm \frac{2\pi i}{\log 3}$, $1 \pm \frac{4\pi i}{\log 3}$ usw. Man zeige ferner, daß das Verhältnis von $\log 3$ zu $\log 2$ irrational ist und folgere, daß $\zeta(s)$ höchstens bei $s = 1$ einen Pol hat (und dort nach Satz 4 sicherlich einen).

§2 Dirichletsche Reihen: formale Eigenschaften

Nachdem wir die Konvergenz von Dirichletschen Reihen besprochen haben, wollen wir erläutern, wie man mit solchen Reihen umgeht - die Regeln für die Handhabung Dirichletscher Reihen sind nämlich anders als bei Potenzreihen.

Es ist klar, daß die Summe von zwei Dirichletschen Reihen die Reihe ist, deren allgemeiner Koeffizient die Summe der Koeffizienten der einzelnen Reihen ist. Wie bildet man das Produkt? Seien

$$(1) \qquad f(s) = \sum_{n=1}^{\infty} a_n n^{-s} , \quad g(s) = \sum_{m=1}^{\infty} b_m m^{-s}$$

zwei in einer offenen Menge U durch absolut konvergente Dirichletsche Reihen gegebene Funktionen; dann ist in U

$$f(s)\, g(s) = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} a_n b_m n^{-s} m^{-s}$$

$$(2) \qquad = \sum_{n,m=1}^{\infty} a_n b_m (nm)^{-s}$$

$$= \sum_{k=1}^{\infty} c_k k^{-s} ,$$

wobei

$$(3) \qquad c_k = \sum_{\substack{n,m\geq 1 \\ nm=k}} a_n b_m = \sum_{n|k} a_n b_{k/n}$$

die *Faltung* der Koeffizienten $\{a_n\}$ und $\{b_m\}$ genannt wird. (Das Symbol $\sum_{n|k}$ bezeichnet eine Summe über alle positiven Teiler n von k.) Das heißt, die additive Faltung $c_k = \sum_{n+m=k} a_n b_m$, die die Multiplikation von Potenzreihen beschreibt, wird in der Theorie der Dirichletschen Reihen durch die multiplikative Faltung (3) ersetzt; es ist diese Tatsache, die für die große Bedeutung der Dirichletschen Reihen in der Zahlentheorie verantwortlich ist.

Wir werden nichts weiteres über die Konvergenz von $\sum c_k k^{-s}$ beweisen; man kann z.B. ohne viel Mühe zeigen, daß diese Reihe mindestens dann konvergiert, wenn beide Reihen (1) konvergieren und eine davon absolut konvergent ist.

Beispiele: a) Sei $d(n)$ die Anzahl der positiven Teiler von n. Dann ist für $\sigma > 1$

(4) $$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta(s)^2 ,$$

da $d(n) = \sum_{d|n} 1 \times 1$ ist.

b) Sei $\tau(n)$ die Summe der positiven Teiler von n, oder allgemeiner

(5) $$\sigma_k(n) = \sum_{d|n} d^k$$

die Summe der k-ten Potenzen der positiven Teiler. Dann ist

(6) $$\sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s} = \zeta(s)\ \zeta(s-k) \qquad (\sigma > k+1) .$$

In beiden Beispielen haben die Koeffizienten die spezielle Eigenschaft, multiplikativ zu sein. Eine *multiplikative* Funktion $f: \mathbb{N} \to \mathbb{C}$ ist eine nicht identisch verschwindende Funktion, die

(7) $$f(mn) = f(m)f(n)$$

für alle m,n mit $(m,n) = 1$ erfüllt (eine Funktion, die (7) für alle m,n erfüllt, heißt *streng multiplikativ*). Diese Eigenschaft wirkt sich auf die entsprechenden Dirichletschen Reihen wie folgt aus: ist f multiplikativ, so ist $f(1) = 1$ (da aus (7) $f(1)^2 = f(1)$ folgt, und $f(1) = 0$ das identische Verschwinden von f implizieren würde) und

$$f(n) = f(p_1^{r_1}) \ldots f(p_k^{r_k})$$

für eine Zahl n mit der Primzahlzerlegung $n = p_1^{r_1} \ldots p_k^{r_k}$.

Es ist also in dem Bereich der absoluten Konvergenz von $\sum f(n)n^{-s}$

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \sum_{r_2,r_3,r_5,\ldots} f(2^{r_2}3^{r_3}5^{r_5}\ldots)\ (2^{r_2}3^{r_3}5^{r_5}\ldots)^{-s}$$

(wo die Summe über alle Zuordnungen $p \mapsto r_p$ läuft mit $r_p \geq 0$ und $r_p = 0$ für alle bis auf endlich viele Primzahlen p)

$$= \sum_{r_2,r_3,r_5,\ldots \geq 0} \frac{f(2^{r_2})}{2^{r_2 s}} \frac{f(3^{r_3})}{3^{r_3 s}} \frac{f(5^{r_5})}{5^{r_5 s}} \ldots$$

$$= \prod_p \left[\sum_{r=0}^{\infty} \frac{f(p^r)}{p^{rs}} \right] ,$$

wo das Produkt über alle Primzahlen p läuft. Wir haben also den

<u>SATZ 1</u>: *Sei* $f: \mathbb{N} \to \mathbb{C}$ *eine multiplikative Funktion, und sei die Reihe*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

absolut konvergent. Dann ist $F(s)$ *gleich dem Euler-Produkt*

(8) $$F(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \ldots\right) ,$$

wo das Produkt über alle Primzahlen p *läuft und auch absolut konvergiert.*

<u>Beispiele</u>: c) Für $\zeta(s)$ sind die Koeffizienten alle gleich 1, also

(9) $$\zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \prod_p \frac{1}{1-p^{-s}} \qquad (\sigma > 1) .$$

Diese von Euler entdeckte Produktentwicklung ist der Grund für die große Rolle, die die Zetafunktion in der Primzahltheorie spielt. Außerdem lehrt sie, daß für $\sigma > 1$ die Funktion $\zeta(s)$ nie verschwinden kann (da das Produkt konvergent ist und seine einzelnen Glieder nicht Null sind). Für die in a) und b) angegebenen Reihen erhält man

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta(s)^2 = \prod_p (1 - p^{-s})^{-2}$$

$$= \prod_p (1 + 2p^{-s} + 3p^{-2s} + \ldots)$$

$$= \prod_p \left(1 + \frac{d(p)}{p^s} + \frac{d(p^2)}{p^{2s}} + \ldots\right) ,$$

$$\sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s} = \zeta(s)\ \zeta(s-k) = \prod_p [(1 - p^{-s})(1 - p^{k-s})]^{-1}$$

$$= \prod_p \left(1 + \frac{p^{k+1}}{p^s} + \frac{p^{2k}+p^k+1}{p^{2s}} + \ldots\right)$$

$$= \prod_p \left(1 + \frac{\sigma_k(p)}{p^s} + \frac{\sigma_k(p^2)}{p^{2s}} + \ldots\right) ,$$

also sind die beiden Funktionen $n \mapsto d(n)$ und $n \mapsto \sigma_k(n)$ multiplikativ (was man auch direkt leicht sieht), da trivialerweise die Umkehrung von Satz 1 gilt: besitzt eine Dirichletsche Reihe ein Euler-Produkt (8), so stellen die Koeffizienten dieser Reihe eine multiplikative Funktion dar.

d) Für den Kehrwert $\frac{1}{\zeta(s)}$ erhalten wir

$$(10)\qquad \frac{1}{\zeta(s)} = \prod_p (1 - p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} ,$$

wo $\mu(n)$ die multiplikative Funktion ist, die für Primzahlpotenzen die Werte $\mu(p) = -1$, $\mu(p^r) = 0$ $(r \geq 2)$ annimmt, d.h.

$$(11)\qquad \mu(n) = \begin{cases} 0, \text{ falls } n \text{ ein Quadrat enthält} \\ (-1)^k, \text{ falls } n = p_1 \cdots p_k,\ p_1 < \ldots < p_k . \end{cases}$$

Die Funktion $\mu(n)$ ist die sogenannte *Möbiussche Funktion*. Aus der Beziehung $\zeta(s) \cdot \frac{1}{\zeta(s)} = 1$ und der Faltungsformel (3) folgt die wichtige Eigenschaft dieser Funktion, daß

$$(12)\qquad \sum_{d|n} \mu(d) = \begin{cases} 1, \text{ falls } n = 1 \\ 0, \text{ falls } n > 1 . \end{cases}$$

Die Möbiussche Funktion ist wegen folgender *Möbiusschen Umkehrformel* wichtig.

SATZ 2: *Seien* f *und* g *zwei Funktionen von* $\mathbb{N}$ *nach* $\mathbb{C}$. *Ist für alle* n

$$(13)\qquad f(n) = \sum_{d|n} g(d) ,$$

so ist für alle n

$$(14)\qquad g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$$

und umgekehrt. Stehen f *und* g *in dieser Beziehung zueinander, so ist* g *multiplikativ genau dann, wenn* f *multiplikativ ist.*

Beweis: Die erste Aussage ist leicht aus (12) herzuleiten; wir wollen sie aber durch Anwendung von Dirichletschen Reihen erhalten, um Übung im Umgang mit solchen Reihen zu bekommen. Die Gleichungen

$$\begin{aligned} f(1) &= g(1) \\ f(2) &= g(1) + g(2) , \\ f(3) &= g(1) + g(3) , \\ f(4) &= g(1) + g(2) + g(4) , \ldots \end{aligned}$$

lassen sich induktiv für g lösen:

$$\begin{aligned} g(1) &= f(1) , \\ g(2) &= f(2) - f(1) , \\ g(3) &= f(3) - f(1) , \\ g(4) &= f(4) - f(2) , \ldots \end{aligned}$$

Es ist also klar, daß eine Beziehung wie (14) mit von f unabhängigen Koeffizienten existieren muß; somit brauchen wir (13) $\leftrightarrow$ (14) nur für Folgen $\{f(n)\}$, $\{g(n)\}$ von langsamem Wachstum zu beweisen (z.B. nur für solche mit $g(n) = 0$ für $n > n_0$) und können deshalb annehmen, daß die zugehörigen Dirichletschen Reihen

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} , \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

absolut konvergent sind (für mindestens ein s). Dann gilt wegen der Faltungsformel (3) und der Beziehung (10)

$$\begin{aligned} (13) \leftrightarrow F(s) &= \sum_{n=1}^{\infty} 1 . n^{-s} \sum_{m=1}^{\infty} g(m) m^{-s} = \zeta(s)\, G(s) \\ \leftrightarrow G(s) &= \zeta(s)^{-1} F(s) = \sum_{n=1}^{\infty} \mu(n) n^{-s} \sum_{m=1}^{\infty} f(m) m^{-s} \\ \leftrightarrow (14) , \end{aligned}$$

und, wenn (13) und (14) gelten,

g multiplikativ $\leftrightarrow$ G(s) besitzt eine Eulersche Produktentwicklung

$\leftrightarrow$ F(s) = ζ(s) G(s) besitzt eine Eulersche Produktentwicklung

$\leftrightarrow$ f multiplikativ .

Beispiel: Sei $\nu(n)$ die Anzahl der Primteiler von n (mit Multiplizität: $\nu(p_1^{r_1} \cdots p_k^{r_k}) = r_1 + \ldots + r_k$) und $\lambda(n) = (-1)^{\nu(n)}$. Dann ist $\lambda(n)$ multiplikativ und

$$(15)\qquad \begin{aligned} \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} &= \prod_p \left[1 - \frac{1}{p^s} + \frac{1}{p^{2s}} - \ldots\right] = \prod_p \left(\frac{1}{1+p^{-s}}\right) \\ &= \prod_p \left(\frac{1-p^{-s}}{1-p^{-2s}}\right) = \frac{\zeta(2s)}{\zeta(s)} \qquad (\sigma > 1) , \end{aligned}$$

also gilt (14) mit $g = \lambda$ und

$$(16)\qquad \begin{aligned} f(n) &= \text{Koeffizient von } n^{-s} \text{ in } \zeta(2s) \\ &= \begin{cases} 1, \text{ falls } n \text{ eine Quadratzahl ist,} \\ 0 \text{ sonst .} \end{cases} \end{aligned}$$

Es gilt also

$$(17)\qquad f(n) = \sum_{d|n} \lambda(d) .$$

Wir führen einige (z.T. schon besprochene) Beispiele von Dirichletschen Reihen mit multiplikativen Koeffizienten auf. Hierbei sind d, τ, σ_k, μ, λ die schon eingeführten arithmetischen Funktionen, $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ die Eulersche Funktion und $\omega(n)$ die Anzahl der verschiedenen Primteiler von n.

$f(n)$	$\sum f(n)n^{-s}$
1	$\zeta(s)$
$\mu(n)$	$1/\zeta(s)$
$\phi(n)$	$\zeta(s-1)/\zeta(s)$
$d(n)$	$\zeta(s)^2$
$\tau(n)$	$\zeta(s)\ \zeta(s-1)$
$\sigma_k(n)$	$\zeta(s)\ \zeta(s-k)$
$\lambda(n)$	$\zeta(2s)/\zeta(s)$
$2^{\omega(n)}$	$\zeta(s)^2/\zeta(2s)$
$\mu(n)^2$	$\zeta(s)/\zeta(2s)$
$d(n)^2$	$\zeta(s)^4/\zeta(2s)$
$d(n^2)$	$\zeta(s)^3/\zeta(2s)$
$\sigma_k(n)\sigma_\ell(n)$	$\zeta(s)\zeta(s-k)\zeta(s-\ell)\zeta(s-k-\ell)/\zeta(2s-k-\ell)$

Als letztes Beispiel sei

$$r(n) = \#\{(a,b)\in\mathbb{Z}^2 \mid a^2 + b^2 = n\}$$

die Anzahl der Darstellungen von n als Summe von zwei Quadraten (z.B. $r(1) = 4$, da $1 = 0^2 + 1^2 = 0^2 + (-1)^2 = 1^2 + 0^2 = (-1)^2 + 0^2$). Dann ist die Funktion $\frac{1}{4} r(n)$ multiplikativ und die entsprechende Dirichletsche Reihe ist durch

$$(18) \qquad \sum_{n=1}^{\infty} \frac{1}{4} r(n)\, n^{-s} = \zeta(s)\, L(s)$$

gegeben, wobei

$$L(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \dots$$

die Dirichletsche Reihe mit den periodischen und multiplikativen Koeffizienten

$$\chi(n) = \begin{cases} +1, & \text{falls } n \equiv 1 \pmod 4 \\ -1, & \text{falls } n \equiv -1 \pmod 4 \\ 0, & \text{falls } n \equiv 0 \pmod 2 \end{cases}$$

bezeichnet. Die Beziehung (18) ist zu dem nichttrivialen Satz

$$r(n) = 4 \sum_{d|n} \chi(d)$$

(oder, nach Satz 2, zu $\chi(n) = \frac{1}{4} \sum_{d|n} \mu(\frac{n}{d})\, r(d)$) äquivalent. Mit Reihen wie $L(s)$ werden wir uns ab §6 eingehend beschäftigen.

Aufgaben:

1. Man beweise die beiden Aussagen von Satz 2 (also die Äquivalenz von (13) und (14) und die Tatsache, daß f genau dann multiplikativ ist, wenn g es ist) ohne Verwendung von Dirichletschen Reihen.

2. Man folgere aus (4) und den Sätzen 2 und 4 des §1, daß

$$\sum_{n\le N} d(n) = O(N^{1+\varepsilon})$$

für alle $\varepsilon > 0$ gilt. (In der Tat gilt die stärkere Aussage $d(n) = O(n^{\varepsilon})$.)

3. Man beweise die Identität $\sum_{d|n} a^{\omega(d)} = d(n^a)$ (a, n natürliche Zahlen).

4. Man beweise die in der Tabelle am Ende des Paragraphen angegebenen Dirichletschen Reihenentwicklungen mit Hilfe des Eulerschen Produkts und bestimme für jede Reihe die Konvergenzabszisse.

5. Sei κ die durch

$$\kappa(1) = 1\ ,\ \kappa(p_1^{r_1}\dots p_k^{r_k}) = r_1\dots r_k \qquad (r_1,\dots,r_k\ge 1,\ p_1<\dots<p_k \text{ Primzahlen})$$

definierte multiplikative Funktion. Man zeige, daß für $0 \le a \le 4$ die Dirichletsche Reihe $\sum_{n=1}^{\infty} \kappa(n^a)\, n^{-s}$ mit Hilfe der Riemannschen Zetafunktion ausgedrückt werden kann. (Dies gilt für keinen anderen Wert von a.)

6. Sei $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ eine Dirichletsche Reihe, die als Produkt von Zetafunktionen ausgedrückt werden kann (also $F(s) =$

$\prod_{i=1}^{N} \zeta(a_i s+b_i)^{c_i}$ für geeignete ganze Zahlen a_i, b_i, c_i; $a_i > 0$).
Man zeige, daß dann auch die Reihe $\sum_{n=1}^{\infty} \lambda(n) f(n) n^{-s}$ so ausgedrückt werden kann und schreibe die entsprechenden Identitäten für die Dirichletschen Reihen der Aufgaben 4 und 5 explizit hin.

7. Sei $g(n)$ die Anzahl der nichtisomorphen abelschen Gruppen der Ordnung n. Man benutze den Strukturssatz für endliche abelsche Gruppen um zu zeigen, daß $g(n)$ die multiplikative Funktion ist, deren Wert für eine Primzahlpotenz p^r gleich der Anzahl der Partitionen von r ist (also der Zerlegungen $r = r_1 + r_2 + \ldots$ mit $r_1 \geq r_2 \geq \ldots > 0$). Man schließe hieraus, daß die Dirichletsche Reihe

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

für $\sigma > 1$ gleich dem (konvergenten) Produkt

$$\zeta(s)\zeta(2s)\zeta(3s)\ldots$$

ist; insbesondere ist $G(s)$ holomorph für $\sigma > 1$ und hat einen Pol bei $s = 1$ mit Residuum

$$C = \zeta(2)\zeta(3)\zeta(4)\ldots = 2{,}29485\ldots .$$

Es kann gezeigt werden, daß

$$\sum_{n=1}^{N} g(n) = CN + O(\sqrt{N}) ;$$

d.h. der Mittelwert von $g(n)$ ist gleich C, also endlich!

§3 Die Gammafunktion

Die Gammafunktion ist eine der wichtigsten mathematischen Funktionen und sicherlich die einfachste von den nichtelementaren Funktionen. Sie spielt eine ganz wesentliche Rolle bei der Untersuchung von Dirichletschen Reihen.

Man sucht eine Interpolationsfunktion für die Funktion $n \mapsto n!$, d.h. eine stetige Funktion $\Pi(x)$, so daß $\Pi(n) = n!$ für alle natürlichen Zahlen n ist. Einem vielleicht unglücklichen, von Legendre

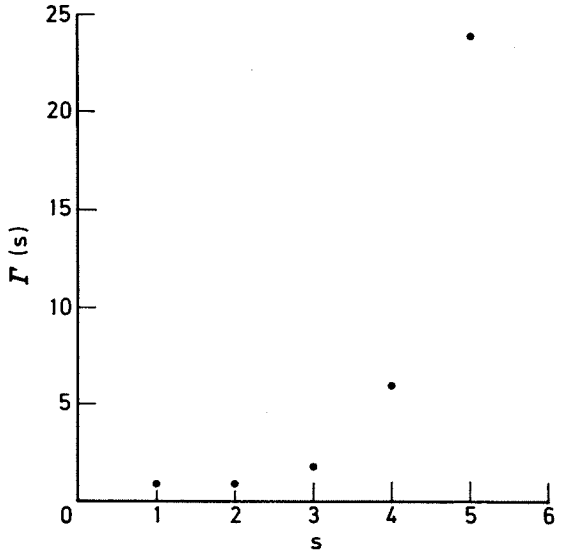
eingeführten Brauch folgend, machen wir die Substitution $x = s - 1$ und schreiben $\Gamma(s)$ für $\Pi(x) = \Pi(s-1)$. Wir suchen also eine stetige Funktion $\Gamma(s)$, die

(1) $\Gamma(n) = (n-1)!$ $(n = 1, 2, \ldots)$

erfüllt und außerdem die Grundeigenschaft $n! = n.(n-1)!$ der Fakultät noch besitzt:

(2) $\Gamma(s+1) = s\Gamma(s)$ für alle $s \neq 0$.

Wie findet man eine solche Funktion? Für s klein muß $\Gamma(s)$ durch folgende Punkte hindurchgehen:



und es ist nicht klar, wie man interpolieren soll; für n groß ist die Funktion $n \mapsto n!$ wegen des schnellen Wachstums viel gleichmäßiger, und es sollte leichter sein, sie zu interpolieren. Durch wiederholte Anwendung von (2) erhalten wir

(3) $\Gamma(s+N) = s(s+1) \ldots (s+N-1)\Gamma(s)$;

es reicht also, eine asymptotische Formel für $\Gamma(s+N)$ $(N \to \infty)$ anzugeben. Für $s \in \mathbb{N}$ gilt

$$\Gamma(s+N) = (N+s-1)! = (N+s-1)(N+s-2)\dots(N+1)\cdot N\cdot(N-1)!$$

$$= N^s(1+\tfrac{s-1}{N})(1+\tfrac{s-2}{N})\dots(1+\tfrac{1}{N})\cdot(N-1)!\ ,$$

also $\Gamma(s+N) \sim N^s(N-1)!$ für $N \to \infty$. Es ist daher naheliegend, $\Gamma(s)$ für alle s durch

$$\Gamma(s) = \lim_{N\to\infty} \frac{N^s(N-1)!}{s(s+1)\dots(s+N-1)} \qquad (s \in \mathbb{C}) \tag{4}$$

zu definieren, falls der Grenzwert existiert. Das ist auch der Fall, falls $s \notin -\mathbb{N}$: sei

$$\Gamma_N(s) = \frac{N^s(N-1)!}{s(s+1)\dots(s+N-1)} \qquad (N \in \mathbb{N})\ ; \tag{5}$$

dann ist

$$\frac{\Gamma_{N+1}(s)}{\Gamma_N(s)} = (\tfrac{N+1}{N})^s \tfrac{N}{s+N} = (1+\tfrac{1}{N})^s\ (1+\tfrac{s}{N})^{-1}$$

$$= (1+\tfrac{s}{N}+O(\tfrac{1}{N^2}))\ (1-\tfrac{s}{N}+O(\tfrac{1}{N^2})) = (1+O(\tfrac{1}{N^2})),$$

und das beweist, daß das Produkt $\prod_{N\ge 1} \frac{\Gamma_{N+1}(s)}{\Gamma_N(s)}$ konvergiert, d.h. daß $\lim_{N\to\infty} \Gamma_N(s)$ existiert. Wir erhalten auch

$$\Gamma_N(s) = \Gamma_1(s) \prod_{n=1}^{N-1} \frac{\Gamma_{n+1}(s)}{\Gamma_n(s)} = \frac{1}{s} \prod_{n=1}^{N-1} [\ (1+\tfrac{1}{n})^s\ (1+\tfrac{s}{n})^{-1}\ ]$$

und somit

$$\Gamma(s+1) = s\Gamma(s) = \prod_{n=1}^{\infty} \frac{(1+\frac{1}{n})^s}{(1+\frac{s}{n})}\ , \tag{6}$$

eine von Euler stammende Produktformel für die Γ-Funktion.

Die Eigenschaft (2) der durch (4) definierten Funktion ist klar, da

$$\Gamma(s+1) = \lim_{N\to\infty} [\ \frac{N^{s+1}(N-1)!}{(s+1)(s+2)\dots(s+N)}\ ]$$

$$= \lim_{N\to\infty} [\ s\cdot\frac{N}{N+s}\cdot\frac{N^s(N-1)!}{s(s+1)\dots(s+N-1)}\ ]$$

$$= \lim_{N\to\infty} [\ s\cdot\frac{N}{N+s}\cdot\Gamma_N(s)\ ] = s\Gamma(s)$$

ist. Die Gleichung (1) folgt jetzt durch Induktion, da $\Gamma(1)$ nach (6) gleich 1 ist.

Wenn wir (4) in der Gestalt

$$\Gamma(s+1) = s\Gamma(s) = \lim_{N\to\infty} [\ \frac{N^s}{(1+\frac{s}{1})(1+\frac{s}{2})\dots(1+\frac{s}{N-1})}\ ] \tag{7}$$

schreiben und Logarithmen nehmen, erhalten wir für $|s| < 1$

$$\log\Gamma(s+1) = \lim_{N\to\infty} [\ s\log N - \sum_{n=1}^{N-1} \log(1+\tfrac{s}{n})\ ]$$

$$= \lim_{N\to\infty} [\ s\log N - \sum_{n=1}^{N-1} (\tfrac{s}{n} - \tfrac{s^2}{2n^2} + \tfrac{s^3}{3n^3} - \dots)\ ]$$

$$= \lim_{N\to\infty} [\ s(\log N - (1+\tfrac{1}{2}+\tfrac{1}{3}+\dots+\tfrac{1}{N-1}))$$

$$+ \tfrac{s^2}{2}(\tfrac{1}{1^2}+\tfrac{1}{2^2}+\dots+\tfrac{1}{(N-1)^2})$$

$$- \tfrac{s^3}{3}(\tfrac{1}{1^3}+\tfrac{1}{2^3}+\dots+\tfrac{1}{(N-1)^3}) + \dots\ ]\ .$$

Die Folge $1+\frac{1}{2}+\dots+\frac{1}{N-1} - \log N$ hat, wie man leicht zeigt, für $N\to\infty$ einen Grenzwert, den man mit γ bezeichnet und die *Eulersche Konstante* nennt. Für $r \ge 2$ strebt $1+\frac{1}{2^r}+\dots+\frac{1}{(N-1)^r}$ nach dem Limes $\sum_{n=1}^{\infty} \frac{1}{n^r} = \zeta(r)$, wo $\zeta(r)$ die in (1.11) eingeführte Riemannsche Zetafunktion bezeichnet. Es gilt also

$$\log\Gamma(1+s) = -\gamma s + \frac{\zeta(2)}{2}s^2 - \frac{\zeta(3)}{3}s^3 + \dots \qquad (|s|<1)\ . \tag{8}$$

(Die Vertauschung von Summation und Grenzübergang ist erlaubt: vgl. Aufgabe 1.) Die Werte der Zetafunktion an ganzzahligen Stellen treten also als Koeffizienten der Taylorentwicklung von $\log\Gamma(s)$ an der Stelle $s = 1$ auf.

Wir können mit Hilfe der Beziehung

$$1+\tfrac{1}{2}+\dots+\tfrac{1}{N} = \log N + \gamma + o(1)$$

auch eine weitere Produktformel für $\Gamma(s)$ herleiten, indem wir

$$N^s = e^{s\log N} = e^{s(1+\frac{1}{2}+\dots+\frac{1}{N}-\gamma+o(1))}$$

$$\sim e^{-\gamma s}\ e^{s(1+\frac{1}{2}+\dots+\frac{1}{N})}$$

in (7) einsetzen; dies liefert die Formel

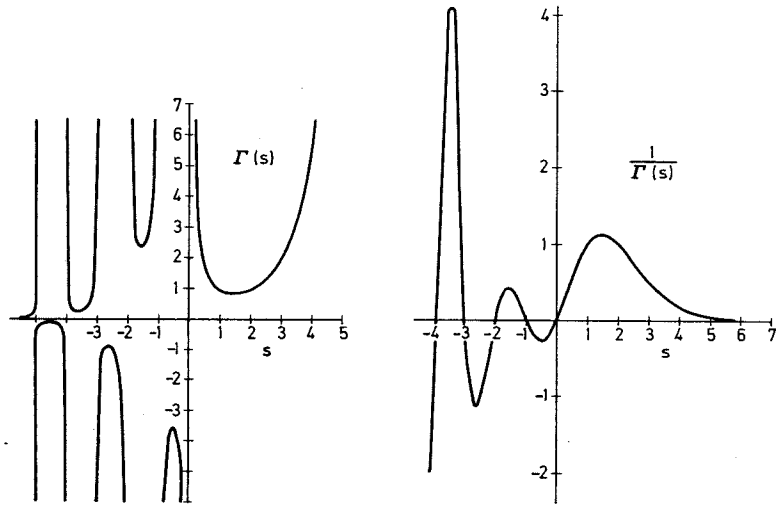
$$\frac{1}{\Gamma(s)} = se^{\gamma s} \prod_{n=1}^{\infty} [(1+\tfrac{s}{n})e^{-s/n}]\ , \tag{9}$$

die sogenannte Weierstraßsche Produktdarstellung. Aus (6) oder (9) folgt, daß die Funktion $1/\Gamma(s)$ in der ganzen komplexen Ebene definiert und holomorph ist (weil die Produktentwicklungen jeweils kon-

vergieren). Ferner hat $1/\Gamma(s)$ nach (9) einfache Nullstellen bei $s = 0, -1, -2, \ldots$ und ist sonst von Null verschieden. Das beweist folgenden

SATZ: *Die durch (4), (6) oder (9) erklärte Funktion* $\Gamma(s)$ *ist in der ganzen komplexen Ebene als meromorphe Funktion von* s *definiert. Sie hat bei* $s = 0, -1, -2, \ldots$ *einfache Pole und ist sonst holomorph. Außerdem ist sie nie gleich Null, d.h. die Funktion* $1/\Gamma(s)$ *ist überall holomorph.*

Auf der reellen Achse sehen $\Gamma(s)$ bzw. $\frac{1}{\Gamma(s)}$ so aus:



Wir geben noch ein paar Eigenschaften der Γ-Funktion an.

1. Sei

$$f(s) = \Gamma(\tfrac{s}{2})\Gamma(\tfrac{s+1}{2}) \ ;$$

dann gilt

$$f(s+1) = \Gamma(\tfrac{s+1}{2})\ \Gamma(\tfrac{s}{2}+1) = \tfrac{s}{2}\,\Gamma(\tfrac{s+1}{2})\ \Gamma(\tfrac{s}{2}) = \tfrac{s}{2}\,f(s)$$

oder $2^{s+1}f(s+1) = s\cdot 2^s f(s)$. Es ist dann naheliegend zu vermuten, daß $2^s f(s)$ eine Konstante mal $\Gamma(s)$ ist, und dies ist auch der Fall:

$$2^s\Gamma(\tfrac{s}{2})\Gamma(\tfrac{s+1}{2}) = \lim_{N\to\infty} 2^s\left[\frac{N^{\frac{s}{2}}(N-1)!}{\frac{s}{2}(\frac{s}{2}+1)\ldots(\frac{s}{2}+N-1)}\cdot\frac{N^{\frac{s+1}{2}}(N-1)!}{(\frac{s+1}{2})(\frac{s+1}{2}+1)\ldots(\frac{s+1}{2}+N-1)}\right]$$

$$= \lim_{N\to\infty}\left[\frac{2^{2N+s}\,N^{s+\frac{1}{2}}\,(N-1)!^2}{s(s+2)(s+4)\ldots(s+2N-2)\ \times\ (s+1)(s+3)\ldots(s+2N-1)}\right]$$

$$= \lim_{N\to\infty}\left[2^{2N}N^{\frac{1}{2}}\frac{(N-1)!^2}{(2N-1)!}\frac{(2N)^s\,(2N-1)!}{s(s+1)(s+2)\ldots(s+2N-1)}\right]$$

$$= C\,\Gamma(s)$$

mit

$$C = \lim_{N\to\infty}\left[2^{2N}N^{\frac{1}{2}}\frac{(N-1)!^2}{(2N-1)!}\right] . \tag{10}$$

Die Konstante C ist gleich $2\sqrt{\pi}$ (siehe Aufgabe 4), also erhalten wir

$$\Gamma(\tfrac{s}{2})\ \Gamma(\tfrac{s+1}{2}) = 2^{1-s}\ \sqrt{\pi}\ \Gamma(s) \ , \tag{11}$$

die Legendresche Verdoppelungsformel. Insbesondere folgt mit $s = 1$, daß

$$\Gamma(\tfrac{1}{2}) = \sqrt{\pi} \ . \tag{12}$$

2. Die Funktion $\frac{1}{\Gamma(s)}$ ist holomorph und hat Nullstellen bei $s = 0, -1, -2, \ldots$, also ist die Funktion

$$g(s) = \frac{1}{\Gamma(s)\ \Gamma(1-s)}$$

auch holomorph und hat Nullstellen bei $s = \ldots, -2, -1, 0, 1, 2, \ldots$ Außerdem ist

$$g(s+1) = \frac{1}{\Gamma(1+s)\Gamma(-s)} = \frac{1}{s\Gamma(s)\ \Gamma(-s)} = \frac{-1}{\Gamma(s)\ \Gamma(1-s)} = -g(s)$$

insbesondere ist $g(s)$ periodisch mit Periode 2. Es liegt dann nahe, daß $g(s) = C \sin \pi s$ ist, wobei die Konstante C wegen $\lim_{s\to 0}[g(s)/s] = \lim_{s\to 0}[1/\Gamma(1+s)\ \Gamma(1-s)] = 1$ gleich $1/\pi$ sein muß:

$$\Gamma(s)\ \Gamma(1-s) = \frac{\pi}{\sin\ \pi s} \ . \tag{13}$$

Diese Formel ist auch richtig, z.B. wegen (9) und der bekannten Beziehung

$$\frac{\sin\ \pi s}{\pi s} = \prod_{n=1}^{\infty}\ (1 - \frac{s^2}{n^2}) \ . \tag{14}$$

3. Schließlich sei

$$h(s) = \int_0^\infty t^{s-1}\ e^{-t}\ dt \ .$$

Das Integral konvergiert für $\sigma > 0$ und es gilt

$$h(s+1) = \int_0^\infty t^s\ d(-e^{-t}) = \int_0^\infty e^{-t}\ d(t^s)$$

$$= s \int_0^\infty t^{s-1}\, e^{-t}\, dt = sh(s)$$

(partielle Integration) und

$$h(1) = \int_0^\infty e^{-t}\, dt = 1 \ ;$$

die Funktion $h(s)$ ist also ein Kandidat für die ursprünglich gesuchte Funktion $\Gamma(s)$ mit den Eigenschaften (1) und (2). Es ist in der Tat nicht schwer zu zeigen, daß $h(s) = \Gamma(s)$ ist (siehe Aufgabe 6), also

$$\Gamma(s) = \int_0^\infty t^{s-1}\, e^{-t}\, dt \qquad (\sigma > 0) \ . \tag{15}$$

Es ist diese Formel, die die Wichtigkeit der Gammafunktion für die Theorie der Dirichletschen Reihen erklärt. Man hat nämlich

$$\int_0^\infty t^{s-1}\, e^{-nt}\, dt = n^{-s} \int_0^\infty u^{s-1}\, e^{-u}\, du \qquad (u = nt)$$

$$= \Gamma(s)\, n^{-s} \ ,$$

also (im Bereich der absoluten Konvergenz)

$$\sum_{n=1}^\infty \frac{a_n}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty \Big(\sum_{n=1}^\infty a_n e^{-nt} \Big)\, t^{s-1}\, dt \ . \tag{16}$$

Das heißt, die (gewöhnliche) Dirichletsche Reihe $f(s) = \sum a_n n^{-s}$ und die Potenzreihe $F(z) = \sum a_n z^n$ mit denselben Koeffizienten sind durch die Integraltransformation

$$f(s) = \frac{1}{\Gamma(s)} \int_0^\infty F(e^{-t})\, t^{s-1}\, dt \ , \tag{17}$$

die sogenannte *Mellinsche Transformation*, miteinander verknüpft. Dies ermöglicht es häufig, von Eigenschaften von Potenzreihen auf Eigenschaften von Dirichletschen Reihen zu schließen oder umgekehrt.

Natürlich gilt auch für nicht-gewöhnliche Dirichletsche Reihen das Analogon von (16), nämlich

$$\sum_{n=1}^\infty a_n \lambda_n^{-s} = \frac{1}{\Gamma(s)} \int_0^\infty \Big(\sum_{n=1}^\infty a_n\, e^{-\lambda_n t} \Big)\, t^{s-1}\, dt \ . \tag{18}$$

Als Beispiele für (16) nehmen wir die Dirichletschen Reihen, die in §1 als Beispiele verwendet wurden:
Für $\zeta(s) = \sum n^{-s}$ ist $a_n = 1$, also $\sum a_n e^{-nt} = \frac{1}{e^t - 1}$, und wir finden

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{t^{s-1}\, dt}{e^t - 1} \qquad (\sigma > 1) \ . \tag{19}$$

Für $\psi(s) = \sum (-1)^{n-1} n^{-s} = (1 - 2^{1-s})\, \zeta(s)$ ist $a_n = (-1)^{n-1}$, also $\sum a_n e^{-nt} = \frac{1}{e^t + 1}$, und wir finden

$$(1 - 2^{1-s})\, \zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{t^{s-1}\, dt}{e^t + 1} \qquad (\sigma > 0) \ . \tag{20}$$

Aufgaben:

1. Man zeige die Existenz von $\gamma = \lim_{N\to\infty} (1 + \frac{1}{2} + \ldots + \frac{1}{N} - \log N)$ und die Zulässigkeit der Vertauschung von Summation und Grenzübergang, die zu (8) führte.

2. Man beweise für jede natürliche Zahl n die Beziehung

$$n^s\, \Gamma(\tfrac{s}{n})\, \Gamma(\tfrac{s+1}{n}) \ldots \Gamma(\tfrac{s+n-1}{n}) = C_n\, \Gamma(s)$$

mit einer nur von n abhängigen Konstanten (es ist $C_n = (2\pi)^{\frac{n-1}{2}} \sqrt{n}$, siehe Aufgabe 5). Diese Formel stammt von Gauß.

3. Man bestimme das Residuum von $\Gamma(s)$ an jeder Polstelle.

4. Man beweise, daß die durch (10) definierte Konstante C gleich $2\sqrt{\pi}$ ist, indem man aus (13) den Wert $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ entnimmt und $s = 1$ in die Beziehung

$$2^s\, \Gamma(\tfrac{s}{2})\, \Gamma(\tfrac{s+1}{2}) = C\, \Gamma(s)$$

einsetzt. Man schließe auch aus (12) und (15), daß

$$\int_0^\infty e^{-t^2}\, dt = \frac{1}{2} \sqrt{\pi}$$

ist.

5. Man beweise die Stirlingsche Formel

$$\Gamma(x) \sim \sqrt{2\pi}\, x^{x-\frac{1}{2}}\, e^{-x} \qquad (x \to \infty) \ ,$$

indem man zunächst den Beweis der Existenz des Limes (4) nachahmt, um zu zeigen, daß der Grenzwert $A = \lim_{x\to\infty} [\Gamma(x)/x^{x-\frac{1}{2}} e^{-x}]$ existiert, und dann aus der in Aufgabe 4 bewiesenen Tatsache, daß die rechte Seite von (10) gleich $2\sqrt{\pi}$ ist, die Beziehung $A = \sqrt{2\pi}$ folgert. Man benutze auch die Stirlingsche Formel, um für die Konstante C_n

in Aufgabe 2 den Wert $(2\pi)^{\frac{n-1}{2}}\sqrt{n}$ zu erhalten.

6. Man beweise (15), indem man die Beziehungen

$$\int_0^N (1-\frac{t}{N})^N t^{s-1}\,dt = N^s \sum_{r=0}^{N} \frac{(-1)^r \binom{N}{r}}{r+s} = \frac{N}{N+s}\,\Gamma_N(s)$$

nachweist (die erste durch gliedweise Integration, die zweite durch Vergleich der Polstellen der zwei rationalen Funktionen von s) und dann unter Benutzung von $\lim_{N\to\infty}(1-\frac{t}{N})^N = e^{-t}$ den Grenzübergang $N \to \infty$ (streng) durchführt.

§4 Die Riemannsche Zetafunktion

Die einfachste und wichtigste Dirichletsche Reihe ist die in (1.11) eingeführte Riemannsche ζ-Funktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (\sigma > 1)\ . \tag{1}$$

Wir haben schon in §1 gesehen, daß $\zeta(s)$ sich als meromorphe Funktion in die Halbebene $\sigma > 0$ fortsetzen läßt, und zwar (Aufgabe 3, §1) mit einem einfachen Pol bei $s = 1$ als einzige Singularität. Wir haben auch in §2 die für $\sigma > 1$ gültige Eulersche Produktdarstellung

$$\zeta(s) = \prod_{p \text{ prim}} \frac{1}{1-p^{-s}} \tag{2}$$

bewiesen und in §3 die ebenfalls für $\sigma > 1$ geltende Integraldarstellung

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{t^{s-1}}{e^t-1}\,dt \tag{3}$$

gewonnen. Die wichtigsten in diesem Paragraphen bewiesenen Eigenschaften der ζ-Funktion sind im folgenden Satz zusammengestellt.

SATZ: *Die durch (1) für $\sigma > 1$ definierte Funktion $\zeta(s)$ besitzt eine meromorphe Fortsetzung in die ganze komplexe Ebene, und zwar mit einem einfachen Pol vom Residuum 1 an der Stelle $s = 1$ als einzige Polstelle. Die Werte der ζ-Funktion bei nichtpositiven ganzen Zahlen sind rational, und zwar ist*

$$\zeta(0) = -\frac{1}{2} \tag{4}$$

$$\zeta(-2n) = 0 \qquad (n = 1, 2, 3, \ldots)\ , \tag{5}$$

$$\zeta(1-2n) = -\frac{B_{2n}}{2n} \qquad (n = 1, 2, 3, \ldots)\ , \tag{6}$$

wobei die rationalen Zahlen $B_2 = \frac{1}{6}$, $B_4 = \frac{-1}{30}, \ldots$ die durch

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} t^k \qquad (|t| < 2\pi) \tag{7}$$

definierten Bernoullischen Zahlen *sind. Die Werte der Zetafunktion an positiven geraden ganzen Zahlen sind durch*

$$\zeta(2n) = \frac{(-1)^{n-1}\, 2^{2n-1}\, B_{2n}}{(2n)!}\,\pi^{2n} \qquad (n = 1, 2, 3, \ldots) \tag{8}$$

gegeben.

Beweis: Wir gehen von der Integraldarstellung (3) aus. Seien die Zahlen B_k $(k = 0, 1, 2, \ldots)$ durch (7) definiert, d.h. wir entwickeln

$$\frac{t}{e^t-1} = \frac{t}{t + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots} = 1 - \frac{t}{2} + \frac{t^2}{12} + 0t^3 - \frac{t^4}{720} + \ldots$$

und definieren B_n als $n!$ mal den Koeffizienten von t^n auf der rechten Seite; aus

$$\frac{t}{e^t-1} - \frac{-t}{e^{-t}-1} = -t$$

folgt, daß abgesehen von $B_1 = -\frac{1}{2}$ alle B_n mit n ungerade Null sind. Sei jetzt $n > 0$ fest und

$$f_n(t) = \sum_{k=0}^{n} (-1)^k \frac{B_k}{k!} t^k = 1 + \frac{t}{2} + \frac{B_2}{2!} t^2 + \ldots + \frac{B_n}{n!} t^n$$

(für $n > 1$ ist $(-1)^n B_n = B_n$). Dann ist für $\sigma > 1$

$$\begin{aligned}\Gamma(s)\cdot\zeta(s) &= \int_0^{\infty} \frac{te^t}{e^t-1} e^{-t} t^{s-2}\,dt \\ &= \int_0^{\infty} \left(\frac{te^t}{e^t-1} - f_n(t)\right) e^{-t} t^{s-2}\,dt + \int_0^{\infty} f_n(t) e^{-t} t^{s-2}\,dt \qquad (9) \\ &= I_1(s) + I_2(s)\ ,\end{aligned}$$

wobei wir mit I_1 und I_2 die beiden Integrale bezeichnen. Die Funk-

tion $\frac{te^t}{e^t-1}$ ist bei $t = 0$ holomorph und hat dort die Taylor-Entwicklung

$$\frac{te^t}{e^t-1} = \frac{-t}{e^{-t}-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} B_k t^k ,$$

und somit

$$\frac{te^t}{e^t-1} - f_n(t) = O(t^{n+1}) \qquad (t \to 0) .$$

Es folgt daraus, daß das Integral $I_1(s)$ konvergiert für alle s mit $\sigma > -n$ (da der Integrand für $t \to 0$ $O(t^{n+\sigma-1})$ ist und für $t \to \infty$ exponentiell klein ist), also stellt $I_1(s)$ im Bereich $\sigma > -n$ eine holomorphe Funktion dar. Das zweite Integral $I_2(s)$ ist nur für $\sigma > 1$ konvergent, läßt sich aber, da $f_n(t)$ ein Polynom ist, mit Hilfe von (3.15) explizit ausrechnen:

$$\begin{aligned} I_2(s) &= \int_0^{\infty} \left[1 + \frac{t}{2} + \sum_{k=2}^{n} \frac{B_k}{k!} t^k \right] e^{-t} t^{s-2} \, dt \\ &= \Gamma(s-1) + \frac{1}{2}\Gamma(s) + \sum_{k=2}^{n} \frac{B_k}{k!} \Gamma(s+k-1) . \end{aligned} \tag{10}$$

Das ist wegen der Ergebnisse von §3 eine in der ganzen komplexen Ebene meromorphe Funktion, und somit haben wir bewiesen, daß $\zeta(s)$ sich in die Halbebene $\sigma > -n$ (und deswegen, da n beliebig war, in ganz $\mathbb{C}$) meromorph fortsetzen läßt. Indem wir (10) in (9) einsetzen und die Funktionalgleichung (3.3) anwenden, erhalten wir die für $\sigma > -n$ gültige Darstellung

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \sum_{k=2}^{n} \frac{B_k}{k!} s(s+1)\dots(s+k-2) + \frac{1}{\Gamma(s)} I_1(s) \tag{11}$$

der ζ-Funktion, wobei $I_1(s)$ in $\sigma > -n$ holomorph ist. Da nach §3 die Funktion $\frac{1}{\Gamma(s)}$ überall holomorph ist, zeigt diese Formel, daß $\zeta(s) - \frac{1}{s-1}$ in $\sigma > -n$ holomorph ist; da n beliebig war, ist $\zeta(s) - \frac{1}{s-1}$ sogar in ganz $\mathbb{C}$ holomorph, und die erste Behauptung des Satzes ist bewiesen.

Sei jetzt s eine ganze Zahl, die $> -n$ und ≤ 0 ist; dann ist $\frac{1}{\Gamma(s)} I_1(s)$ wegen des Pols der Γ-Funktion an der Stelle s gleich Null, und somit ist

$$\begin{aligned} \zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \frac{s}{12} - \frac{s(s+1)(s+2)}{720} + \frac{s(s+1)(s+2)(s+3)(s+4)}{30240} \\ - \dots + \frac{B_n}{n!} s(s+1)\dots(s+n-2) \qquad (s = 0,-1,-2,\dots,-n+1) \end{aligned} \tag{12}$$

Dies zeigt, daß

$$\begin{aligned} \zeta(0) &= \frac{1}{-1} + \frac{1}{2} = -\frac{1}{2} \\ \zeta(-1) &= \frac{1}{-2} + \frac{1}{2} - \frac{1}{12} = -\frac{1}{12} \\ \zeta(-2) &= \frac{1}{-3} + \frac{1}{2} - \frac{1}{6} + 0 = 0 \\ \zeta(-3) &= \frac{1}{-4} + \frac{1}{2} - \frac{1}{4} + 0 + \frac{1}{120} = \frac{1}{120} \\ \zeta(-4) &= \frac{1}{-5} + \frac{1}{2} - \frac{1}{3} + 0 + \frac{1}{30} + 0 = 0 \end{aligned} \tag{13}$$

gilt. Es ist klar, daß man dieses Verfahren (mit n genügend groß) fortsetzen könnte, um $\zeta(-k)$ für jede nichtnegative ganze Zahl k auszurechnen, und daß die Werte alle rational ausfallen. Aus (12) bekommt man explizit

$$\begin{aligned} \zeta(-k) &= \frac{-1}{k+1} + \frac{1}{2} + \sum_{r=2}^{n} \frac{B_r}{r!} (-k)(-k+1)\dots(-k+r-2) \qquad (n > k) \\ &= -\frac{1}{k+1} + \frac{1}{2} + \sum_{r=2}^{k+1} (-1)^{r-1} \frac{B_r}{r!} \frac{k!}{(k+1-r)!} \\ &= -\frac{1}{k+1} \sum_{r=0}^{k+1} \binom{k+1}{r} B_r . \end{aligned}$$

Daß diese Summe, wie in (5), (6) behauptet, für $k > 0$ immer gleich ihrem letzten Glied $-\frac{B_{k+1}}{k+1}$ ist (vgl. die Beispiele (13)), d.h. daß die Bernoullischen Zahlen der Beziehung

$$\sum_{r=0}^{n} \binom{n}{r} B_r = (-1)^n B_n \tag{14}$$

genügen, läßt sich leicht mit Hilfe der erzeugenden Reihe (7) beweisen:

$$\begin{aligned} \sum_{n=0}^{\infty} \left[\sum_{r=0}^{n} \binom{n}{r} B_r \right] \frac{t^n}{n!} &= \sum_{0 \leq r \leq n} \sum \frac{B_r t^n}{r!(n-r)!} \\ &= \sum_{r=0}^{\infty} \sum_{k=0}^{\infty} \frac{B_r t^{r+k}}{r!k!} = \left(\sum_{r=0}^{\infty} \frac{B_r}{r!} t^r \right) \left(\sum_{k=0}^{\infty} \frac{t^k}{k!} \right) \\ &= \frac{t}{e^t-1} \cdot e^t = \frac{-t}{e^{-t}-1} = \sum_{n=0}^{\infty} (-1)^n B_n \frac{t^n}{n!} . \end{aligned}$$

Die Beziehung (14) kann übrigens als Rekursionsformel zur Berechnung der B_n benutzt werden.

Es bleibt nur noch, die Behauptung (8) über die Werte von $\zeta(2n)$ zu beweisen, also die Beziehungen

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}\ ,\quad \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}\ ,\quad \sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{\pi^6}{945}\ ,$$

$$\sum_{n=1}^{\infty} \frac{1}{n^8} = \frac{\pi^8}{9450}\ ,\quad \sum_{n=1}^{\infty} \frac{1}{n^{10}} = \frac{\pi^{10}}{93555}\ ,\quad \sum_{n=1}^{\infty} \frac{1}{n^{12}} = \frac{691\,\pi^{12}}{638512875}\ ,\ \ldots$$

von denen die beiden ersten von Euler entdeckt wurden, der sehr stolz darauf war. Mit Hilfe der Gleichungen (13) und (8) aus §3 erhält man

$$\sum_{n=1}^{\infty} (-1)^{n-1}\, 2^{2n-1}\, \pi^{2n}\, \frac{B_{2n}}{(2n)!}\, s^{2n} = -\frac{1}{2}\left[\frac{2\pi i s}{e^{2\pi i s}-1} - 1 + \frac{2\pi i s}{2}\right] \qquad (|s| < 1)$$

$$= \frac{1}{2} - \frac{\pi i s}{2}\,\frac{e^{\pi i s} + e^{-\pi i s}}{e^{\pi i s} - e^{-\pi i s}}$$

$$= \frac{1}{2}\,\left(1 - \frac{\pi s}{\tan \pi s}\right)$$

$$= \frac{s}{2}\,\frac{d}{ds}\,\log \frac{\pi s}{\sin \pi s}$$

$$= \frac{s}{2}\,\frac{d}{ds}\,\log\left[\,\Gamma(1+s)\,\Gamma(1-s)\,\right]$$

$$= \frac{s}{2}\,\frac{d}{ds}\left[\,\zeta(2)\,s^2 + \frac{\zeta(4)}{2}\,s^4 + \ldots\,\right]$$

$$= \sum_{n=1}^{\infty} \zeta(2n)\, s^{2n}$$

(man braucht übrigens hier nicht die Γ-Funktion, sondern kann direkt aus (3.14) schließen, daß $\frac{s}{2}\frac{d}{ds}\log\frac{\pi s}{\sin \pi s} = \sum_{k=1}^{\infty} \zeta(2k)s^{2k}$ ist). Damit ist der Satz vollständig bewiesen.

Die Tatsache, daß die Werte von $\zeta(2n)$ und $\zeta(1-2n)$ dieselben Bernoulli-Zahlen enthalten, läßt denken, daß es vielleicht überhaupt eine Beziehung zwischen $\zeta(s)$ und $\zeta(1-s)$ gibt. Wenn wir (5), (6) und (8) zusammenfassen als

$$\frac{2^{k-1}\,\pi^k}{(k-1)!}\,\zeta(1-k) = \begin{cases} (-1)^{k/2}\,\zeta(k) & k > 0,\ k \text{ gerade} \\ 0 & k > 1,\ k \text{ ungerade} \end{cases}$$

und bedenken, daß die Funktion $k \mapsto (k-1)!$ nach §3 die Interpolationsfunktion $\Gamma(k)$ hat, während

$$k \mapsto \begin{cases} (-1)^{k/2} & k \text{ gerade} \\ 0 & k \text{ ungerade} \end{cases}$$

auf natürliche Weise durch $\cos \frac{\pi k}{2}$ interpoliert wird, dann liegt es nahe, die Beziehung

$$(15) \qquad \frac{2^{s-1}\,\pi^s}{\Gamma(s)}\,\zeta(1-s) = \cos\frac{\pi s}{2}\,\zeta(s)$$

zu vermuten. Das ist die berühmte *Funktionalgleichung der ζ-Funktion*, die von Euler 1749 aufgrund analoger Überlegungen vermutet wurde (in "Remarques sur un beau rapport entre les series des puissances tant directes que réciproques", einer der Berliner Akademie vorgelegten Arbeit) und erst 1859 von Riemann in seiner bahnbrechenden Arbeit "Über die Anzahl der Primzahlen unter einer gegebenen Größe" bewiesen wurde. (Ein Beweis der Funktionalgleichung wird in Aufgabe 2 angedeutet.) Durch Anwendung der Funktionalgleichungen (3.11), (3.13) der Γ-Funktion kann sie auch symmetrischer geschrieben werden in der Form

$$(16) \qquad \pi^{-\frac{s}{2}}\,\Gamma(\tfrac{s}{2})\,\zeta(s) = \pi^{-\frac{1-s}{2}}\,\Gamma(\tfrac{1-s}{2})\,\zeta(1-s)\ .$$

Für $\sigma > 1$ ist die linke Seite von (16) von Null verschieden, da (wie in §2 schon bemerkt) die Produktdarstellung (2) impliziert, daß $\zeta(s)$ dort nicht verschwindet. Es folgt dann aus (16), daß $\zeta(s)$ in der Halbebene $\sigma < 0$ nur dort Nullstellen hat, wo $\Gamma(\frac{s}{2})$ Polstellen hat, d.h. nur einfache Nullstellen bei $s = -2, -4, -6, \ldots$. Die Funktion $\zeta(s)$ hat also

- eine einfache Polstelle bei $s = 1$,
- einfache Nullstellen bei $s = -2, -4, \ldots$ (die sog. "trivialen Wurzeln") ,
- und sonst Nullstellen höchstens in dem "kritischen Streifen" $0 < \sigma < 1$, wo sie in der Tat unendlich viele besitzt .

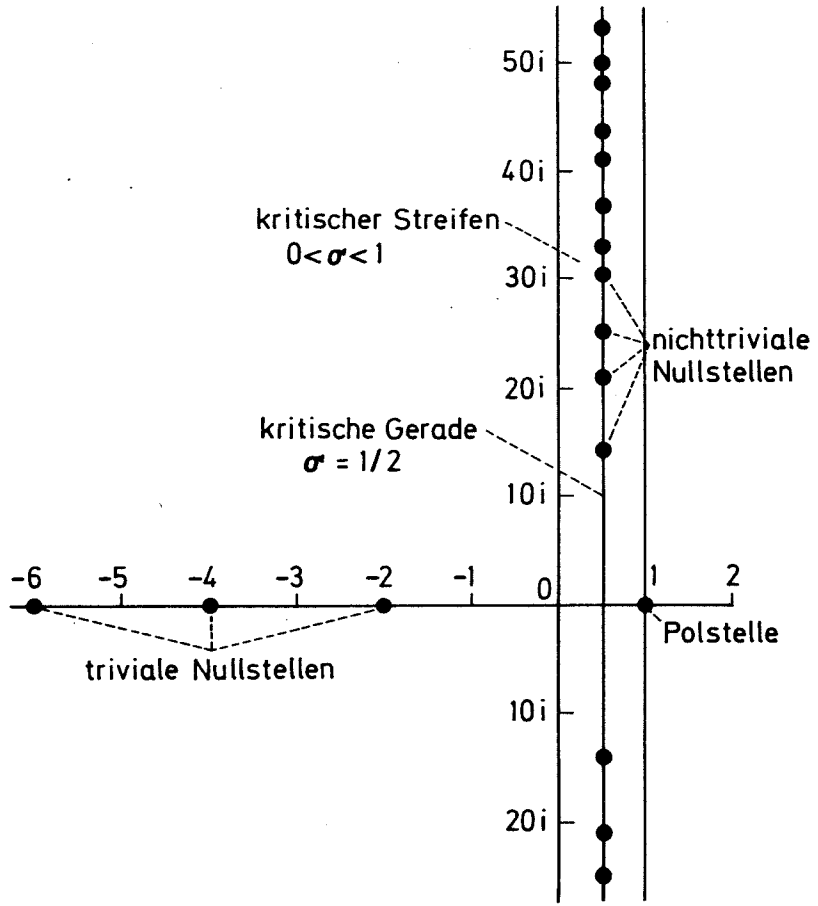
Die dem Absolutbetrag nach kleinsten Nullstellen in dem kritischen Streifen sind

$$\tfrac{1}{2} \pm 14{,}134725\ldots i\ ,$$

$$\tfrac{1}{2} \pm 21{,}022040\ldots i\ ,$$

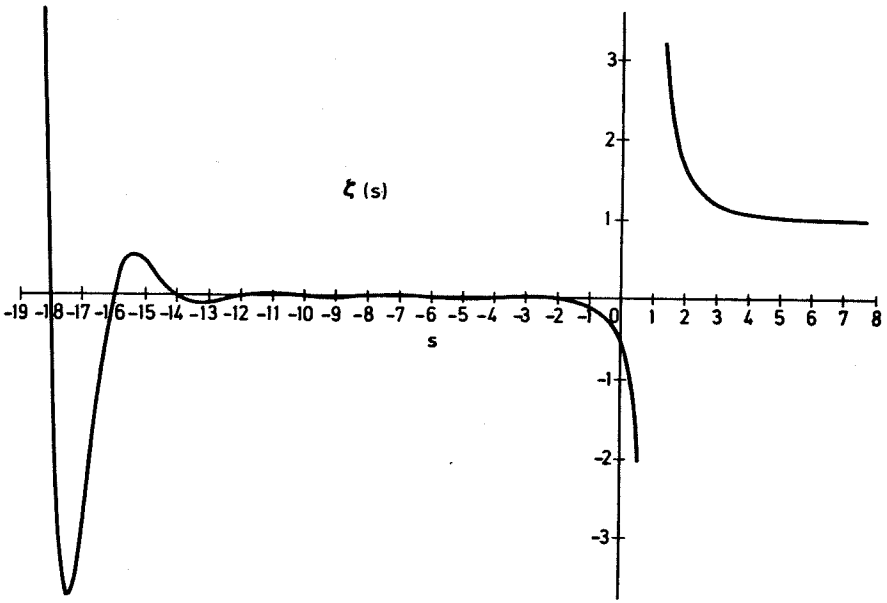
$$\tfrac{1}{2} \pm 25{,}010856\ldots i\ ,$$

$$\tfrac{1}{2} \pm 30{,}424878\ldots i\ .$$



Es ist naheliegend zu vermuten, daß *alle* Nullstellen in dem kritischen Streifen Realteil 1/2 haben. Das ist die berühmte, bis heute unbewiesene (und möglicherweise falsche) *Riemannsche Vermutung*. Man weiß, daß unendlich viele Nullstellen von $\zeta(s)$ auf der Geraden $\sigma = \frac{1}{2}$ liegen und auch, daß die ersten 150.000.000 Nullstellen in dem kritischen Streifen das tun.

Auf der reellen Achse sieht $\zeta(s)$ so aus:



Aufgaben:

1. Für die am Ende des §2 eingeführte Funktion

$$L(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \ldots$$

zeige man:

a) $L(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{t^{s-1}}{e^t + e^{-t}}\, dt \qquad (\sigma > 0)$,

b) $L(s)$ hat eine holomorphe Fortsetzung auf ganz $\mathbb{C}$.

c) $L(-n) = \frac{1}{2} E_n \qquad (n = 0, 1, 2, \ldots)$,

wobei E_n die durch

$$\frac{1}{\cos x} = \sum_{n=0}^{\infty} \frac{E_n}{n!} x^n$$

definierten *Eulerschen Zahlen* sind ($E_0 = 1$, $E_2 = -1$, $E_4 = 5$, $E_6 = -61, \ldots$, $E_1 = E_3 = E_5 = \ldots = 0$).

d) $L(2n+1) = \frac{(-1)^n E_{2n}}{2^{2n+2}(2n)!} \pi^{2n+1} \qquad (n = 0, 1, 2, \ldots)$.

2. Man beweise die Funktionalgleichung (15), indem man folgende Schritte durchführt:

a) Ausgehend von (3) zeige man für $\sigma > 1$

$$\Gamma(s)\,\zeta(s) = \int_0^1 \left(\frac{1}{e^x-1} - \frac{1}{x}\right) x^{s-1}\,dx + \frac{1}{s-1} + \int_1^\infty \frac{x^{s-1}\,dx}{e^x-1} ;$$

diese Gleichung gilt für $\sigma > 0$ wegen analytischer Fortsetzung und läßt sich für $0 < \sigma < 1$ schreiben als

$$\Gamma(s)\,\zeta(s) = \int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) x^{s-1}\,dx .$$

b) Ausgehend von a) zeige man für $0 < \sigma < 1$

$$\Gamma(s)\,\zeta(s) = \int_0^1 \left(\frac{1}{e^x-1} - \frac{1}{x} + \frac{1}{2}\right) x^{s-1}\,dx - \frac{1}{2s} + \int_1^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) x^{s-1}\,dx ,$$

was wiederum für $-1 < \sigma < 1$ wegen analytischer Fortsetzung gelten muß und für $-1 < \sigma < 0$ die Formel

$$\Gamma(s)\,\zeta(s) = \int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x} + \frac{1}{2}\right) x^{s-1}\,dx$$

liefert.

c) Man schließe aus (3.14), daß

$$\frac{\pi s}{\tan \pi s} - 1 = s\,\frac{d}{ds} \log \frac{\sin \pi s}{\pi s} = -\sum_{n=1}^\infty \frac{2s^2}{n^2-s^2}$$

gilt, und setze $s = \frac{ix}{2\pi}$, um

$$\frac{1}{e^x-1} - \frac{1}{x} + \frac{1}{2} = \frac{1}{x}\left(\frac{ix/2}{\tan ix/2} - 1\right) = \sum_{n=1}^\infty \frac{2x}{x^2+4n^2\pi^2}$$

zu erhalten.

d) Man setze c) in b) ein, um (nach einer wegen absoluter Konvergenz zulässigen Vertauschung von Integral und Summation) die Formel

$$\Gamma(s)\,\zeta(s) = 2 \sum_{n=1}^\infty (2\pi n)^{s-1} \int_0^\infty \frac{t^s\,dt}{t^2+1} = \frac{2^{s-1}\,\pi^s}{\cos \frac{\pi s}{2}}\,\zeta(1-s)$$

für $-1 < \sigma < 0$ zu beweisen; nach analytischer Fortsetzung ist die Funktionalgleichung dann für alle s bewiesen.

use binomial expansion of $\left(1-\frac{1}{m}\right)^{1-s}$ $m=2,3,4,\ldots$

3. Man beweise für $\sigma > 1$ die Beziehung

$$\zeta(s) = \frac{s}{s-1} - \frac{s}{2!}[\zeta(s+1) - 1] - \frac{s(s+1)}{3!}[\zeta(s+2) - 1] - \ldots ,$$

indem man $\zeta(s) = \sum n^{-s}$ einsetzt und die Summationen vertauscht; man benutze diese Formel, um zu zeigen, daß $\zeta(s) - \frac{s}{s-1}$ sich holomorph in ganz $\mathbb{C}$ fortsetzen läßt.

Show by induction that it's holomorphic for $\sigma > 1-n$

4. Man zeige, daß

$$(17) \qquad \zeta(s) = \frac{1}{s-1} + \gamma + O(s-1) \qquad (s \to 1)$$

gilt, wo γ die Eulersche Konstante ist.

Show that $\sum_{n=1}^\infty \left(\frac{1}{n^s} - \int_n^{n+1} \frac{dt}{t^s}\right)$ is continuous at $s=1$

§5 Charaktere

Die wichtigsten Dirichletschen Reihen (neben der Zetafunktion) sind die "L-Reihen", die ebenfalls von Dirichlet eingeführt wurden und von ihm benutzt wurden, um

a) die Existenz unendlich vieler Primzahlen in jeder arithmetischen Folge $\{Nk+a\}_{k\in\mathbb{Z}}$ mit $(N,a) = 1$ zu beweisen, und

b) eine Formel anzugeben für die Anzahl der Äquivalenzklassen von binären quadratischen Formen mit gegebener Diskriminante.

Die L-Reihen sind Funktionen, die gewissen Charakteren zugeordnet sind, und bevor wir in §§ 6 - 8 eine Beschreibung von Dirichlets Ergebnissen geben können, müssen wir diese Charaktere etwas studieren.

Ein *Charakter* auf einer endlichen Gruppe G ist ein Homomorphismus

$$\chi : G \to \mathbb{C}^* ,$$

wo $\mathbb{C}^*$ die Gruppe der von Null verschiedenen komplexen Zahlen ist (mit der Multiplikation als Gruppenoperation). Falls χ und χ' zwei Charaktere auf G sind, können wir das *Produkt* $\chi\chi'$ und das *Inverse* χ^{-1} durch

$$\chi\chi'(g) = \chi(g)\,\chi'(g) , \quad \chi^{-1}(g) = \chi(g)^{-1} \qquad (\forall g \in G)$$

definieren. Somit bilden die Charaktere auf G eine Gruppe, die wir mit $\hat{G}$ bezeichnen.

SATZ 1: *Sei* G *eine endliche abelsche Gruppe. Dann ist* $\hat{G}$ *zu* G *isomorph. Insbesondere ist* $|\hat{G}| = |G|$.

Beweis: Bekanntlich ist G eine direkte Summe von endlichen zyklischen Gruppen, also hat G Erzeugende $g_1, \ldots, g_k$ der Ordnungen $n_1, \ldots, n_k$ und jedes Element $g \in G$ läßt sich in der Gestalt $g = g_1^{r_1} \ldots g_k^{r_k}$ schreiben mit $r_1, \ldots, r_k \in \mathbb{Z}$. Ist χ ein Charakter auf G und $\chi(g_i) = \xi_i$ $(i = 1, \ldots, k)$, so ist

$$\xi_i^{n_i} = \chi(g_i)^{n_i} = \chi(g_i^{n_i}) = \chi(e) = 1$$

und

$$\chi(g_1^{r_1} \ldots g_k^{r_k}) = \chi(g_1)^{r_1} \ldots \chi(g_k)^{r_k} = \xi_1^{r_1} \ldots \xi_k^{r_k}, \tag{1}$$

d.h. die ξ_i sind n_i-te Einheitswurzeln und χ ist durch die ξ_i bestimmt. Umgekehrt, wenn $\xi_1, \ldots, \xi_k \in \mathbb{C}^*$ mit $\xi_i^{n_i} = 1$ $(i = 1, \ldots, k)$ beliebig gewählt werden, so definiert (1) einen Charakter. Es gibt also eine bijektive Korrespondenz zwischen Charakteren χ und k-Tupeln $(\xi_1, \ldots, \xi_k)$ mit $\xi_i^{n_i} = 1$, wobei das Produkt von Charakteren dem Produkt der ξ_i entspricht. Somit ist

$$\hat{G} \cong \{(\xi_1, \ldots, \xi_k) \in \mathbb{C}^k \mid \xi_1^{n_1} = \ldots = \xi_k^{n_k} = 1\}$$

$$\cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \cong G .$$

Bemerkung: Für G endlich ist $\chi(g)$ für jedes $g \in G$ eine Einheitswurzel, also vom Absolutbetrag 1, und somit ist der durch

$$\bar{\chi}(g) = \overline{\chi(g)} \qquad (\forall g \in G)$$

erklärte zu χ konjugierte Charakter mit dem oben definierten inversen Charakter identisch.

Definition: Ein *Dirichletscher Charakter modulo* N (N eine natürliche Zahl) ist ein Charakter auf der Gruppe

$$(\mathbb{Z}/N\mathbb{Z})^\times = \{n \pmod N \mid (n,N) = 1\} .$$

Wenn χ ein solcher Charakter ist, definieren wir eine (ebenfalls mit χ bezeichnete) Funktion $\chi: \mathbb{Z} \to \mathbb{C}$ durch

$$\chi(n) = \begin{cases} \chi(n \pmod N), & \text{falls } (n,N) = 1 \\ 0, & \text{falls } (n,N) > 1 . \end{cases}$$

Auch diese Funktion χ wird als Dirichletscher Charakter bezeichnet.

Ein Dirichletscher Charakter (mod N) kann auch beschrieben werden als eine Funktion $\chi: \mathbb{Z} \to \mathbb{C}$ mit den Eigenschaften

(1) $\chi(n) = 0 \iff (n,N) > 1$

(2) χ ist streng multiplikativ: $\chi(mn) = \chi(m)\,\chi(n)$ für alle $m,n \in \mathbb{Z}$

(3) $\chi(n)$ hängt nur von $n \pmod N$ ab.

Nach Satz 1 gibt es $\phi(N)$ Dirichletsche Charaktere, wo

$$\phi(N) = |(\mathbb{Z}/N\mathbb{Z})^\times| = \#\{n \pmod N \mid (n,N) = 1\}$$

$$= N \prod_{p \mid N} \left(1 - \frac{1}{p}\right)$$

die Eulersche Funktion von N bezeichnet.

Beispiele: a) Für jedes N ist der *Hauptcharakter* $\chi_0 \pmod N$ durch

$$\chi_0(n) = \begin{cases} 1 & (n,N) = 1 \\ 0 & (n,N) > 1 \end{cases}$$

erklärt (das entspricht der Eins von $\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$).

b) Für $N = 2$ ist $\phi(N) = 1$, also χ_0 der einzige Charakter. Für $N = 3, 4, 6$ ist $\phi(N)$ jeweils gleich 2, und es gibt neben dem Hauptcharakter die Charaktere

n	0	1	2	3	4	5	6	...
$\varepsilon_3(n)$	0	1	-1	0	1	-1	0	...

n	0	1	2	3	4	5	6	7	8	...
$\varepsilon_4(n)$	0	1	0	-1	0	1	0	-1	0	...

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$\varepsilon_6(n)$	0	1	0	0	0	-1	0	1	0	0	0	-1	0	1	...

Für $N = 5$ gibt es neben χ_0 drei Charaktere:

$n \pmod 5$	0	1	2	3	4
$\chi(n)$	0	1	i	$-i$	-1
	0	1	-1	-1	1
	0	1	$-i$	$+i$	-1

c) Für jede Primzahl p ist das *Legendresche Symbol*

$$(2)\qquad \left(\frac{n}{p}\right) = \begin{cases} 0, & \text{falls } p \mid n \\ 1, & \text{falls } p \nmid n,\ n \equiv x^2 \pmod p \text{ für ein } x \in \mathbb{Z} \\ -1, & \text{sonst} \end{cases}$$

ein Dirichletscher Charakter (mod p).

Wir haben zwei einfache, aber sehr nützliche Sätze:

SATZ 2: *Sei* χ *ein Dirichletscher Charakter modulo* N. *Dann ist*

$$(3)\qquad \sum_{n \pmod N} \chi(n) = \begin{cases} \phi(N), & \text{falls } \chi = \chi_0 \\ 0, & \text{falls } \chi \neq \chi_0 . \end{cases}$$

(Hier bezeichnet $\sum_{n \pmod N}$ eine Summe über ein beliebiges Vertretersystem von $\mathbb{Z}/N\mathbb{Z}$, z.B. $\sum_{n=1}^{N}$.)

KOROLLAR: *Seien* χ_1, χ_2 *zwei Dirichletsche Charaktere* (mod N). *Dann ist*

$$(4)\qquad \frac{1}{\phi(N)} \sum_{n \pmod N} \chi_1(n)\,\bar{\chi}_2(n) = \begin{cases} 1, & \text{falls } \chi_1 = \chi_2 \\ 0, & \text{falls } \chi_1 \neq \chi_2 . \end{cases}$$

Beweis: Für $\chi = \chi_0$ ist (3) trivial. Sei $\chi \neq \chi_0$ und $m \in \mathbb{Z}$ so gewählt, daß $(m,N) = 1$ und $\chi(m) \neq 1$ ist. Dann ist

$$(1 - \chi(m)) \sum_{n \pmod N} \chi(n) = \sum_{n \pmod N} [\chi(n) - \chi(mn)]$$

$$= \sum_{n \pmod N} \chi(n) - \sum_{n \pmod N} \chi(n) = 0$$

(da mit n auch mn ein Vertretersystem von $\mathbb{Z}$ (mod N) durchläuft), also, da $\chi(m) \neq 1$,

$$\sum_{n \pmod N} \chi(n) = 0 .$$

Das Korollar folgt, indem man $\chi_1 \bar{\chi}_2$ für χ wählt.

SATZ 3: *Sei* $n \in \mathbb{Z}$. *Dann ist*

$$(5)\qquad \sum_{\chi} \chi(n) = \begin{cases} \phi(N), & \text{falls } n \equiv 1 \pmod N \\ 0, & \text{falls } n \not\equiv 1 \pmod N , \end{cases}$$

wobei über alle Dirichletschen Charaktere (mod N) *summiert wird.*

Korollar: *Seien* $a,b \in \mathbb{Z}$, $(b,N) = 1$. *Dann ist*

$$(6)\qquad \frac{1}{\phi(N)} \sum_{\chi} \chi(a)\,\bar{\chi}(b) = \begin{cases} 1, & \text{falls } a \equiv b \pmod N \\ 0, & \text{falls } a \not\equiv b \pmod N . \end{cases}$$

Beweis: Für $n \equiv 1 \pmod N$ ist (5) trivial, da es $\phi(N)$ Charaktere gibt und für alle χ $\chi(n) = 1$ gilt. Für $(n,N) > 1$ gilt (5) auch, da dann $\chi(n)$ für alle χ verschwindet. Sei $n \not\equiv 1 \pmod N$, $(n,N) = 1$, und χ_1 ein Dirichletscher Charakter (mod N) mit $\chi_1(n) \neq 1$. Ein solcher existiert wegen Satz 1, denn die Charaktere χ mit $\chi(n) = 1$ sind Charaktere auf der Quotientengruppe $(\mathbb{Z}/N\mathbb{Z})^\times/\langle n\rangle$, und deren Anzahl ist demnach kleiner als $|(\mathbb{Z}/N\mathbb{Z})^\times|$. Dann ist

$$(1 - \chi_1(n)) \sum_{\chi} \chi(n) = \sum_{\chi} [\chi(n) - \chi\chi_1(n)]$$

$$= \sum_{\chi} \chi(n) - \sum_{\chi} \chi(n) = 0 ,$$

da $\chi\chi_1$ mit χ über die Gruppe $(\mathbb{Z}/N\mathbb{Z})^\times$ läuft. Da $1 - \chi_1(n) \neq 0$, folgt hieraus, daß die Summe verschwindet. Das Korollar folgt, indem man n mit $nb \equiv a \pmod N$ wählt.

Sei N_1 ein von N verschiedener Teiler von N und χ_1 ein Charakter (mod N_1). Dann definiert die Zusammensetzung

$$(7)\qquad (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/N_1\mathbb{Z})^\times \xrightarrow{\chi_1} \mathbb{C}^* ,$$

wobei der erste Pfeil die Reduktion (mod N_1) ist, einen Charakter χ (mod N). Wir sagen, daß χ von χ_1 *induziert* wird und nennen einen Charakter χ, der so entsteht, *imprimitiv*; ein Charakter, der nicht auf diese Weise erhalten werden kann, heißt *primitiv* (oder *eigentlich*). Z.B. ist der Hauptcharakter χ_0 (mod N) für $N > 1$ nie primitiv, weil er von dem trivialen Charakter (mod 1) induziert wird. Für jeden Dirichletschen Charakter χ (mod N) gibt es eine kleinste Zahl N_1, so daß χ dargestellt werden kann als die Zusammensetzung (7) mit geeignetem Charakter χ_1 (mod N_1), und dies ist die einzige Darstellung (7) von χ, für die χ_1 primitiv ist. Diese Zahl N_1 mit der Eigenschaft, daß χ von einem primitiven Charakter (mod N_1) induziert wird, nennt man den *Führer* von χ.

Wir werden uns vor allem für *reelle* Charaktere ($\chi = \bar{\chi}$) interessieren, d.h. solche, die nur die Werte 1, 0, -1 annehmen. Wir beweisen einen Satz, in dem alle primitiven reellen Charaktere angegeben

werden.

Definition: Eine *Grundzahl* ist eine ganze Zahl D mit

$$D \equiv 1 \pmod 4,\ D \text{ quadratfrei},$$

oder

$$D \equiv 0 \pmod 4,\ \tfrac{D}{4} \text{ quadratfrei},\ \tfrac{D}{4} \equiv 2 \text{ oder } 3 \pmod 4 .$$

(Solche Zahlen nennt man auch *Fundamentaldiskriminanten*). Für eine Grundzahl D definieren wir eine Funktion $\chi_D\colon \mathbb{N} \to \mathbb{Z}$ durch

$$\chi_D(p) = \left(\frac{D}{p}\right) \qquad (p \text{ ungerade Primzahl}) \tag{8a}$$

$$\chi_D(2) = \begin{cases} 0, & \text{falls } D \equiv 0 \pmod 4, \\ 1, & \text{falls } D \equiv 1 \pmod 8, \\ -1, & \text{falls } D \equiv 5 \pmod 8, \end{cases} \tag{8b}$$

$$\chi_D(p_1^{n_1}\cdots p_k^{n_k}) = \chi_D(p_1)^{n_1}\cdots\chi_D(p_k)^{n_k} . \tag{8c}$$

Insbesondere ist χ_1 der triviale Charakter.

SATZ 4: *Die Funktion* $n \mapsto \chi_D(n)$ *(D eine Grundzahl) ist periodisch* (mod $|D|$) *und definiert einen primitiven Dirichletschen Charakter modulo* $|D|$ (ebenfalls mit χ_D bezeichnet) *mit*

$$\chi_D(-1) = \begin{cases} 1, & \textit{falls } D > 0, \\ -1, & \textit{falls } D < 0. \end{cases} \tag{9}$$

Jeder primitive reelle Dirichletsche Charakter ist einer der Charaktere χ_D.

Beweis: Wegen Satz 1 ist jeder Dirichletsche Charakter χ (mod N), mit $N = p_1^{r_1}\cdots p_k^{r_k}$, gleich einem Produkt $\chi_1\cdots\chi_k$, wo χ_i von einem Charakter (mod $p_i^{r_i}$) induziert wird:

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \xrightarrow{\ \cong\ } & (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times\cdots\times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})^\times \\ & {\scriptstyle\chi} \searrow \quad \swarrow {\scriptstyle\chi_1\times\cdots\times\chi_k} & \\ & \mathbb{C}^* & \end{array}$$

Aus dem Diagramm geht hervor, daß χ dann und nur dann primitiv ist, wenn jeder χ_i das ist. Für die Klassifizierung solcher Charaktere genügt es also, sich auf Primzahlpotenzführer $N = p^r$ zu beschränken.

Fall i: p ungerade. In diesem Fall ist bekanntlich $(\mathbb{Z}/p^r\mathbb{Z})^\times$ zyklisch (siehe Aufgabe 1). Sei x ein erzeugendes Element ("primitive Wurzel modulo p^r"). Ist χ reell und $\neq \chi_0$, so ist sicherlich $\chi(x) = -1$; es gibt also höchstens einen solchen Charakter. Andererseits ist $n \mapsto \left(\frac{n}{p}\right)$ ein von χ_0 verschiedener reeller Charakter (mod p^r). Da dieser Charakter den Führer p hat, erhalten wir:

> Für p ungerade gibt es genau einen reellen primitiven Charakter χ (mod p). Dieser ist durch $\chi(n) = \left(\frac{n}{p}\right)$ gegeben. Es gibt keinen reellen primitiven Charakter modulo p^r mit $r > 1$.

Fall ii: $p = 2$. Für $r = 1$ ist $(\mathbb{Z}/2^r\mathbb{Z})^\times$ trivial, also $\chi = \chi_0$ der einzige Charakter. Für $r = 2$ ist $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$, also ε_4 (Beispiel b) oben) der einzige von χ_0 verschiedene Charakter; er ist auch primitiv. Für $r = 3$ ist $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ und es gibt genau die zwei durch

n (mod 8)	0	1	2	3	4	5	6	7
$\varepsilon_8'(n)$	0	1	0	−1	0	−1	0	1
$\varepsilon_8''(n)$	0	1	0	1	0	−1	0	−1

definierten primitiven reellen Charaktere ε_8' und ε_8'' (es muß $\chi(3) = \alpha$, $\chi(5) = \beta$, $\chi(7) = \chi(3\times 5) = \alpha\beta$ mit $\alpha, \beta = \pm 1$ sein, und von den 4 Möglichkeiten sind zwei die imprimitiven Charaktere χ_0 und ε_4). Für $r > 3$ ist bekanntlich jede zu 1 (mod 8) kongruente Zahl modulo 2^r zu einem Quadrat kongruent (siehe Aufgabe 1), also gilt für χ reell

$$n \equiv 1 \pmod 8 \Rightarrow n \equiv x^2 \pmod{2^r}$$

$$\Rightarrow \chi(n) = \chi(x^2) = \chi(x)^2 = (\pm 1)^2 = 1 ,$$

und χ kann nicht primitiv sein. Das zeigt:

> Es gibt genau einen primitiven reellen Charakter (ε_4) modulo 4 und genau zwei (ε_8' und ε_8'') modulo 8; für $r \neq 2, 3$ gibt es keinen reellen primitiven Charakter (mod 2^r).

Wir haben jetzt alle reellen primitiven Charaktere gefunden: das sind die Produkte von Legendre Symbolen $\left(\frac{n}{p}\right)$ für verschiedene ungerade Primzahlen p sowie die Produkte von solchen Charakteren mit ε_4, ε_8' oder ε_8''; insbesondere sind die einzigen Zahlen N, für die

es überhaupt reelle primitive Charaktere gibt, von der Gestalt 1 mal, 4 mal oder 8 mal eine ungerade quadratfreie Zahl. Wir wenden jetzt das quadratische Reziprozitätsgesetz bzw. die sogenannten 1. und 2. Ergänzungssätze an, um folgende Identitäten zu erhalten:

$$\left(\frac{n}{p}\right) = \chi_{p'}(n) \quad \text{für} \quad p \neq 2,\ p \text{ prim, wobei } p' = (-1)^{\frac{p-1}{2}} p ,$$

$$\varepsilon_4(n) = \left(\frac{-4}{n}\right) = \chi_{-4}(n) ,$$

$$\varepsilon_8'(n) = \left(\frac{8}{n}\right) = \chi_8(n) ,$$

$$\varepsilon_8''(n) = \left(\frac{-8}{n}\right) = \chi_{-8}(n) .$$

Außerdem ist das Produkt zweier teilerfremder Grundzahlen D_1 und D_2 wieder eine Grundzahl und es gilt

$$\chi_{D_1 D_2} = \chi_{D_1}\chi_{D_2} \qquad ((D_1,D_2) = 1) . \tag{10}$$

Somit ist bewiesen, daß die reellen primitiven Charaktere genau die χ_D sind, für die D ein Produkt von teilerfremden Zahlen aus der Menge

$$-4,\ +8,\ -8,\ p\ (p\equiv 1 \pmod 4 \text{ prim}),\ -p\ (p\equiv 3 \pmod 4 \text{ prim}) \tag{11}$$

ist (die Zahlen aus (11) heißen *Primdiskriminanten*). Aber es ist leicht zu sehen, daß jede Grundzahl D ein solches Produkt ist, da D eine der Formen m, $-4m$, $8m$, $-8m$ hat mit m quadratfrei und $m \equiv 1 \pmod 4$, also $m = \prod_{p|m} p'$. Damit sind alle Aussagen des Satzes bewiesen bis auf (9), und auch diese Formel brauchen wir wegen (10) nur für eine Primdiskriminante D zu beweisen, was mit Hilfe des ersten Ergänzungssatzes leicht ist:

$$\chi_{-4}(-1) = \varepsilon_4(-1) = -1 = \operatorname{sign}(-4) ,$$

$$\chi_8(-1) = \varepsilon_8'(-1) = 1 = \operatorname{sign}(8) ,$$

$$\chi_{-8}(-1) = \varepsilon_8''(-1) = -1 = \operatorname{sign}(-8) ,$$

$$\chi_{p'}(-1) = \left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1 \pmod 4 \\ -1, & \text{falls } p \equiv 3 \pmod 4 \end{cases} = \operatorname{sign}(p') .$$

Aufgaben

1. Man beweise die in diesem Paragraphen benutzten Tatsachen

   a) $(\mathbb{Z}/p^r\mathbb{Z})^\times$ ist zyklisch $(p > 2$ prim, $r \geq 1)$,

   b) $n \equiv 1 \pmod 8 \Rightarrow n \equiv x^2 \pmod{2^r}$ $\quad (r \geq 3)$,

   jeweils durch Induktion über r (der Fall $r = 1$ der ersten Aussage ist Spezialfall eines bekannten Satzes über die Einheitengruppe eines endlichen Körpers), indem man das Element, das für p^r eine Lösung liefert, modulo p^{r+1} (bzw. 2^{r-1} für $p = 2$) abändert, um eine Lösung $(\bmod p^{r+1})$ zu erhalten.

2. Man beweise mit Hilfe von Aufgabe 1 folgende Isomorphismen

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z} \qquad (p \text{ ungerade})$$

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{r-2}\mathbb{Z} \qquad (r \geq 2)$$

   und benutze sie, um *alle* primitiven Dirichletschen Charaktere zu bestimmen. Wieviele gibt es modulo N?

3. Man zeige durch ein Beispiel, daß für einen Dirichletschen Charakter $\chi \pmod N$ der Definitionsmodul (also die Zahl N), die Periode (also die kleinste Zahl r mit $\chi(n+r) = \chi(n)$ für alle n) und der Führer verschieden sein können. Welche Beziehung gibt es zwischen diesen drei Zahlen?

§6 L-Reihen

Sei χ ein Dirichletscher Charakter $(\bmod N)$. Die χ zugeordnete *Dirichletsche L-Reihe* ist die Reihe

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} . \tag{1}$$

Wegen $|\chi(n)| \leq 1$ ist diese Reihe für $\sigma > 1$ absolut konvergent. Wegen der Multiplikativität von χ hat sie nach §2 eine Eulersche Produktdarstellung

$$L(s,\chi) = \prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \ldots\right) ;$$

wegen der strengen Multiplikativität $\chi(p^r) = \chi(p)^r$ ist sogar

$$L(s,\chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \qquad (\sigma > 1) \; . \tag{2}$$

Für den Hauptcharakter χ_0 ist nach (2)

$$\begin{aligned} L(s,\chi_0) &= \prod_p (1 - \chi_0(p)p^{-s})^{-1} \\ &= \prod_{p \nmid N} (1 - p^{-s})^{-1} \\ &= \prod_{p \mid N} (1 - p^{-s}) \cdot \prod_{\text{alle } p} (1 - p^{-s})^{-1} \\ &= \prod_{p \mid N} (1 - p^{-s}) \cdot \zeta(s) \; ; \end{aligned} \tag{3}$$

also ist die L-Reihe in diesem Fall bis auf einen einfachen multiplikativen Faktor mit der Riemannschen Zetafunktion identisch. Insbesondere läßt sie sich auf die ganze komplexe Ebene meromorph fortsetzen mit einem einfachen Pol mit Residuum $\prod_{p \mid N} (1 - p^{-1}) = \frac{\phi(N)}{N}$ an der Stelle $s = 1$ als einziger Singularität.

Für $\chi \neq \chi_0$ ist für $x \to \infty$

$$\begin{aligned} \Big| \sum_{n=1}^{x} \chi(n) \Big| &= \Big| \sum_{n=1}^{N[x/N]} \chi(n) + \sum_{n=N\cdot[\frac{x}{N}]+1}^{x} \chi(n) \Big| \\ &= \Big| [\tfrac{x}{N}] \sum_{n \,(\mathrm{mod}\, N)} \chi(n) + \sum_{n=N[\frac{x}{N}]+1}^{x} \chi(n) \Big| \\ &= \Big| \sum_{n=N[\frac{x}{N}]+1}^{x} \chi(n) \Big| \leq |x - N[\tfrac{x}{N}]| \leq N = O(1) \end{aligned}$$

wegen Satz 2, §5; deswegen ist nach Satz 2 von §1 die Konvergenzabszisse von $L(s,\chi)$ kleiner oder gleich 0 (offensichtlich sogar gleich 0); insbesondere definiert (1) eine in $\sigma > 0$ holomorphe Funktion. In der Tat läßt sich diese Funktion auf ganz $\mathbb{C}$ holomorph fortsetzen und genügt einer Funktionalgleichung analog zu der von $\zeta(s)$ (s. §7).

Der wichtigste Satz über L-Reihen ist die Tatsache, daß der Wert von $L(1,\chi)$ (der nach dem eben Gesagten definiert ist) stets von Null verschieden ist; hieraus kann man leicht die Existenz unendlich vieler Primzahlen in arithmetischen Folgen schließen. Wir beweisen jetzt diese beiden Ergebnisse.

SATZ: *Sei χ ein von χ_0 verschiedener Dirichletscher Charakter. Dann ist*

$$L(1,\chi) \neq 0 \; . \tag{4}$$

Beweis: Sei

$$F(s) = \prod_{\chi} L(s,\chi) \; , \tag{5}$$

wo χ über sämtliche Dirichletschen Charaktere (mod N) läuft. Dann ist für $\sigma > 1$ nach (2)

$$\begin{aligned} \log F(s) &= \sum_{\chi} \sum_{p} \log (1 - \chi(p)p^{-s})^{-1} \\ &= \sum_{\chi} \sum_{p} \sum_{r=1}^{\infty} \frac{1}{r} \frac{\chi(p)^r}{p^{rs}} \\ &= \phi(N) \sum_{\substack{p \\ p^r \equiv 1 \,(\mathrm{mod}\, N)}} \sum_{r \geq 1} \frac{1}{rp^{rs}} \end{aligned} \tag{6}$$

(die letzte Gleichung folgt aus Satz 3, §5); insbesondere ist $\log F(s) \geq 0$ für s reell und > 1, und somit

$$\lim_{\substack{s \to 1 \\ s \text{ reell}}} F(s) \geq 1 \; . \tag{7}$$

Das Produkt (5) enthält nur einen Faktor, der an der Stelle $s = 1$ einen Pol hat, nämlich $L(s,\chi_0)$, und dieser Pol ist nach (3) einfach. Wenn $L(1,\chi) = 0$ wäre für *zwei oder mehr* Charaktere $\chi \neq \chi_0$, müßte demnach $F(s)$ an der Stelle $s = 1$ holomorph sein und den Wert 0 haben, was offensichtlich (7) widerspricht. Es kann also *höchstens einen* Charakter $\chi \neq \chi_0$ mit $L(1,\chi) = 0$ geben. Da mit $L(1,\chi) = 0$ auch $L(1,\bar{\chi}) = \overline{L(1,\chi)} = 0$ wäre, ist dieser Charakter χ (falls er existiert) gleich $\bar{\chi}$, also *reell*. Wir können uns also für den Beweis des Satzes auf reelle Charaktere beschränken.

Sei also χ reell mit $L(1,\chi) = 0$, und sei

$$\Phi(s) = \frac{L(s,\chi)\, L(s,\chi_0)}{L(2s,\chi_0)} \; . \tag{8}$$

Diese Funktion ist für $\sigma > \frac{1}{2}$ holomorph, da der Pol von $L(s,\chi_0)$ bei $s = 1$ durch die Nullstelle von $L(s,\chi)$ dort aufgehoben wird, während der Nenner $L(2s,\chi_0)$ wegen (3) für $\sigma > \frac{1}{2}$ von Null verschieden ist. Für $\sigma > 1$ ist

$$\begin{aligned} \Phi(s) &= \prod_p \frac{1 - \chi_0(p)p^{-2s}}{(1 - \chi(p)p^{-s})(1 - \chi_0(p)p^{-s})} \\ &= \prod_{p \nmid N} \frac{1 - p^{-2s}}{(1 - \chi(p)p^{-s})(1 - p^{-s})} \end{aligned}$$

$$= \prod_{p \nmid N} \frac{1 + p^{-s}}{1 - \chi(p)p^{-s}}$$

$$= \prod_{\chi(p)=1} \frac{1 + p^{-s}}{1 - p^{-s}}$$

(da $\chi(p) = \pm 1$ für $p \nmid N$ ist), also

$$\Phi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad (\sigma > 1) \qquad \text{mit } a_n \geq 0 .$$

(Um dies zu erreichen, brauchten wir den Faktor $1 + p^{-s} = \frac{1 - p^{-2s}}{1 - p^{-s}}$ in dem Euler-Produkt von Φ; das ist der Grund für die Wahl der Funktion (8).) Da $\Phi(s)$ in $\sigma > \frac{1}{2}$ holomorph ist, ist für $|s-2| < \frac{3}{2}$

$$\Phi(s) = \sum_{k=0}^{\infty} \frac{(s-2)^k}{k!} \Phi^{(k)}(2) = \sum_{k=0}^{\infty} \frac{(2-s)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n (\log n)^k}{n^2} ,$$

und wegen $a_n \geq 0$ stellt die rechts stehende Doppelsumme für s reell, $\frac{1}{2} < s < 2$, eine monoton fallende Funktion dar, also ist

$$\Phi(s) \geq \Phi(2) \geq 1 \qquad (s \text{ reell}, \ \tfrac{1}{2} < s < 2) .$$

Aber nach (8) ist

$$\lim_{s \to \frac{1}{2}} \Phi(s) = \frac{L(\frac{1}{2},\chi)\ L(\frac{1}{2},\chi_0)}{\lim\limits_{s \to \frac{1}{2}} L(2s,\chi_0)} = 0 ,$$

da $L(2s,\chi_0)$ nach (3) an der Stelle $s = \frac{1}{2}$ einen Pol hat. Dieser Widerspruch beweist den Satz.

Es ist dem Leser vielleicht aufgefallen, daß dieser Beweis zu dem Beweis des Landauschen Satzes (Satz 4, §1) sehr analog ist, und in der Tat kann man (4) auch durch direkte Anwendung jenes Satzes beweisen. Sei nämlich χ reell, und

$$\psi(s) = L(s,\chi)\ \zeta(s) = \sum_{n=1}^{\infty} \frac{\rho(n)}{n^s} , \tag{9}$$

$$\rho(n) = \sum_{d \mid n} \chi(d) . \tag{10}$$

Dann ist

$$\psi(s) = \prod_{p\ (1 - \chi(p)p^{-s})(1 - p^{-s})}^{1}$$

$$= \prod_{\chi(p)=1} \frac{1}{(1 - p^{-s})^2} \cdot \prod_{\chi(p)=0} \frac{1}{1 - p^{-s}} \cdot \prod_{\chi(p)=-1} \frac{1}{1 - p^{-2s}} \tag{11}$$

$$= \prod_{\chi(p)=1} \left(1 + \frac{2}{p^s} + \frac{3}{p^{2s}} + \dots\right) \cdot \prod_{\chi(p)=0} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

$$\cdot \prod_{\chi(p)=-1} \left(1 + \frac{1}{p^{2s}} + \frac{1}{p^{4s}} + \dots\right) ,$$

also für alle n

$$\rho(n) \geq 0 , \qquad \rho(n^2) \geq 1 \tag{12}$$

(die Beziehungen (11) und (12) werden später eine Bedeutung erhalten, indem $\psi(s)$ als Zetafunktion eines quadratischen Körpers und $\rho(n)$ als Anzahl der Ideale mit Norm n erkannt werden). Ist $L(1,\chi) = 0$, so hat $\psi(s)$ nach (9) keine Singularität in $\sigma > 0$; nach (12) und dem Landauschen Satz muß also die Reihe $\sum \rho(n)n^{-s}$ für $\sigma > 0$ konvergent sein, was im Widerspruch zu der aus (12) folgenden Beziehung

$$\sum_{n=1}^{\infty} \frac{\rho(n)}{n^{1/2}} \geq \sum_{n=1}^{\infty} \frac{\rho(n^2)}{n} \geq \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

steht. Damit ist unser Satz wieder bewiesen.

Man kann mit dem Landauschen Satz einen noch kürzeren Beweis angeben, und zwar einen, der die Reduktion auf den Fall eines reellen χ nicht braucht, sondern (4) simultan für alle $\chi \pmod N$ zeigt (wegen der Wichtigkeit des Satzes scheuen wir uns nicht, drei verschiedene Beweise anzugeben). Es folgt nämlich aus (6), daß die durch (5) definierte Funktion $F(s)$ für $\sigma > 1$ durch eine Dirichletsche Reihe mit positiven Koeffizienten gegeben wird. Gäbe es auch nur einen Charakter $\chi \neq \chi_0$ mit $L(1,\chi) = 0$, so wäre nach (5) die Funktion $F(s)$ an der Stelle $s = 1$ und deswegen in der ganzen Halbebene $\sigma > 0$ holomorph, also nach dem Landauschen Satz die entsprechende Dirichletsche Reihe für $\sigma > 0$ konvergent und damit auch die Reihe (6) in diesem Gebiet konvergent. Aber nach der Eulerschen Verallgemeinerung des kleinen Fermatschen Satzes ist (für s reell)

$$\sum_{\substack{p \\ p^r \equiv 1 \pmod N}} \sum_{r \geq 1} \frac{1}{rp^{rs}} \geq \phi(N) \sum_{p \nmid N} \sum_{\substack{r=1 \\ \phi(N) \mid r}}^{\infty} \frac{1}{rp^{rs}}$$

$$= \sum_{p \nmid N} \sum_{k=1}^{\infty} \frac{1}{kp^{ks\phi(N)}}$$

$$= \sum_{p \nmid N} \log \frac{1}{1 - p^{-s\phi(N)}}$$

$$= \log L(s\phi(N),\chi_0) ,$$

also für $s = \frac{1}{\phi(N)}$ sicherlich nicht konvergent.

Noch ein vierter Beweis dafür, daß (4) für reelle Charaktere gilt, wird aus einem Ergebnis von §8 folgen, das besagt, daß für solche χ der Wert von $L(1,\chi)$ zu einer (stets von 0 verschiedenen) *Klassenzahl* proportional ist; auf diesem Wege hat ursprünglich Dirichlet den Satz bewiesen.

KOROLLAR: *Sei* N *eine natürliche Zahl,* a *zu* N *teilerfremd. Dann enthält die arithmetische Folge* $\{Nk + a\}_{k\in\mathbb{N}}$ *unendlich viele Primzahlen; es ist sogar*

$$\sum_{\substack{p \text{ prim} \\ p\equiv a \pmod N}} \frac{1}{p} = \infty . \tag{13}$$

Beweis: Nach dem Korollar zu Satz 3, §5, ist für $\sigma > 1$

$$\begin{aligned}
\sum_{\substack{p \\ p^r\equiv a \pmod N}} \sum_{r\geq 1} \frac{1}{rp^{rs}} &= \sum_{p} \sum_{r\geq 1} \frac{1}{\phi(N)} \sum_{\chi} \bar\chi(a)\,\chi(p^r)\cdot\frac{1}{rp^{rs}} \\
&= \frac{1}{\phi(N)} \sum_{\chi} \bar\chi(a) \sum_{p} \sum_{r=1}^{\infty} \frac{\chi(p)^r}{rp^{rs}} \\
&= \frac{1}{\phi(N)} \sum_{\chi} \bar\chi(a)\,\log L(s,\chi) \\
&= \frac{1}{\phi(N)}\left[\log L(s,\chi_0) + \sum_{\chi\neq\chi_0} \bar\chi(a)\,\log L(s,\chi)\right],
\end{aligned} \tag{14}$$

wobei die Vertauschung wegen der absoluten Konvergenz erlaubt ist (hier bedeuten $\sum_p$ und $\sum_\chi$ wie üblich die über alle Primzahlen bzw. alle Dirichletschen Charaktere (mod N) erstreckten Summationen). Da $\log L(s,\chi_0)$ für $s \to 1$ nach Unendlich strebt, aber $\log L(s,\chi)$ für $\chi \neq \chi_0$ wegen (4) beschränkt ist, folgt aus (14), daß die Summe auf der linken Seite für $s = 1$ divergiert. Aber

$$\sum_{\substack{p \\ p^r\equiv a \pmod N}} \sum_{r>1} \frac{1}{rp^r} \leq \sum_{p} \sum_{r=2}^{\infty} \frac{1}{rp^r}$$

$$\leq \sum_{p} \sum_{r=2}^{\infty} \frac{1}{2p^r} = \sum_{p} \frac{1}{2p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \frac{1}{2} ,$$

also muß die Summe der Termen mit $r = 1$ divergieren.

Aufgaben

1. Man beweise elementar die Existenz unendlich vieler Primzahlen der Gestalt $4n - 1$ bzw. $4n + 1$, indem man unter der Annahme, es gäbe nur endlich viele, die Zahlen

$$4 \prod_{p\equiv 3 \pmod 4} p - 1 \quad \text{bzw.} \quad 4 \prod_{p\equiv 1 \pmod 4} p^2 + 1$$

bildet und einen Widerspruch ableitet. Für welche anderen arithmetischen Folgen gibt es einen analogen Beweis?

2. Man zeige, daß für jeden Dirichletschen Charakter χ

$$\frac{1}{L(s,\chi)} = \sum_{n=1}^{\infty} \frac{\mu(n)\,\chi(n)}{n^s} \qquad (\sigma > 1)$$

ist, wobei $\mu(n)$ die in §2 eingeführte Möbiussche Funktion bezeichnet. Kann man aus dem Satz dieses Paragraphen schließen, daß die Reihe für $s = 1$ konvergiert?

§7 Werte von Dirichletschen Reihen, insbesondere von L-Reihen, an negativen ganzen Stellen

In §4 haben wir gesehen, daß die Riemannsche Zetafunktion $\zeta(s)$ für alle geraden Argumente $s > 1$ und für alle ganzzahligen Argumente $s < 1$ Werte annimmt, die man in geschlossener Gestalt angeben kann; für $s < 1$ sind diese Werte stets rational und in der Hälfte der Fälle gleich Null. Ähnliche Eigenschaften gelten für alle Dirichletschen L-Reihen. Da diese Reihen Funktionalgleichungen erfüllen, braucht man die Werte nur für $s \geq 1$ oder für $s \leq 0$ zu berechnen. Überraschenderweise stellt sich heraus, daß die Werte an den negativen ganzzahligen Stellen trotz der Nichtkonvergenz der Reihen wesentlich einfacher auszurechnen sind als die an positiven ganzzahligen Stellen. Dies liegt an folgendem Satz, welcher es ermöglicht, unter sehr allgemeinen Voraussetzungen Werte von Dirichtletschen Reihen für ganzzahlige negative Argumente zu bestimmen.

SATZ 1: *Sei* $\varphi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *eine Dirichletsche Reihe, die für mindestens einen* (komplexen) *Wert von* s *konvergiert, und sei* $f(t) = \sum_{n=1}^{\infty} a_n e^{-nt}$ *die entsprechende Exponentialreihe* (welche für alle $t > 0$ konvergiert). *Hat*

$f(t)$ *für* $t \to 0$ *die asymptotische Entwicklung*

$$(1) \qquad f(t) \sim b_0 + b_1 t + b_2 t^2 + \dots \qquad (t \to 0) ,$$

so läßt sich $\varphi(s)$ *holomorph in die ganze komplexe Ebene fortsetzen und es gilt*

$$(2) \qquad \varphi(-n) = (-1)^n\, n!\, b_n \qquad (n = 0, 1, 2, \dots) .$$

Allgemeiner, wenn $f(t)$ *für* $t \to 0$ *die asymptotische Entwicklung*

$$(3) \qquad f(t) \sim \frac{b_{-1}}{t} + b_0 + b_1 t + b_2 t^2 + \dots$$

besitzt, so hat $\varphi(s)$ *eine meromorphe Fortsetzung, die Funktion* $\varphi(s) - \frac{b_{-1}}{s-1}$ *ist ganz, und die Werte* $\varphi(0)$, $\varphi(-1)$, ... *werden nach wie vor durch die Formel (2) gegeben.*

Bemerkungen: 1. "Asymptotische Entwicklung" bedeutet, daß für jede natürliche Zahl N die Abschätzung

$$(4) \qquad \Big| f(t) - \sum_{n<N} b_n t^n \Big| \le C t^N \qquad (0 < t < t_0)$$

gilt (kurz: $f(t) = \sum_{n<N} b_n t^n + O(t^N)$). Insbesondere ist (1) erfüllt, falls $f(t)$ im Punkt $t = 0$ analytisch ist und die Taylor-Entwicklung $\sum_{n=0}^{\infty} b_n t^n$ hat; i.a. wird aber nicht verlangt, daß die Reihe $\sum_{n=0}^{\infty} b_n t^n$ konvergiert, noch, falls sie das tut, daß ihr Wert gleich $f(t)$ ist.

2. Wie aus dem Beweis ersichtlich sein wird, gilt der Satz auch für allgemeine Dirichletsche Reihen $\varphi(s) = \sum_{n=0}^{\infty} \frac{a_n}{\lambda_n^s}$ (falls sie für mindestens ein s absolut konvergieren), wenn man $f(t) = \sum_{n=0}^{\infty} a_n e^{-\lambda_n t}$ setzt.

Beweis des Satzes: Es ist klar, daß die Reihe für $f(t)$ für alle positiven Werte von t absolut konvergiert, da die a_n höchstens polynomial wachsen und die e^{-nt} exponentiell abfallen. Wegen Gleichung (16) von §3 (bzw. Gleichung (18) von §3 im Falle von allgemeinen Dirichletschen Reihen) gilt im Bereich der absoluten Konvergenz die Formel

$$\Gamma(s)\varphi(s) = \int_0^\infty f(t) t^{s-1}\, dt .$$

Wir zerlegen das Integral als $I_1(s) + I_2(s)$ mit

$$I_1(s) = \int_0^1 f(t) t^{s-1}\, dt , \quad I_2(s) = \int_1^\infty f(t) t^{s-1}\, dt .$$

Da $f(t)$ für $t \to \infty$ exponentiell abfällt (nämlich $f(t) = O(e^{-t})$ bzw. $f(t) = O(e^{-\lambda_0 t})$), konvergiert das zweite Integral für alle s, und zwar absolut und gleichmäßig auf kompakten Mengen, es stellt also eine ganze Funktion von s dar. Weiter gilt

$$\int_0^1 \Big(\sum_{n<N} b_n t^n \Big) t^{s-1}\, dt = \sum_{n<N} b_n \frac{t^{n+s}}{n+s} \Big|_0^1 = \sum_{n<N} \frac{b_n}{n+s} \qquad (\sigma > 1) ,$$

also

$$I_1(s) = \sum_{n<N} \frac{b_n}{n+s} + \int_0^1 \Big(f(t) - \sum_{n<N} b_n t^n \Big) t^{s-1}\, dt \qquad (\sigma > 1) ,$$

wobei das Integral wegen (4) für alle s mit $\mathrm{Re}(s) > -N$ absolut und auf kompakten Mengen gleichmäßig konvergiert, also in diesem Gebiet eine holomorphe Funktion darstellt. Die Funktion $\Gamma(s)\varphi(s) - \sum_{n<N} \frac{b_n}{n+s}$ hat also eine holomorphe Fortsetzung in die Halbebene $\mathrm{Re}(s) > -N$. Da N beliebig groß gewählt werden kann, folgt, daß $\Gamma(s)\varphi(s)$ eine meromorphe Fortsetzung auf ganz $\mathbb{C}$ hat, die bis auf (eventuelle) einfache Pole bei $s = -n$ ($n = -1, 0, 1, 2, \dots$) mit Residuum b_n holomorph ist. Da die Funktion $1/\Gamma(s)$ ganz ist und für $s = 0$, $s = -1$, $s = -2$, ... verschwindet, ist $\varphi(s)$ bis auf einen einfachen Pol bei $s = 1$ mit dem Residuum b_{-1} holomorph. Durch Vergleich der Residuen von $\Gamma(s)\varphi(s)$ und $\Gamma(s)$ (vgl. Aufgabe 3, §3) erhält man die Werte (2).

Als erstes Beispiel nehmen wir $\varphi(s) = \zeta(s)$, die Riemannsche Zetafunktion. Hier ist $a_n = 1$, also

$$f(t) = \sum_{n=1}^{\infty} e^{-nt} = \frac{1}{e^t - 1}$$

mit der asymptotischen Entwicklung (hier sogar konvergent für $t < 2\pi$)

$$f(t) \sim \frac{1}{t} + \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!} t^n ,$$

und der Satz gibt sofort die holomorphe Fortsetzung von $\zeta(s) - \frac{1}{s-1}$

auf die ganze Ebene sowie die in §4 erhaltenen Werte

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1} = \begin{cases} -\frac{1}{2} & (n = 0) , \\ -\frac{B_{n+1}}{n+1} & (n \geq 1,\ n \text{ ungerade}) , \\ 0 & (n \geq 2,\ n \text{ gerade}) . \end{cases}$$

Wir betrachten jetzt einen Dirichletschen Charakter χ (mod N) und setzen $a_n = \chi(n)$, $\varphi(s) = L(s,\chi)$ in Satz 1. Wegen der Periodizität der Koeffizienten gilt dann

$$\begin{aligned} f(t) &= \sum_{n=1}^{\infty} \chi(n)\, e^{-nt} \\ &= \sum_{m=1}^{N} \chi(m) (e^{-mt} + e^{-(m+N)t} + e^{-(m+2N)t} + \ldots) \\ &= \sum_{m=1}^{N} \chi(m) \frac{e^{-mt}}{1-e^{-Nt}} . \end{aligned}$$

Die Funktion e^{-mt} hat für $t \to 0$ die asymptotische Entwicklung $\sum_{k=0}^{\infty} \frac{(-m)^k}{k!} t^k$ und die Funktion $\frac{1}{1-e^{-Nt}}$ hat die Entwicklung $\sum_{r=0}^{\infty} \frac{(-1)^r B_r}{r!} (Nt)^{r-1}$, wobei die B_r Bernoullische Zahlen sind (s. (4.7)). Es gilt also

$$f(t) \sim \sum_{m=1}^{N} \chi(m) \sum_{k=0}^{\infty} \sum_{r=0}^{\infty} \frac{(-1)^{k+r} m^k N^{r-1} B_r}{r!\, k!} t^{r+k-1} ,$$

d.h. eine asymptotische Entwicklung der Gestalt (3) mit

$$(5) \qquad b_n = \sum_{m=1}^{N} \chi(m) \sum_{\substack{k,r \geq 0 \\ k+r=n+1}} \frac{(-1)^{k+r} B_r m^k N^{r-1}}{k!\, r!} \qquad (n \geq -1) .$$

Für $n = -1$ reduziert sich diese Summe auf

$$b_{-1} = \frac{1}{N} \sum_{m=1}^{N} \chi(m) ,$$

was für $\chi \neq \chi_0$ verschwindet (§5, Satz 2); nach Satz 1 läßt sich also $L(s,\chi)$ in diesem Fall zu einer für alle s holomorphen Funktion fortsetzen. Für $\chi = \chi_0$ ist

$$b_{-1} = \frac{1}{N} \sum_{\substack{m=1 \\ (m,N)=1}}^{N} 1 = \frac{\phi(N)}{N}$$

und $L(s,\chi)$ hat einen einfachen Pol mit Residuum $\frac{\phi(N)}{N}$ bei $s = 1$, in Übereinstimmung mit (6.3).

Wir können (5) etwas bequemer schreiben, wenn wir die durch

$$(6) \qquad B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} x^k$$

definierten *Bernoullischen Polynome* einführen, also

$$\begin{aligned} B_0(x) &= 1 , \\ B_1(x) &= x - \tfrac{1}{2} , \\ B_2(x) &= x^2 - x + \tfrac{1}{6} , \\ B_3(x) &= x^3 - \tfrac{3}{2} x^2 + \tfrac{1}{6} x , \\ &\vdots \end{aligned}$$

Dann ist nämlich

$$b_n = \frac{(-1)^{n+1}}{(n+1)!} N^n \sum_{m=1}^{N} \chi(m) B_{n+1}\left(\frac{m}{N}\right) ,$$

und wir erhalten aus Satz 1 den

SATZ 2: *Sei χ ein Dirichletscher Charakter modulo N und $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ ($\mathrm{Re}(s) > 1$) die entsprechende L-Reihe. Dann läßt sich $L(s,\chi)$ meromorph auf die ganze Ebene fortsetzen, und zwar holomorph bis auf einen einfachen Pol mit Residuum $\frac{\phi(N)}{N}$ bei $s = 1$ für $\chi = \chi_0$, und es gilt*

$$(7) \qquad L(-n,\chi) = -\frac{N^n}{n+1} \sum_{m=1}^{N} \chi(m) B_{n+1}\left(\frac{m}{N}\right) \qquad (n = 0, 1, 2, \ldots) .$$

Als Beispiel des Satzes haben wir

$$(8) \qquad L(0,\chi) = -\frac{1}{N} \sum_{m=1}^{N} \chi(m)\, m \qquad (\chi \neq \chi_0) .$$

Die Bernoullischen Polynome, die in der Mathematik in vielen Zusammenhängen vorkommen, haben sehr schöne Eigenschaften. Aus (6) erhält man sofort die Formeln

$$(9) \qquad B_n(0) = B_n ,$$

$$(10) \qquad \frac{d}{dx} B_n(x) = n B_{n-1}(x)$$

(die zusammen eine zweite, induktive Definition der Polynome $B_n(x)$ liefern), sowie die erzeugende Funktion

$$(11) \qquad \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!} = \frac{te^{xt}}{e^t-1}$$

(die ebenfalls als Definition der $B_n(x)$ dienen kann). Aus der erzeugenden Funktion erhält man zwei weitere Eigenschaften der Polynome $B_n(x)$: die Symmetrie

$$(12) \qquad B_n(1-x) = (-1)^n B_n(x)$$

und die Rekursion

$$(13) \qquad B_n(x+1) = B_n(x) + nx^{n-1} \ .$$

Es ist übrigens wegen der aus (13) folgenden Formel für Potenzsummen

$$(14) \qquad 1^n + 2^n + \ldots + N^n = \frac{B_{n+1}(N+1)-B_{n+1}(0)}{n+1} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} B_k \frac{N^{n+1-k}}{n+1-k} \ ,$$

daß Jakob Bernoulli die nach ihm benannten Zahlen B_k eingeführt hat.

Wegen $\chi(-1)^2 = \chi(1) = 1$ gilt für jeden Dirichletschen Charakter χ entweder $\chi(-1) = +1$ oder $\chi(-1) = -1$; wir nennen χ im ersten Fall *gerade* und im zweiten Fall *ungerade*. Der triviale Charakter ist z.B. immer gerade. Mit Hilfe von (12) erhält man nun leicht das folgende Korollar zu Satz 2:

KOROLLAR: *Außer im Falle* $N = 1$, $n = 0$ *gilt für alle* χ *und alle* $n \geq 0$

$$\chi(-1) = (-1)^n \Rightarrow L(-n,\chi) = 0 \ ,$$

d.h. die L-Reihe von einem geraden bzw. ungeraden Charakter verschwindet an den negativen geraden bzw. ungeraden Stellen.

Das Korollar sowie seine Umkehrung (d.h., daß $L(-n,\chi)$ nur für die genannten Werte von n verschwindet) können auch aus der Funktionalgleichung der L-Reihe $L(s,\chi)$ abgeleitet werden. Wegen ihrer großen Bedeutung für die analytische Zahlentheorie werden wir diese Funktionalgleichung hier angeben, obwohl sie in diesem Buch weder bewiesen noch verwendet werden wird. Wir können uns dabei auf primitive Charaktere beschränken, da für einen von einem Charakter χ_1 induzierten Charakter $\chi \pmod N$ die elementare Beziehung

$$L(s,\chi) = \prod_{p \mid N} \left(1 - \frac{\chi_1(p)}{p^s}\right) \cdot L(s,\chi_1)$$

zwischen den L-Reihen gilt. Die Funktionalgleichung für χ primitiv ist

$$(15) \qquad \pi^{-s/2} N^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi) = \frac{G}{i^\delta \sqrt{N}} \pi^{-(1-s)/2} N^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s,\bar{\chi}) \ ;$$

dabei ist $\bar{\chi}$ der zu χ konjugierte Charakter, δ gleich 0 bzw. 1 für χ gerade bzw. ungerade und G die *Gaußsche Summe* $\sum_{n=1}^{N} \chi(n) e^{2\pi i n/N}$. Der Faktor $\frac{G}{i^\delta \sqrt{N}}$ in (15) hat stets den Absolutbetrag 1.

Aus der Funktionalgleichung und Satz 2 erhält man die Werte von $L(n,\chi)$ für $n \geq 1$, $\chi(-1) = (-1)^n$; z.B. liefern (8) und (15)

$$L(1,\chi) = -\frac{\pi i G}{N^2} \sum_{m=1}^{N} \bar{\chi}(m)\, m$$

für χ primitiv und ungerade. Da wir aber die Funktionalgleichung nicht bewiesen haben und ohnehin auf diese Weise nur die Hälfte der Fälle erledigen können, werden wir in §9 einen anderen Weg zur Berechnung von $L(1,\chi)$ beschreiben.

Wir schließen mit einer kleinen Tabelle von Werten von L-Reihen an negativen ganzen Stellen für die in §5 bestimmten primitiven reellen Charaktere χ_D.

Tabelle 1. Werte von $L(-n,\chi_D)$

D	-3	-4	-7	-8	-11	-15	-19	-20	-23	-24	-31	-35
$L(0,\chi_D)$	$\frac{1}{3}$	$\frac{1}{2}$	1	1	1	2	1	2	3	2	3	2
$-\frac{1}{2}L(-2,\chi_D)$	$\frac{1}{9}$	$\frac{1}{4}$	$\frac{8}{7}$	$\frac{3}{2}$	3	8	11	15	24	23	48	54
$\frac{1}{2}L(-4,\chi_D)$	$\frac{1}{3}$	$\frac{5}{4}$	16	$\frac{57}{2}$	$\frac{1275}{11}$	496	1345	1761	3408	3985	12960	21186

D	1	5	8	12	13	17	21	24	28	29	33
$-\frac{1}{2}L(-1,\chi_D)$	$\frac{1}{24}$	$\frac{1}{5}$	$\frac{1}{2}$	1	1	2	2	3	4	3	6
$\frac{1}{2}L(-3,\chi_D)$	$\frac{1}{240}$	1	$\frac{11}{2}$	23	29	82	154	261	452	471	846
$-\frac{1}{2}L(-5,\chi_D)$	$\frac{1}{504}$	$\frac{67}{5}$	$\frac{361}{2}$	1681	$\frac{33463}{13}$	11582	35942	76083	177844	211833	445386

Aufgaben:

1. Man beweise die erste Aussage von Satz 1 (nämlich, daß sich aus der Existenz einer asymptotischen Entwicklung (1) die holomorphe Fortsetzbarkeit von $\varphi(s)$ sowie die Werte (2) ergeben) auf folgende Weise:

   a) Die Aussage gilt für $\varphi(s) = n^{-s}$ und daher für jede endliche Dirichletsche Reihe.

   b) Für φ und f wie im Satz folgt aus $f(t) = O(t^N)$ $(t \to 0)$, daß $\varphi(s)$ in die Halbebene $\mathrm{Re}(s) > -N$ holomorph fortsetzbar ist und daß $\varphi(-n) = 0$ für $0 \le n < N$.

   c) Für vorgegebene $b_0, \ldots, b_{N-1}$ gibt es eine endliche Dirichletsche Reihe, deren zugehörige Exponentialreihe für $t \to 0$ gleich $\sum_{0 \le n < N} b_n t^n + O(t^N)$ ist.

2. Man verifiziere die Eigenschaften (9) - (14) der Bernoullischen Polynome.

3. Sei $\zeta(s,a) = \sum_{n=0}^{\infty} (n+a)^{-s}$ $(\mathrm{Re}(s) > 1,\ a > 0)$ die *Hurwitzsche Zetafunktion*. Mit Hilfe von Satz 1 zeige man, daß $\zeta(s,a) - \frac{1}{s-1}$ eine holomorphe Fortsetzung in die ganze Ebene hat und für $s = 0, -1, -2, \ldots$ die Werte

$$\zeta(-n,a) = -\frac{1}{n+1} B_{n+1}(a)$$

   annimmt. Insbesondere folgt Satz 2 aus der Identität $L(s,\chi) = N^{-s} \sum_{m=1}^{N} \chi(m)\, \zeta(s,\frac{m}{N})$ und (13) aus der Identität $\zeta(s,a) = a^{-s} + \zeta(s,a+1)$.

4. Man zeige, daß $B_n(\frac{1}{2}) = -(1 - 2^{1-n})B_n$, und allgemeiner, daß

$$B_n(kx) = k^{n-1} \sum_{j=0}^{k-1} B_n(x + \tfrac{j}{k}) \qquad (k = 1, 2, \ldots)\ .$$

5. Man beweise die Euler-Maclaurinsche Summationsformel

$$\sum_{r=1}^{N} f(r) = \int_0^N f(x)dx + \sum_{k=0}^{K-1} \frac{(-1)^k B_{k+1}}{(k+1)!} \left(f^{(k)}(0) - f^{(k)}(N)\right) - \frac{(-1)^K}{K!} \int_0^N B_K(x-[x])\, f^{(K)}(x)dx\ ,$$

   wobei $K \ge 1$ und N natürliche Zahlen sind, $f(x)$ eine genügend oft differenzierbare Funktion auf $[0,N]$ ist und $[x]$ den ganzzahligen Teil von x bezeichnet. Formel (14) ist der Spezialfall $f(x) = x^n$, $N > n$.

   Hinweis: Der Fall $N = 1$ folgt aus (10) durch partielle Integration; den allgemeinen Fall erhält man, indem man diesen Spezialfall auf $f(x), f(x+1), \ldots, f(x+N-1)$ anwendet und summiert.

Literatur zu Teil I

Die analytischen bzw. formalen Eigenschaften von Dirichletschen Reihen werden in

G.H. Hardy und M. Riesz, *The General Theory of Dirichlet's Series*, Cambridge Tracts No. 18, Cambridge 1915

bzw.

G.H. Hardy und E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford 1971, Kap. XVI, XVII

(in deutscher Übersetzung erschienen bei Oldenburg, München 1958) ausführlich behandelt, wobei das zweite Buch auch sonst als Einführung und Nachschlagewerk für die elementare Zahlentheorie sehr zu empfehlen ist. Beide Themen werden auch in

T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York-Heidelberg-Berlin 1976, Kap. 2, 11

behandelt. Die Eigenschaften der Gammafunktion werden in fast jedem Buch über Funktionentheorie und in vielen über analytische Zahlentheorie angegeben, z.B.

L.V. Ahlfors, *Complex Analysis*, McGraw-Hill, New York 1966, §5.2.4.

Für die Mellin-Transformation und ihre zahlentheoretischen Anwendungen siehe etwa

H. Rademacher, *Topics in Analytic Number Theory*, Grundlehren 169, Springer-Verlag, New York-Heidelberg-Berlin 1973, Kap. 3.

Das beste Werk speziell über die Riemannsche Zetafunktion ist

H. Edwards, *Riemann's Zeta Function*, Academic Press, New York-London 1974,

während die allgemeine Theorie der Dirichletschen Charaktere und L-Reihen im oben zitierten Buch von Apostol (Kap. 6, 12) und in

H. Davenport, *Multiplicative Number Theory*, Markham, Chicago 1967,

C.L. Siegel, *Analytische Zahlentheorie I, II*, vervielfältigte Vorlesungsausarbeitung, Göttingen 1963,

die beide ausgezeichnet sind, behandelt wird.

Teil II. Quadratische Körper und ihre Zetafunktionen

§8 Binäre quadratische Formen

Neben dem Beweis des Satzes, daß arithmetische Folgen unendlich viele Primzahlen enthalten, war der Wunsch, Klassenzahlen binärer quadratischer Formen ausrechnen zu können, einer der Hauptgründe Dirichlets, Charaktere und L-Reihen einzuführen. Was diese Klassenzahlen sind und wie sie mit L-Reihen zusammenhängen, wollen wir in diesem Paragraphen erläutern, wobei wir im wesentlichen Dirichlets Argument folgen werden.

Als erstes müssen wir etwas über die Theorie der quadratischen Formen erzählen, die fast ganz von Gauß in den *Disquisitiones Arithmeticae* entwickelt wurde. Der Ausgangspunkt dieser Theorie ist die Frage nach der *Lösbarkeit* von quadratischen Diophantischen Gleichungen, z.B. der Nachweis, daß die *Pellsche Gleichung*

$$t^2 - Du^2 = 4 \tag{1}$$

für jede Nichtquadratzahl $D > 0$ eine Lösung mit $u \neq 0$ hat oder der Fermatsche Satz, daß jede Primzahl $p \equiv 1 \pmod 4$ eine Darstellung

$$p = x^2 + y^2 \tag{2}$$

zuläßt. Außerdem interessiert man sich für die *Anzahl* der Lösungen, z.B für die Tatsache, daß die Darstellung (2) bis auf die Reihenfolge von x und y eindeutig ist. Allgemein ist eine *binäre quadratische Form* ein Ausdruck der Gestalt

$$f(x,y) = ax^2 + bxy + cy^2 , \tag{3}$$

wobei a, b, c (die *Koeffizienten* der Form) als fest und x, y als veränderlich anzusehen sind. Wir werden stets annehmen, daß die Koeffizienten a, b, c in $\mathbb{Z}$ liegen und auch, da wir nur binäre Formen (d.h. Formen in zwei Variablen) betrachten, das Wort "binär" häufig

weglassen. Die Hauptfrage ist dann, für eine gegebene quadratische Form f und ganze Zahl n die Lösungen der Gleichung $f(x,y) = n$ $(x,y \in \mathbb{Z})$ zu beschreiben.

Sei $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ eine 2×2 Matrix mit ganzzahligen Koeffizienten und Determinante 1. Ersetzen wir x und y in (3) durch

$$\begin{aligned} x' &= \alpha x + \beta y \ , \\ y' &= \gamma x + \delta y \ , \end{aligned} \tag{4}$$

so geht (3) in die Form $a'x^2 + b'xy + c'y^2$ mit

$$a'x^2 + b'xy + c'y^2 = a(\alpha x+\beta y)^2 + b(\alpha x+\beta y)(\gamma x+\delta y) + c(\gamma x+\delta y)^2, \tag{5}$$

d.h. mit

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 \ , \end{aligned} \tag{6}$$

über. Die Frage, ob für eine Zahl n die Gleichung

$$ax^2 + bxy + cy^2 = n \tag{7}$$

lösbar ist, ist jetzt offensichtlich mit der Frage äquivalent, ob

$$a'x^2 + b'xy + c'y^2 = n \qquad (x, y \in \mathbb{Z}) \tag{8}$$

lösbar ist, denn jede Lösung von (8) liefert wegen (5) eine Lösung $(\alpha x + \beta y, \gamma x + \delta y)$ von (7), und umgekehrt führt jede Lösung von (7) vermöge der zu (4) inversen Transformation

$$\begin{aligned} x &= \delta x' - \beta y' \\ y &= -\gamma x' + \alpha y' \end{aligned}$$

zu einer Lösung von (8). Es gibt also eine natürliche bijektive Korrespondenz zwischen den Lösungsmengen der Gleichungen (7) und (8), und da wir uns ja gerade für diese Lösungen interessieren, ist es natürlich, die entsprechenden quadratischen Formen als äquivalent zu betrachten. Dies führt zu folgender

Definition: Zwei quadratische Formen $f(x,y) = ax^2 + bxy + cy^2$ und $f'(x,y) = a'x^2 + b'xy + c'y^2$ heißen *äquivalent*, falls sie unter einer Substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$ wie in (5) ineinander übergehen, d.h. falls die Koeffizienten von f und f' durch (6) verknüpft sind.

Da die Menge $SL_2(\mathbb{Z})$ der Matrizen $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$, eine Gruppe bildet, also unter Inversenbildung und Zusammensetzung abgeschlossen ist, ist es klar, daß diese Relation symmetrisch und transitiv, also wirklich eine Äquivalenzrelation ist.

Wieviele Äquivalenzklassen gibt es? Sicherlich unendlich viele, denn - wie man leicht nachprüft - die *Diskriminante*

$$D = b^2 - 4ac \tag{9}$$

einer Form (3) ist eine Invariante der Äquivalenzklasse (d.h., sie bleibt unverändert unter der Transformation (6)), und es gibt umgekehrt zu jeder Zahl D mit

$$D \equiv 0 \text{ oder } 1 \pmod 4 \tag{10}$$

mindestens eine Form der Diskriminante D, nämlich die *Grundform*

$$f_1(x,y) = \begin{cases} x^2 - \frac{D}{4} y^2 \ , & \text{falls } D \equiv 0 \pmod 4 \\ x^2 + xy + \frac{1-D}{4} y^2 \ , & \text{falls } D \equiv 1 \pmod 4 \ . \end{cases} \tag{11}$$

Eine vernünftigere Frage wäre also: wieviele Äquivalenzklassen von Formen gibt es mit gegebener Diskriminante? Das erste Hauptergebnis besagt, daß es nur endlich viele gibt:

SATZ 1: *Sei* $D \in \mathbb{Z}$, D *kein Quadrat. Dann gibt es nur endlich viele Äquivalenzklassen von quadratischen Formen mit der Diskriminante* D.

Bemerkung: Die Behauptung des Satzes bleibt richtig für D ein Quadrat, $D \neq 0$ (s. Aufgabe 1). Formen mit quadratischer Diskriminante werden wir im folgenden aber nicht betrachten, da diese in lineare Faktoren zerfallen.

Beweis: Wir zeigen, daß jede Form $f = ax^2 + bxy + cy^2$ zu einer Form $a'x^2 + b'xy + c'y^2$ äquivalent ist, deren Koeffizienten den Ungleichungen

$$|b'| \leq |a'| \leq |c'| \tag{12}$$

genügen. Die Behauptung folgt dann, da es nur endlich viele Zahlentripel (a', b', c') gibt, die (12) erfüllen und einen gegebenen Wert $b'^2 - 4a'c' = D$ haben: es ist nämlich

$$|D| = |b'^2 - 4a'c'| \geq |4a'c'| - |b'|^2$$

$$\geq 4|a'|^2 - |a'|^2 = 3a'^2 ,$$

also

$$|a'| \leq \sqrt{\frac{|D|}{3}} , \quad |b'| \leq |a'| , \quad c' = \frac{b'^2 - D}{4a'} ,$$

so daß nur endlich viele Werte für a', b', c' in Frage kommen. Um (12) zu erreichen, wählen wir a' als die dem Absolutbetrag nach kleinste Zahl, die durch f darstellbar ist. Dann gibt es Zahlen α und γ mit

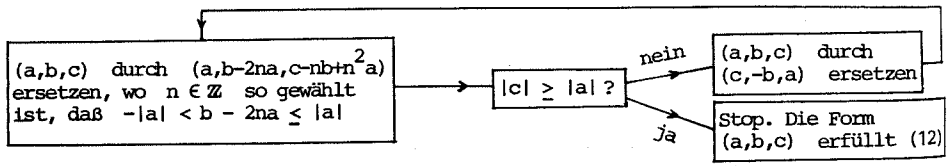
$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 ,$$

und der größte gemeinsame Teiler r von α und γ muß gleich 1 sein, weil a'/r^2 durch f darstellbar ist. Wir können also Zahlen β und δ so wählen, daß $\alpha\delta - \beta\gamma = 1$ ist; dann transformiert $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ die Form f in eine Form $a'x^2 + b''xy + c''y^2$ mit a' als erstem Koeffizienten (vgl. (6)). Wir wählen dann eine ganze Zahl n so, daß $b' := b'' - 2a'n$ dem Absolutbetrag nach kleiner gleich a' ist. Wegen

$$a'(x - ny)^2 + b''(x - ny)y + c''y^2$$

$$= a'x^2 + (b'' - 2a'n)xy + (a'n^2 - b''n + c'')y^2$$

ist dann $a'x^2 + b''xy + c''y^2$ (und somit auch f) zu einer Form $a'x^2 + b'xy + c'y^2$ äquivalent mit $|b'| \leq |a'|$ (oder sogar $-|a'| < b' \leq |a'|$). Schließlich ist nach Wahl von a' automatisch $|c'| \geq |a'|$, also (12) erfüllt. Damit ist der Satz bewiesen. Dieser Beweis, der ineffektiv ist (wie findet man a'?), kann durch einen effektiven Algorithmus ersetzt werden; dieser Algorithmus wird durch das Flußdiagramm



verdeutlicht und bricht deswegen nach endlich vielen Schritten ab, weil $|a|$ bei jedem Umlauf um mindestens 1 heruntergeht.

Die Aussage des Satzes folgt auch aus den später in diesem Paragraphen ausgeführten Überlegungen über Darstellungsanzahlen.

Wir wollen die Klassenzahl von D, also die Anzahl der Äquivalenzklassen von quadratischen Formen der Diskriminante D, einführen und studieren. Neben der Diskriminante gibt es aber zwei weitere elementare Invarianten von quadratischen Formen, und wir wollen die Einteilung von Formen in Äquivalenzklassen verfeinern, indem wir auch diese festlegen. Die Invarianten sind:

1) der g.g.T. der Koeffizienten von f,
2) das Vorzeichen des ersten Koeffizienten, falls $D < 0$.

In der Tat, wenn a, b und c durch r teilbar sind, ist r nach (6) auch ein Teiler von a', b' und c'; es gilt also $(a,b,c) \mid (a',b',c')$ und wegen der Symmetrie dann $(a,b,c) = (a',b',c')$. Sind $ax^2 + bxy + cy^2$ und $a'x^2 + b'xy + c'y^2$ äquivalent und $D < 0$, so ist nach (6)

$$(13) \qquad aa' = a^2\alpha^2 + ab\alpha\gamma + ac\gamma^2 = (a\alpha + \tfrac{1}{2}b\gamma)^2 + \tfrac{1}{4}|D|\gamma^2 > 0 ,$$

also haben a und a' dasselbe Vorzeichen. Ist dieses Vorzeichen positiv, so ist $f(\alpha,\gamma)$ wegen (13) für alle $(\alpha,\gamma) \neq (0,0)$ positiv; die Form heißt dann *positiv-definit*. Ist $a < 0$, so stellt f nur negative Zahlen dar und heißt *negativ-definit*. Die Äquivalenzklassen von quadratischen Formen zerfallen also für $D < 0$ in zwei Typen, je nachdem, ob sie positiv- oder negativ-definite Formen enthalten; wir brauchen nur die positiv-definiten zu betrachten, da die negativ-definiten Formen durch Multiplikation mit -1 aus ihnen entstehen. Wir können uns auch auf Formen beschränken, für die der g.g.T. der Koeffizienten gleich 1 ist - solche Formen heißen *primitiv* - weil eine Form der Diskriminante D mit $(a,b,c) = r$ einfach r mal eine primitive Form der Diskriminante D/r^2 ist. Wir definieren also die *Klassenzahl* von D als

$$h(D) = \begin{cases} \text{Anzahl der Äquivalenzklassen von primitiven quadratischen Formen der Diskriminante } D, \\ \text{falls } D > 0, \\ \\ \text{Anzahl der Äquivalenzklassen von positiv-definiten primitiven Formen der Diskriminante } D, \text{ falls } D < 0. \end{cases}$$

Diese Anzahl ist nach Satz 1 endlich. Sie ist Null, falls (10) nicht erfüllt ist, da dann (9) keine Lösung hat, ist dagegen ≥ 1, falls (10) erfüllt ist, da es dann immer mindestens die Grundform (11) gibt. Wir fügen eine kleine Tabelle von Klassenzahlen bei. (Wie man diese Werte berechnet, werden wir später sehen.)

D	-24	-23	-20	-19	-16	-15	-12	-11	-8	-7	-4	-3
h(D)	2	3	2	1	1	2	1	1	1	1	1	1

D	1	4	5	8	9	12	13	16	17	20	21	24	25	28	29
h(D)	1	1	1	1	2	2	1	2	1	3	2	2	4	2	1

Warnung: Es gibt zwei Begriffe von Äquivalenz (und damit auch zwei Klassenzahlen), die in der Literatur gebraucht werden. Die oben eingeführte Äquivalenz bezüglich $SL_2(\mathbb{Z})$ heißt *Äquivalenz im engeren Sinne*. Die *Äquivalenz im weiteren Sinne* ist definiert durch die Formel: $f' \sim f$, falls

$$f'(x,y) = \mu f(\alpha x+\beta y, \gamma x+\delta y) \quad , \tag{14}$$

wobei $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ eine 2×2 Matrix mit ganzzahligen Koeffizienten und Determinante $\alpha\delta - \beta\gamma = \mu = \pm 1$ ist. Dieser letzte Begriff (allerdings häufig fehlerhaft definiert, indem der Faktor μ in (14) fehlt) wird in vielen Lehrbüchern zugrundegelegt und die Klassenzahl $h(D)$ entsprechend definiert als die Anzahl der Äquivalenzklassen von primitiven quadratischen Formen der Diskriminante D (nicht notwendig positiv-definit, falls $D < 0$) im weiteren Sinne. Diese andere Klassenzahl, die wir mit $h_0(D)$ bezeichnen werden, stimmt für D negativ mit unserer Klassenzahl überein, da die Transformationen (14) mit $\mu = -1$ einfach die positiv- und negativ-definiten Formen vertauschen. Für $D > 0$ gilt $h_0(D) = h(D)$ oder $h_0(D) = \frac{1}{2} h(D)$ (s. Aufgabe 5).

Sei jetzt f eine quadratische Form. Wir wollen wissen, welche Zahlen f darstellt und wie oft, d.h. die Lösungen der Diophantischen Gleichung

$$f(x,y) = n \qquad (x, y \in \mathbb{Z}) \tag{15}$$

untersuchen. Auf der Menge dieser Lösungen gibt es eine natürliche Äquivalenzrelation. Ist nämlich $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ eine Matrix mit der Eigenschaft, daß die durch (6) definierte quadratische Form $a'x^2 + b'xy + c'y^2$ mit f übereinstimmt, dann führt die Transformation (4) offenbar eine Lösung von (15) in eine andere über. In diesem Falle nennen wir $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ einen *Automorphismus* von f. Es ist klar, daß die Automorphismen von f eine Untergruppe U_f von $SL_2(\mathbb{Z})$ bilden; nach (6) ist

$$U_f = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \textcircled{1}\ a\alpha^2 + b\alpha\gamma + c\gamma^2 = a,\ \textcircled{2}\ 2a\alpha\beta + b\beta\gamma + b\alpha\delta + 2c\gamma\delta = b,\ \textcircled{3}\ a\beta^2 + b\beta\delta + c\delta^2 = c \right\}. \tag{16}$$

Wir definieren die *Darstellungsanzahl* $R(n,f)$ *von* n *durch die Form* f als die Anzahl der unter der Operation von U_f inäquivalenten Lösungen der Gleichung (15). Es wird sich herausstellen, daß $R(n,f)$ endlich ist. Offenbar hängt sie nur von der Äquivalenzklasse von f ab. Wir definieren die *Gesamtdarstellungsanzahl* $R(n)$ *von* n *durch Formen der Diskriminante* D als

$$R(n) = \sum_{i=1}^{h(D)} R(n,f_i) \quad , \tag{17}$$

wobei $f_1, \ldots, f_{h(D)}$ Repräsentanten der Äquivalenzklassen von primitiven binären quadratischen Formen der Diskriminante D sind (positiv- bzw. negativ-definit, falls $D < 0$ und n positiv bzw. negativ ist).

Für die einzelnen Darstellungsanzahlen $R(n,f_i)$ ist kein geschlossener Ausdruck bekannt; man kann i.a. nur den Mittelwert $\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} R(n,f_i)$ berechnen. Dagegen läßt sich die Gesamtdarstellungsanzahl $R(n)$ in geschlossener Form angeben. Die Schritte zur Berechnung der Klassenzahl nach Gauß und Dirichlet werden also die folgenden sein:

i) Bestimmung der Struktur der Automorphismengruppe U_f;
ii) Berechnung von $R(n)$ (also auch von deren mittlerem Wert);
iii) Berechnung der mittleren Werte der $R(n,f_i)$, $1 \le i \le h(D)$;
iv) Bestimmung von $h(D)$ durch Vergleich von ii) und iii).

Diese vier Schritte werden in den nächsten vier Sätzen durchgeführt.

SATZ 2: *Sei* $f(x,y) = ax^2 + bxy + cy^2$ *eine primitive quadratische Form der Diskriminante* D, D *keine Quadratzahl. Dann liefert die Abbildung*

$$(t,u) \mapsto \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix} \tag{18}$$

eine Bijektion zwischen der Menge der Lösungen (t,u) *der Pellschen Gleichung (1) und der Automorphismengruppe von* f. *Diese Bijektion ist ein Gruppenisomorphismus bezüglich der Kompositionsregel*

$$(t_1,u_1) \circ (t_2,u_2) = \left(\frac{t_1t_2 + Du_1u_2}{2}, \frac{t_1u_2 + u_1t_2}{2} \right) \tag{19}$$

für Lösungen von (1). Die Gruppe U_f *ist für* $D < 0$ *endlich, und zwar zyklisch von der Ordnung*

$$w = \begin{cases} 6 & \text{für } D = -3, \\ 4 & \text{für } D = -4, \\ 2 & \text{für } D < -4. \end{cases} \tag{20}$$

Für $D > 0$ *ist* $U_f \cong \mathbb{Z} \times \mathbb{Z}/2$.

Beweis: Aus (16) finden wir für $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in U_f$

$$\begin{aligned} a\beta &= \beta(a\alpha^2 + b\alpha\gamma + c\gamma^2) \qquad \text{(wegen ①)}\\ &= \alpha(a\alpha\beta + b\beta\gamma) + c\beta\gamma^2\\ &= \alpha(-c\gamma\delta) + c\beta\gamma^2 \end{aligned}$$

(da wegen ② $2(a\alpha\beta + b\beta\gamma + c\gamma\delta) = b(1 - \alpha\delta + \beta\gamma) = 0$)

$$= -c\gamma \qquad \text{(wegen } \alpha\delta - \beta\gamma = 1)$$

und analog

$$\begin{aligned} c(\alpha-\delta) &= \alpha(a\beta^2 + b\beta\delta + c\delta^2) - c\delta \qquad \text{(wegen ③)}\\ &= \beta(a\alpha\beta + c\gamma\delta) + b\alpha\beta\delta \qquad \text{(wegen } \alpha\delta - \beta\gamma = 1)\\ &= -\beta(b\beta\gamma) + b\alpha\beta\delta \quad \text{(wieder wegen } a\alpha\beta + b\beta\gamma + c\gamma\delta = 0)\\ &= \beta b\ , \end{aligned}$$

also $\frac{\gamma}{a} = \frac{\delta-\alpha}{b} = \frac{-\beta}{c}$. Da $(a,b,c) = 1$ ist, ist dieser gemeinsame Wert eine ganze Zahl u; mit $t = \alpha + \delta$ haben wir dann

$$\alpha = \frac{t-bu}{2}\ ,\ \delta = \frac{t+bu}{2}\ ,\ \beta = -cu\ ,\ \gamma = au\ ,$$

und aus $\alpha\delta - \beta\gamma = 1$ folgt dann $t^2 - Du^2 = 4$. Umgekehrt findet man durch Einsetzen, daß die Matrix in (18) ein Automorphismus von f ist. Daß die Matrizenmultiplikation der Regel (19) entspricht, ergibt sich ebenfalls durch direktes Rechnen.

Ist jetzt $D < 0$, so ist $t^2 - Du^2 \geq t^2$ und $t^2 - Du^2 \geq |D|u^2$; also hat (1) nur Lösungen für $|t| \leq 2$, $|u| \leq 2$, und zwar

$$\begin{aligned} &(t,u) = (\pm 2,0) \text{ oder } (\pm 1,\pm 1) \text{ für } D = -3\ ,\\ (21)\qquad &(t,u) = (\pm 2,0) \text{ oder } (0,\pm 1) \text{ für } D = -4\ ,\\ &\text{nur } (t,u) = (\pm 2,0)\ , \qquad \text{falls } D < -4\ . \end{aligned}$$

Damit ist gezeigt, daß die Anzahl der Lösungen von (1) gleich der in (20) angegebenen Zahl w ist. Wenn wir für jede Lösung (t,u) von (1)

$$(22)\qquad \varepsilon = \frac{t + u\sqrt{D}}{2}\ ,\ \varepsilon' = \frac{t - u\sqrt{D}}{2} \qquad (\varepsilon\varepsilon' = 1)$$

setzen (bei fester Wahl von $\sqrt{D}$), dann entspricht (19) einfach der Multiplikation der entsprechenden Zahlen ε; wir erhalten also durch

$$(23)\qquad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \mapsto \varepsilon = \frac{\alpha+\delta}{2} + \frac{\gamma}{2a}\sqrt{D}$$

einen injektiven Homomorphismus von U_f in $\mathbb{C}^*$. Für $D < 0$ haben wir nach (21)

$$(24)\qquad \begin{aligned} &\varepsilon = \pm 1 \text{ oder } \frac{\pm 1 \pm i\sqrt{3}}{2} \text{ für } D = -3\\ &\varepsilon = \pm 1 \text{ oder } \pm i \text{ für } D = -4\\ &\varepsilon = \pm 1 \text{ für } D < -4\ , \end{aligned}$$

also genau die w-ten Einheitswurzeln; das zeigt, daß U_f zyklisch ist. (Man kann natürlich auch direkt nachrechnen, daß alle Lösungen (21) unter dem Gruppengesetz (19) Potenzen von $(1,1)$ bzw. $(0,1)$ bzw. $(-2,0)$ sind.)

Für $D > 0$ liefert (23) eine Injektion $U_f \to \mathbb{R}^*$. Das Bild ist eine Untergruppe von $\mathbb{R}^*$, die -1 enthält. Da (mit der positiven Wahl von $\sqrt{D}$) die Zahl ε in (22) für $t, u > 0$ mindestens gleich $\frac{1 + \sqrt{D}}{2} > 1$ ist, ist das Bild nicht dicht in $\mathbb{R}^*$. Es gibt also nur zwei Möglichkeiten: entweder ist die Pellsche Gleichung nur trivial (d.h. mit $u = 0$, $t = \pm 2$) lösbar und $U_f = \{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\}$, oder es gibt eine kleinste Lösung (t_0,u_0) von (1) mit $t_0, u_0 > 0$ und die Menge der ε in (22) ist gleich $\{\pm\varepsilon_0^n | n \in \mathbb{Z}\}$ mit $\varepsilon_0 = \frac{t_0 + u_0\sqrt{D}}{2}$, also $U_f \cong \mathbb{Z} \times \mathbb{Z}/2$. Wir werden später sehen, daß stets der zweite Fall zutrifft, womit auch die letzte Behauptung des Satzes bewiesen sein wird. Die Zahl ε_0 heißt die *Grundeinheit* der Form f. Sie hängt nur von D ab.

Der Einfachheit halber formulieren wir den nächsten Satz und sein Korollar nur für Fundamentaldiskriminanten. Für den allgemeinen Fall s. Aufgabe 8.

SATZ 3: *Sei* D *eine Fundamentaldiskriminante,* $n \neq 0$ *eine ganze Zahl. Dann wird die Gesamtanzahl* $R(n)$ *der Darstellungen von* n *durch (primitive) Formen der Diskriminante* D *durch*

$$(25)\qquad R(n) = \sum_{m|n} \chi_D(m)$$

gegeben, wobei m *über alle positiven Teiler von* n *läuft und* $\chi_D(m)$ *der in §5 eingeführte Charakter ist. Insbesondere sind* $R(n)$ *und somit alle* $R(n,f)$ *endlich.*

Bemerkung: Die rechte Seite von (25) ist identisch mit der in (6.10) eingeführten Summte $\rho(n)$. Somit erhalten die in §6 für den Nachweis

von $L(1,\chi) \neq 0$ benutzten Ungleichungen (6.12) eine anschauliche Bedeutung, da offensichtlich $R(n) \geq 0$ und $R(n^2) > 0$ ist (ein Quadrat hat immer eine Darstellung durch (11) mit $y = 0$).

Beweis: Da es keine imprimitiven Formen der Diskriminante D gibt, können wir den Zusatz "primitive" im Satz weglassen. Sei $R^*(n)$ die Anzahl der inäquivalenten *primitiven* Darstellungen von n durch Formen der Diskriminante D (eine Darstellung (15) heißt primitiv, falls x und y teilerfremd sind). Offensichtlich ist

$$R(n) = \sum_{\substack{g \geq 1 \\ g^2 | n}} R^*\left(\frac{n}{g^2}\right) , \tag{26}$$

da jede Darstellung Vielfaches einer primitiven ist. Der Hauptschritt im Beweis ist der Nachweis der Formel

$$R^*(n) = \#\{b \pmod{2n} \mid b^2 \equiv D \pmod{4n}\} . \tag{27}$$

Der Beweis von (27) stützt sich auf folgendes allgemeine Prinzip. Sei G eine Gruppe, X und Y zwei Mengen, auf denen G operiert, und $S \subseteq X \times Y$ eine unter der Diagonaloperation von G invariante Teilmenge. Wenn zwei Elemente $s = (x,y)$, $s' = (x',y') \in S$ unter G äquivalent sind, also $(x',y') = (gx,gy)$, so sind insbesondere ihre ersten Komponenten G-äquivalent. Wir können also die Bahnenmenge S/G analysieren, indem wir erst X/G beschreiben und dann fragen, wieviele Elemente von S/G ein gegebenes Element von X/G als erste Komponente haben. Als Vertreter für diese Bahnen können wir Paare (x,y) nehmen, deren erste Komponente ein fester Vertreter der gegebenen Bahn in X/G ist. Zwei solche Paare (x,y) und (x,y') sind genau dann äquivalent, wenn $y' = gy$ mit $g \in G$, $gx = x$; die besagten Bahnen stehen also in eineindeutiger Korrespondenz mit den Bahnen von $Y_x = \{y \in Y \mid (x,y) \in S\}$ unter der Operation des Stabilisators $G_x = \{g \in G \mid gx = x\}$ von x in G. Insbesondere gilt für die Anzahl der Bahnen die Formel

$$|S/G| = \sum_{x \in X/G} |Y_x/G_x| , \tag{28}$$

falls beide Seiten endlich sind, und durch Rollenvertauschung natürlich auch

$$|S/G| = \sum_{y \in Y/G} |X_y/G_y| . \tag{29}$$

Wir wenden diese Formel an mit

$$G = SL_2(\mathbb{Z}) = \{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z},\ \alpha\delta - \beta\gamma = 1\} ,$$

$$X = \{\text{quadratische Formen } f(x,y) = ax^2+bxy+cy^2,\ b^2-4ac = D\} ,$$

$$Y = \{\text{Zahlenpaare } z = (x,y) \text{ mit } x, y \in \mathbb{Z} \text{ teilerfremd}\} ,$$

$$S = \{(f,z) \in X \times Y \mid f(z) = n\} .$$

Dann sind die Elemente von X/G die Äquivalenzklassen von Formen der Diskriminante D, und für $f \in X$ ist Y_f/G_f die Menge der inäquivalenten primitiven Darstellungen von n durch f, also nach (28)

$$|S/G| = \sum_{\substack{\text{Äquivalenz-} \\ \text{klassen von } f}} R^*(n,f) = R^*(n) .$$

Andererseits können wir $|S/G|$ durch (29) berechnen. Jedes Element von Y ist zu $(1,0)$ äquivalent, da es für $(x,y) \in Y$ Zahlen $a, b \in \mathbb{Z}$ gibt mit $ax + by = 1$, also $\begin{pmatrix} x & -b \\ y & a \end{pmatrix} \in G$, $\begin{pmatrix} x & -b \\ y & a \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$. Somit besteht Y/G aus einer Bahn mit dem Vertreter $z = (1,0)$. Für dieses Element ist $G_z = \{\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix},\ r \in \mathbb{Z}\}$ und X_z die Menge der Formen $f \in X$ mit erstem Koeffizienten $a = n$, also

$$X_z = \{nx^2 + bxy + \frac{b^2-D}{4n} y^2,\ b \in \mathbb{Z},\ b^2 \equiv D \pmod{4n}\} .$$

Da die Operation von $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \in G_z$ durch $b \to b + 2nr$ gegeben wird, ist $|X_z/G_z|$ gleich der rechten Seite der Formel (27), womit diese Formel auch bewiesen ist.

Um den Satz zu beweisen, müssen wir noch den Ausdruck in (27) explizit berechnen und das Ergebnis in (26) substituieren. Für $n = 2^{r_0}p_1^{r_1}\dots p_s^{r_s}$ (p_i ungerade) sieht man aus (27) leicht, daß

$$R^*(n) = R^*(2^{r_0})R^*(p_1^{r_1})\dots R^*(p_s^{r_s})$$

mit

$$R^*(p^r) = \#\{b \bmod p^r) \mid b^2 \equiv D \pmod{p^r)\} \qquad (p \neq 2) . \tag{30}$$

Da die rechte Seite von (25) auch multiplikativ ist, brauchen wir nur Primzahlpotenzen zu betrachten. Für $p \nmid D$ (und $r > 0$) ist die rechte Seite von (30) gleich 0 oder 2, je nachdem, ob D ein quadratischer Rest oder Nichtrest modulo p ist; für $p|D$ ist sie gleich 1 für $r = 1$ (es gibt nur die Lösung $b = 0$) und gleich 0 für $r > 1$ (da $p^2 \nmid D$). Wenn wir diese Werte in (26) substituieren, finden wir:

$$R(p^r) = \sum_{0 \leq s < \frac{r}{2}} 2 + \sum_{s = \frac{r}{2}} 1$$

$$= r + 1 = \sum_{0 \leq i \leq r} \chi_D(p^i) ,$$

falls $(\frac{D}{p}) = +1$,

$$R(p^r) = \sum_{0\le s<\frac{r}{2}} 0 + \sum_{s=\frac{r}{2}} 1$$

$$= \begin{cases} 1 & (r \text{ gerade}) \\ 0 & (r \text{ ungerade}) \end{cases} = \sum_{0\le i\le r} \chi_D(p^i) ,$$

falls $(\frac{D}{p}) = -1$, und

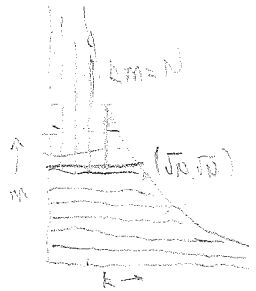
$$R(p^r) = \sum_{0\le s<\frac{r-1}{2}} 0 + \sum_{\frac{r-1}{2}\le s\le\frac{r}{2}} 1$$

$$= 1 = \sum_{0\le i\le r} \chi_D(p^i) ,$$

falls $p|D$. Somit ist (25) für $n = p^r$, p ungerade, in allen Fällen bewiesen. Den Beweis für $n = 2^r$, der ähnlich ist, überlassen wir dem Leser.

KOROLLAR: *Seien* D *und* χ_D *wie im Satz. Dann ist der Mittelwert der Gesamtdarstellungsanzahlen* $R(n)$ *gleich dem Wert der L-Reihe* $L(s,\chi_D)$ *an der Stelle* $s = 1$:

$$\lim_{N\to\infty} \left(\frac{1}{N} \sum_{n=1}^{N} R(n)\right) = L(1,\chi_D) . \tag{31}$$



Beweis: Nach (25) ist

$$\sum_{n=1}^{N} R(n) = \sum_{n\le N} \sum_{m|n} \chi_D(m)$$

$$= \sum_{km\le N} \chi_D(m)$$

$$= \sum_{m<\sqrt{N}} \chi_D(m) \cdot \sum_{k\le N/m} 1 + \sum_{k\le\sqrt{N}} \sum_{\sqrt{N}\le m\le\frac{N}{k}} \chi_D(m) .$$

(In der zweiten Summe, nämlich über die $m \ge \sqrt{N}$, ist wegen $km \le N$ automatisch $k \le \sqrt{N}$.) Es ist aber

$$\sum_{k\le N/m} 1 = [\frac{N}{m}] = \frac{N}{m} + O(1)$$

und

$$\sum_{\sqrt{N}\le m\le\frac{N}{k}} \chi_D(m) = O(1)$$

(da in jedem Intervall $(r-1)|D| < m \le r|D|$ die Summe von $\chi_D(m)$ wegen Satz 2, §5, verschwindet und die beiden Endintervalle

$\sqrt{N} \le m \le \left[\frac{\sqrt{N}}{|D|} + 1\right]|D|$ und $\left[\frac{N}{k|D|}\right]|D| < m \le \frac{N}{k}$ beschränkte Länge haben). Somit ist

$$\sum_{n\le N} R(n) = \sum_{m<\sqrt{N}} \chi_D(m)\cdot\left(\frac{N}{m} + O(1)\right) + \sum_{k\le\sqrt{N}} O(1)$$

$$= N \cdot \sum_{m=1}^{[\sqrt{N}]} \frac{\chi_D(m)}{m} + O(\sqrt{N}) ,$$

woraus die Behauptung folgt.

SATZ 4: *Sei* f *eine primitive, für* $D < 0$ *auch positiv definite, binäre quadratische Form der Diskriminante* D. *Dann wird der Mittelwert der Darstellungsanzahlen* $R(n,f)$ *gegeben durch*

$$\lim_{N\to\infty} \frac{1}{N}\left(\sum_{n=1}^{N} R(n,f)\right) = \begin{cases} \dfrac{2\pi}{w\sqrt{|D|}} , & \text{falls } D < 0 , \\ \dfrac{\log \varepsilon_0}{\sqrt{D}} , & \text{falls } D > 0 , \end{cases} \tag{32}$$

wo w *die durch (20) angegebene Ordnung von* U_f *und* ε_0 *die Grundeinheit von* f *bezeichnen.*

Beweis: Dieser Satz wird auf geometrische Weise bewiesen. Sei zunächst $D < 0$. Weil $|U_f| = w < \infty$ ist und U_f auf $\mathbb{Z}^2 - 0$ ohne Fixpunkte operiert, sind jeweils genau w Lösungen von (15) zueinander äquivalent, also die Anzahl $R(n,f)$ der inäquivalenten Lösungen gleich $\frac{1}{w}$ mal die Anzahl sämtlicher Lösungen:

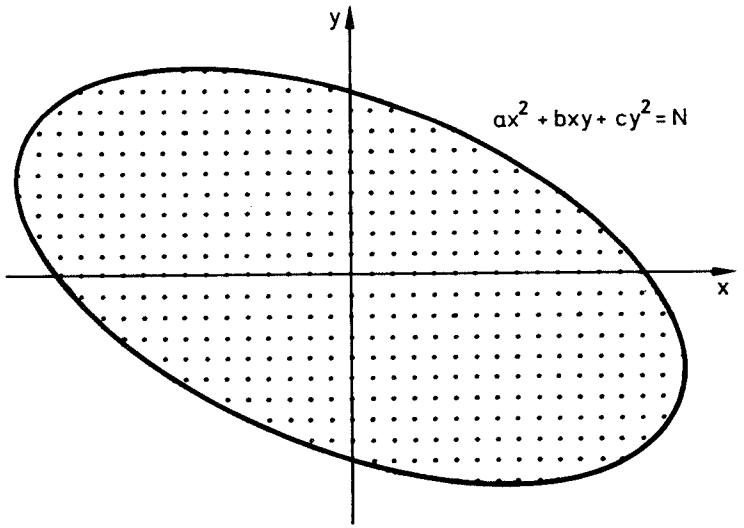
$$R(n,f) = \frac{1}{w} \#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 = n\} . \tag{33}$$

Somit ist

$$\sum_{n=1}^{N} R(n,f) = \frac{1}{w} \#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 \le N\} .$$

Die Ungleichung $ax^2 + bxy + cy^2 \le N$ beschreibt das Innere einer Ellipse (s. Bild). Dieses Gebiet hat den Flächeninhalt $\frac{2\pi N}{\sqrt{|D|}}$ (Aufgabe 6). Für N groß ist die Anzahl der Gitterpunkte in diesem Gebiet asymptotisch gleich dem Flächeninhalt (im Bild ist z.B. $a = 2$, $b = 3$, $c = 5$, $N = 400$, Anzahl der Gitterpunkte = 457, $\frac{2\pi N}{\sqrt{|D|}} = 451{,}4$), also

$$\lim_{N\to\infty} \frac{1}{N} \#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 \le N\} = \frac{2\pi}{\sqrt{|D|}} .$$



Für $D > 0$ ist U_f unendlich, das Argument also anders. Falls (x',y') eine Lösung von (15) ist, die aus (x,y) durch Anwendung der Substitution (4) entsteht, wobei $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ ein Automorphismus von f ist, der unter (23) der Zahl ε entspricht, so ist

$$x' + \frac{b - \sqrt{D}}{2a} y' = \varepsilon(x + \frac{b - \sqrt{D}}{2a} y) ,$$

wie man leicht ausrechnet. Mit den Abkürzungen

$$\theta = \frac{-b + \sqrt{D}}{2a} , \quad \theta' = \frac{-b - \sqrt{D}}{2a}$$

(so daß $ax^2 + bxy + cy^2 = a(x - \theta y)(x - \theta' y)$ gilt) folgt also

$$x' - \theta y' = \varepsilon(x - \theta y) , \; x' - \theta' y' = \varepsilon'(x - \theta' y) ,$$

$$\frac{x'-\theta'y'}{x'-\theta y'} = \varepsilon^{-2} \frac{x-\theta' y}{x-\theta y} .$$

Da jedes ε die Gestalt $\pm\varepsilon_0^n$ hat, können wir genau eine zu (x,y) äquivalente Lösung (x',y') finden, die die Bedingungen

$$x' - \theta y' > 0 , \; 1 < \frac{x'-\theta'y'}{x'-\theta y'} \le \varepsilon_0^2$$

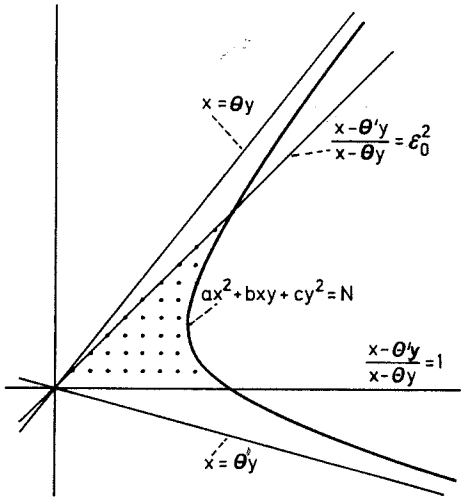
erfüllt. Das Analogon zu (33) für indefinite Formen ist also

$$R(n,f) = \#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 = n, \; x - \theta y > 0, \; 1 < \frac{x-\theta' y}{x-\theta y} \le \varepsilon_0^2\} .$$

Es folgt dann genau wie im Falle $D < 0$, daß der Limes in (32) gleich

$$\lim_{N\to\infty} \frac{1}{N} \cdot \text{Flächeninhalt von } \{(x,y) \in \mathbb{R}^2 \mid ax^2 + bxy + cy^2 \le N, \; x - \theta y > 0, \; 1 < \frac{x-\theta' y}{x-\theta y} \le \varepsilon_0^2\}$$

ist. Die Ungleichungen beschreiben einen Sektor einer Hyperbel (s. Bild, wo $a = 1$, $b = 3$, $c = -3$, $N = 100$, $\varepsilon_0 = \frac{5+\sqrt{21}}{2}$), dessen Flächen-



inhalt gleich $\frac{\log \varepsilon_0}{\sqrt{D}} N$ ist (Aufgabe 7). Hieraus folgt die Behauptung des Satzes wie im Fall $D < 0$. Die Existenz der Grundeinheit folgt ebenfalls: wäre nämlich $U_f = \{\pm 1\}$, so wäre im Widerspruch zu der Existenz des Mittelwertes von $R(n)$ der Mittelwert von $R(n,f)$ unendlich, da das Gebiet zwischen der Hyperbel $ax^2 + bxy + cy^2 = N$ und ihren Asymptoten unendlichen Flächeninhalt hat.

Aus den Tatsachen, daß $R(n)$ den endlichen Mittelwert $L(1,\chi_D)$ hat und daß der Mittelwert von $R(n,f)$ positiv und nur von der Diskriminante abhängig ist, erhalten wir neue Beweise für die Endlichkeit der Klassenzahl und für das Nichtverschwinden von $L(1,\chi_D)$. Aus Satz 4 und dem Korollar zu Satz 3 erhalten wir (mindestens für Fundamentaldiskriminanten; für den allgemeinen Fall s. Aufgabe 8) das erste Haupt-

ergebnis Dirichlets, nämlich eine Beziehung zwischen $h(D)$ und $L(1,\chi_D)$:

SATZ 5: *Sei* D *eine Diskriminante. Dann ist*

$$h(D) = \begin{cases} \frac{w\sqrt{|D|}}{2\pi} L(1,\chi_D), & \text{falls } D < 0, \\ \frac{\sqrt{D}}{\log \varepsilon_0} L(1,\chi_D), & \text{falls } D > 0. \end{cases} \tag{34}$$

Im nächsten Paragraphen werden wir $L(1,\chi_D)$ berechnen und somit die endgültige Klassenzahlformel erhalten.

Aufgaben:

1. Man zeige, daß es genau m Äquivalenzklassen von quadratischen Formen (bzw. $\phi(m)$ Äquivalenzklassen von primitiven quadratischen Formen) der Diskriminante m^2, $m > 0$ gibt. Wie ist die Klassifikation der Formen der Diskriminante 0? Wie groß ist die Automorphismengruppe einer Form, deren Diskriminante eine Quadratzahl bzw. gleich Null ist?

2. Was sind die Automorphismen der Formen $x^2 + y^2$, $x^2 + xy + y^2$, $2x^2 + 3xy + y^2$, $x^2 - 5y^2$, $2x^2 + 6xy + 3y^2$?

3. Wieviele Darstellungen als Summe von zwei Quadraten hat eine ungerade Zahl n? (Zunächst Primzahlen betrachten; man braucht $h(-4) = 1$.) Vgl. das letzte Beispiel in §2. Wie lautet das Ergebnis für n gerade?

4. Unter Benutzung von $h(5) = 1$ zeige man, daß die einzigen Lösungen von

$$t^2 - 5u^2 = 4$$

durch $u = \pm F_{2n}$, $t = \pm(F_{2n-1} + F_{2n+1})$ gegeben sind, wo F_n die n-te Fibonacci-Zahl bezeichnet ($F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$).

5. Man zeige, daß für $D > 0$ die Klassenzahlen im engeren und im weiteren Sinne durch $h_0(D) = h(D)$ oder $h_0(D) = \frac{1}{2} h(D)$ verknüpft sind, je nachdem, ob die Gleichung $t^2 - Du^2 = -4$ eine ganzzahlige Lösung hat oder nicht.

6. Man verifiziere die im Beweis von Satz 4 benutzten Beziehungen

$$\iint_{ax^2+bxy+cy^2 \le N} dx\,dy = \frac{2\pi N}{\sqrt{4ac-b^2}} \qquad (4ac > b^2,\ a > 0),$$

$$\iint_{\substack{x,y\ge 0 \\ y \le x(\varepsilon_0^2-1)/(\varepsilon_0^2\theta-\theta') \\ ax^2+bxy+cy^2 \le N}} dx\,dy = \frac{\log \varepsilon_0}{\sqrt{b^2-4ac}} N$$

($b^2 - 4ac > 0$, ε_0 und θ, θ' wie im Text).

7. Man berechne $\sum_{n=1}^{\infty} \frac{1}{9n^2-1}$, $\sum_{n=1}^{\infty} \frac{1}{16n^2-1}$, $\sum_{n=1}^{\infty} \frac{n}{(25n^2-1)(25n^2-4)}$.

8. Sei D ($\not\equiv 0$ und $\not\equiv 0$ oder $1 \pmod 4$) eine allgemeine Diskriminante; D läßt sich dann eindeutig als $D_0 r^2$ schreiben mit $r \in \mathbb{N}$ und D_0 eine Fundamentaldiskriminante. Sei

$$\chi_D(m) = \begin{cases} \chi_{D_0}(m), & \text{falls } (m,r) = 1 \\ 0 & \text{sonst} \end{cases}$$

der von χ_{D_0} induzierte Charakter. Man zeige:

a) Die Aussage von Satz 3 bleibt für zu r teilerfremde Zahlen richtig, d.h.

$$R_D(n) = \sum_{m \mid n} \chi_D(n) \qquad \left(= \sum_{m \mid n} \chi_{D_0}(n)\right) \quad \text{für } (n,r) = 1.$$

(Es ist hierbei gleichgültig, ob man die Darstellungen durch alle oder nur durch primitive Formen betrachtet, da eine zu r teilerfremde Zahl nicht durch eine imprimitive Form der Diskriminante D dargestellt werden kann.)

b) Das Korollar zu Satz 3 bleibt richtig, wenn man den Mittelwert nur über die n mit $(n,r) = 1$ bildet, d.h.

$$\lim_{N\to\infty} \left(\sum_{\substack{n=1 \\ (n,r)=1}}^{N} R_D(n) \Big/ \frac{\phi(r)}{r} N \right) = L(1,\chi_D).$$

Hinweis: Im Beweis des Korollars muß man $(k,r) = 1$, aber nicht $(m,r) = 1$ zu den Summationsbedingungen hinzunehmen, da $\chi_D(m)$ für $(m,r) > 1$ sowieso verschwindet. Es gilt außerdem

$$\sum_{\substack{k \le \frac{N}{m} \\ (k,r)=1}} 1 = \frac{\phi(r)}{r} \frac{N}{m} + O(1).$$

c) Satz 4 bleibt ebenfalls richtig, wenn man den Mittelwert über die zu r teilerfremden Zahlen bildet, weil in jedem großen Gebiet der Ebene die Dichte der Zahlenpaare (x,y) mit $(f(x,y),r) = 1$ gleich $\frac{\phi(r)}{r}$ ist.

Hinweis: Für $p|r$ und $f(x,y) = ax^2 + bxy + cy^2$ eine primitive Form der Diskriminante D können a und c nicht beide durch p teilbar sein; ist etwa a zu p teilerfremd und $p \neq 2$, so folgt aus $4af(x,y) \equiv (2ax+by)^2 \pmod p$, daß

$$\#\{(x,y) \bmod p \,|\, p \nmid f(x,y)\} = p(p-1) .$$

d) Formel (34) (Satz 5) bleibt für Nichtfundamentaldiskriminanten richtig. Folglich sind die Klassenzahlen von $D = D_0 r^2$ und D_0 durch die Relation

$$h(D) = \frac{\gamma_{D_0}(r)}{\nu_r} h(D_0)$$

verknüpft. Hierbei ist

$$\gamma_{D_0}(r) = r \prod_{p|r} \left(1 - \frac{\chi_{D_0}(p)}{p}\right)$$

und ν_r der Index von U_D in U_{D_0} ($U_D = \{(t,u) \mid t^2 - Du^2 = 4\}$ mit dem Multiplikationsgesetz (19)), also $\nu_r = 1$ für $D < 0$ (außer im Falle $D_0 = -3$ bzw. -4 und $r > 1$, wo $\nu_r = 3$ bzw. 2) und

$$\nu_r = \min \{n \,|\, n > 0,\ u_n \equiv 0 \pmod r\}$$

für $D > 0$, wobei $\frac{t_n + u_n\sqrt{D_0}}{2} = \left(\frac{t_0+u_0\sqrt{D_0}}{2}\right)^n$ mit (t_0,u_0) = kleinste positive Lösung der Pellschen Gleichung (1).

Bemerkung: Teil a) der Aufgabe gibt den Wert von $R_D(n)$ für $(n,r) = 1$ an. Das allgemeine Ergebnis, das sich ebenfalls aus (27) ableiten läßt, lautet wie folgt: Ist (r^2,n) kein Quadrat, so ist $R_D(n) = 0$. Ist $(r^2,n) = s^2$, also $n = n's^2$ und $D = D's^2$ mit $(n', \frac{D'}{D_0}) = 1$, so ist $R_D(n) = \gamma_{D'}(s) \cdot \sum_{m|n'} \chi_{D'}(m)$ (siehe etwa F. Hirzebruch, D. Zagier, *Invent. math. 36* (1976), S. 69-70, Proposition 2).

§9 Die Berechnung von $L(1,\chi)$ und die Klassenzahlformeln

Wir haben in §8 gesehen, wie man die Bestimmung der Klassenzahl binärer quadratischer Formen auf die Berechnung von $L(1,\chi)$ für reelle Charaktere $\chi = \chi_D$ zurückführen kann. In diesem Paragraphen werden wir $L(1,\chi)$ für beliebige Dirichletsche Charaktere $\chi \neq \chi_0$ berechnen. Wir haben schon bewiesen, daß dieser Wert endlich und von Null verschieden ist.

Sei also χ ein von dem Hauptcharakter verschiedener Dirichletscher Charakter. Wir setzen voraus, daß χ primitiv ist. (Wenn nämlich χ von einem Charakter χ_1 induziert wird, gibt es eine einfache Beziehung zwischen $L(1,\chi)$ und $L(1,\chi_1)$, da die L-Reihen $L(s,\chi)$ und $L(s,\chi_1)$ sich nur in endlich vielen Faktoren der Euler-Produkte unterscheiden.) Um $L(1,\chi)$ zu berechnen, machen wir Gebrauch von der *Gaußschen Summe*

$$(1) \qquad G = \sum_{n=1}^{N} \chi(n)\, e^{2\pi i n/N} .$$

Die Eigenschaften von G, die wir brauchen, sind in dem folgenden Hilfssatz zusammengestellt.

HILFSSATZ 1: *Sei χ ein primitiver Dirichletscher Charakter (mod N) und G durch (1) definiert. Dann gilt*

a) $$\sum_{n=1}^{N} \chi(n)\, e^{2\pi i k n/N} = \overline{\chi(k)} G \quad \textit{für alle} \quad k \in \mathbb{Z},$$

b) $$|G| = \sqrt{N} .$$

Beweis: a) ist leicht, falls $(k,N) = 1$, denn in diesem Fall ist

$$\begin{aligned} \sum_{n (\mathrm{mod}\ N)} \chi(n)\, e^{2\pi i n k/N} &= \sum_{n (\mathrm{mod}\ N)} \chi(nk^{-1}) e^{2\pi i n/N} \\ &= \sum_{n (\mathrm{mod}\ N)} \overline{\chi(k)}\, \chi(n)\, e^{2\pi i n/N} \\ &= \overline{\chi(k)} G , \end{aligned}$$

wobei k^{-1} eine Zahl mit $k \cdot k^{-1} \equiv 1 \pmod N$ bezeichnet. Sei jetzt $(k,N) = d > 1$; dann ist $\chi(k) = 0$ und wir müssen zeigen, daß $\sum \chi(n) e^{2\pi i k n/N}$ auch 0 ist. Mit $k_1 = k/d$, $N_1 = N/d$ ist

$$\sum_{n (\mathrm{mod}\ N)} \chi(n)\, e^{2\pi i n k/N} = \sum_{n (\mathrm{mod}\ N)} \chi(n)\, e^{2\pi i n k_1/N_1}$$

$$= \sum_{n_1 \pmod{N_1}} e^{2\pi i n_1 k_1/N_1} \Big[\sum_{\substack{n \pmod N \\ n \equiv n_1 \pmod{N_1}}} \chi(n) \Big],$$

da $e^{2\pi i n k_1/N_1}$ nur von dem Wert von $n \pmod{N_1}$ abhängt. Wir behaupten, daß die innere Summe verschwindet. Wir können nämlich eine ganze Zahl c finden mit

$$(c,N) = 1 \ , \ c \equiv 1 \pmod{N_1} \ , \ \chi(c) \neq 1$$

(sonst würde χ auf dem Kern von $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N_1\mathbb{Z})^\times$ immer gleich 1 sein, so daß χ über $(\mathbb{Z}/N_1\mathbb{Z})^\times$ faktorisieren würde, was der Primitivität widerspräche). Dann ist, analog zum Beweis von Satz 2, §5,

$$(1 - \chi(c)) \sum_{\substack{n \pmod N \\ n \equiv n_1 \pmod{N_1}}} \chi(n) = \sum_{\substack{n \pmod N \\ n \equiv n_1 \pmod{N_1}}} \chi(n) - \sum_{\substack{n \pmod N \\ n \equiv n_1 \pmod{N_1}}} \chi(nc) = 0 ,$$

da $nc \pmod N$ über dieselbe Menge läuft wie $n \pmod N$; wegen $1 - \chi(c) \neq 0$ ist dann die Summe Null.

Wir benutzen a), um b) zu beweisen:

$$|G|^2 = G\overline{G} = G \sum_{k=1}^{N} \overline{\chi(k)}\, e^{-2\pi i k/N}$$

$$= \sum_{k=1}^{N} \sum_{n=1}^{N} \chi(n)\, e^{2\pi i k n/N}\, e^{-2\pi i k/N}$$

$$= \sum_{n=1}^{N} \chi(n) \sum_{k \pmod N} e^{2\pi i k(n-1)/N} .$$

Die innere Summe ist für $n = 1$ offensichtlich gleich N, während sie für $n \neq 1$ verschwindet (wenn man nämlich k durch $k + 1$ ersetzt, wird sie mit $e^{2\pi i (n-1)/N} \neq 1$ multipliziert); es ist also

$$|G|^2 = \chi(1) \cdot N = N .$$

Aus b) folgt insbesondere, daß $G \neq 0$ ist; wir können also die Formel in a) durch G teilen und beide Seiten konjugieren, um

$$\chi(k) = \frac{1}{G} \sum_{n=1}^{N} \overline{\chi}(n)\, e^{-2\pi i n k/N} \tag{2}$$

zu erhalten. Es ist diese Beziehung, die die Bedeutung der Gaußschen Summe erklärt, weil sie es ermöglicht, die periodische Funktion

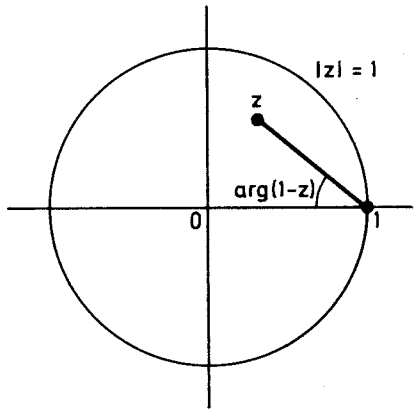
$k \mapsto \chi(k)$ als Linearkombination der einfacheren periodischen Funktionen $k \mapsto e^{2\pi i k n/N}$ zu schreiben.

Wir brauchen noch einen Hilfssatz.

HILFSSATZ 2: *Für* $0 < \theta < 2\pi$ *ist*

$$\sum_{n=1}^{\infty} \frac{e^{in\theta}}{n} = -\log(2 \sin \tfrac{\theta}{2}) + i(\tfrac{\pi}{2} - \tfrac{\theta}{2}) . \tag{3}$$

Beweis: Die Summe $\sum_{n=1}^{\infty} z^n/n$ konvergiert für $|z| \leq 1$, $z \neq 1$ nach $-\log(1-z)$, wobei derjenige Zweig des Logarithmus zu wählen ist, der auf der positiven reellen Achse reell ist. Ein Bild zeigt, daß $1 - z$ für $|z| < 1$ immer ein Argument zwischen $-\frac{\pi}{2}$ und $+\frac{\pi}{2}$ hat; daher



müssen wir den Zweig von $\log(1-z)$ wählen, dessen Imaginärteil zwischen diesen Grenzen liegt. Für $0 < \theta < 2\pi$ ist $\sin \frac{\theta}{2} > 0$ und $|\frac{\pi}{2} - \frac{\theta}{2}| < \frac{\pi}{2}$, also

$$\sum e^{in\theta}/n = -\log(1 - e^{i\theta})$$

$$= -\log\Big(-e^{\frac{i\theta}{2}}(e^{\frac{i\theta}{2}} - e^{-\frac{i\theta}{2}})\Big)$$

$$= -\log\Big(-e^{\frac{i\theta}{2}}(2i \sin \tfrac{\theta}{2})\Big)$$

$$= -\log\Big(e^{-\frac{i\pi}{2} + \frac{i\theta}{2}} \cdot 2 \sin \tfrac{\theta}{2}\Big)$$

$$= -\log(2 \sin \tfrac{\theta}{2}) + i(\tfrac{\pi}{2} - \tfrac{\theta}{2}) .$$

Mit den Gleichungen (2) und (3) können wir leicht $L(1,\chi)$ bestimmen:

$$L(1,\chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k} = \frac{1}{G} \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{N-1} \overline{\chi}(n)\, e^{-2\pi i n k/N}$$

(wegen $\overline{\chi}(N) = 0$ können wir $n = N$ weglassen)

$$= \frac{1}{G} \sum_{n=1}^{N-1} \overline{\chi}(n) \sum_{k=1}^{\infty} \frac{e^{-2\pi i k n/N}}{k}$$

$$= \frac{1}{G} \sum_{n=1}^{N-1} \overline{\chi(n)} \left(-\log(2 \sin \tfrac{\pi n}{N}) - i(\tfrac{\pi}{2} - \tfrac{\pi n}{N}) \right)$$

(wir haben hier die komplex konjugierte Form von (3) benutzt). Wegen $\sum_{n=1}^{N-1} \overline{\chi(n)} = 0$ kann man die Terme $-\log 2$ und $-i\frac{\pi}{2}$ in den eckigen Klammern weglassen. Wir haben also bewiesen:

SATZ 1: *Sei* χ *ein primitiver Dirichletscher Charakter* (mod N), $N > 1$. *Dann ist*

$$L(1,\chi) = -\frac{1}{G} \sum_{n=1}^{N-1} \overline{\chi}(n) \log \sin \frac{\pi n}{N} + \frac{i\pi}{N\overline{G}} \sum_{n=1}^{N-1} \overline{\chi}(n) n \,. \tag{4}$$

Wir betrachten jetzt den Fall, daß χ reell ist, also $\chi = \chi_D$ und $N = |D|$ mit einer Fundamentaldiskriminante D. Wegen

$$\overline{G} = \sum_{n (\mathrm{mod}\ N)} \overline{\chi(n)}\, e^{-2\pi i n/N} = \sum_{n (\mathrm{mod}\ N)} \chi(n)\, e^{-2\pi i n/N}$$

$$= \sum_{n (\mathrm{mod}\ N)} \chi(-n)\, e^{2\pi i n/N} = \chi(-1) G$$

ist dann G reell oder rein imaginär, je nachdem, ob $\chi(-1)$ gleich $+1$ oder -1 ist; nach (5.9) wissen wir, daß das wiederum davon abhängt, ob $D > 0$ oder $D < 0$. Aus Hilfssatz 1, b) erhalten wir

$$G = \begin{cases} \pm \sqrt{D}\,, & \text{falls } D > 0\,, \\ \pm i\sqrt{|D|}\,, & \text{falls } D < 0\,. \end{cases} \tag{5}$$

Die Bestimmung des Vorzeichens in dieser Gleichung ist eine der wichtigsten Episoden in der Geschichte der Zahlentheorie gewesen und hat Gauß (der in seinem Leben mehrere Beweise fand) einige Jahre gekostet; die Antwort lautet

$$G = \begin{cases} + \sqrt{D}\,, & \text{falls } D > 0 \\ + i\sqrt{|D|}\,, & \text{falls } D < 0\,. \end{cases} \tag{6}$$

Wir werden das nicht beweisen, da es für den Zweck der Bestimmung von $L(1,\chi_D)$ und $h(D)$ völlig ausreicht, G nur bis aufs Vorzeichen zu kennen - wir wissen ja ohnehin, daß beide Größen positiv sind.

Weil $L(1,\chi)$ für χ reell sicherlich auch reell ist, G aber nach (5) entweder reell oder rein imaginär, muß in jedem Fall eine der beiden Summen in (4) identisch verschwinden - die erste, falls $\chi(-1) = -1$, die zweite, falls $\chi(-1) = 1$ (vgl. auch Aufgabe 1). Somit erhalten wir aus (4) und (6) das Ergebnis:

SATZ 2: *Sei* D *eine Fundamentaldiskriminante. Dann ist für* $D < 0$

$$L(1,\chi_D) = -\frac{\pi}{|D|^{3/2}} \sum_{n=1}^{|D|-1} \chi_D(n) n \tag{7}$$

und für $D > 0$

$$L(1,\chi_D) = -\frac{1}{\sqrt{D}} \sum_{n=1}^{D-1} \chi_D(n) \log \sin \frac{\pi n}{D}\,. \tag{8}$$

In Verbindung mit Satz 5, §8, liefern diese Formeln endlich den gesuchten elementaren Ausdruck für die Klassenzahl:

SATZ 3: *Sei* D *eine Fundamentaldiskriminante. Für* $D < 0$ *ist*

$$h(D) = -\frac{w/2}{|D|} \sum_{n=1}^{|D|-1} \chi_D(n) n\,, \tag{9}$$

wo w *durch (8.20) gegeben wird. Für* $D > 0$ *ist*

$$h(D) = -\frac{1}{\log \varepsilon_0} \sum_{n=1}^{D-1} \chi_D(n) \log \sin \frac{\pi n}{D}\,, \tag{10}$$

wobei $\varepsilon_0 > 1$ *die Grundeinheit ist.*

Es sei nochmals betont, daß diese Formeln zwar richtig sind, hier aber nur bis auf das Vorzeichen bewiesen worden sind. Wenn man direkt - d.h. ohne analytische Methoden und ohne Satz 3 - zeigen könnte, daß die Summen in den Gleichungen (7) - (10) negativ sind, dann würde aus $L(1,\chi) > 0$ bzw. $h(D) > 0$ folgen, daß die Minuszeichen in diesen Gleichungen richtig sind, womit man auch noch den Beweis für (6) (die Bestimmung des Vorzeichens von G) hätte. Bisher hat aber niemand einen solchen Beweis gefunden*

---

* Allerdings ist kürzlich ein Beweis von (9) gefunden worden, der zwar den Hauptsatz über Darstellungen durch quadratische Formen (Satz 3, §8) benutzt, aber keinen Gebrauch von unendlichen Reihen oder von Grenzverfahren macht (H. Orde, On Dirichlet's class number formula, J. London Math. Soc. 18 (1978) 409 - 420).

Mit Satz 3 ist unser Ziel erreicht. Wir werden die gewonnenen Klassenzahlformeln jetzt weiter diskutieren. Zunächst geben wir einige Beispiele:

D = -3: Hier ist w = 6, also nach (9)

$$h(-3) = -\frac{3}{3}\sum_{n=1}^{2}\chi_{-3}(n)n = -(1-2) = 1 .$$

D = -4: Hier ist w = 4, also

$$h(-4) = -\frac{2}{4}\sum_{n=1}^{3}\chi_{-4}(n)n = -\frac{1}{2}(1-3) = 1 .$$

Für D < -4 ist w = 2, also

$$h(-7) = -\frac{1}{7}(1+2-3+4-5-6) = 1 ,$$

$$h(-8) = -\frac{1}{8}(1+3-5-7) = 1 ,$$

$$h(-11) = -\frac{1}{11}(1-2+3+4+5-6-7-8+9-10) = 1 ,$$

$$h(-15) = -\frac{1}{15}(1+2+4-7+8-11-13-14) = 2 .$$

Das letzte Beispiel zeigt, daß h(D) nicht immer = 1 ist. Weiteres Rechnen gibt

$$h(-19) = 1,\ h(-20) = 2,\ h(-23) = 3,\ h(-24) = 2 .$$

Wenn wir diese Werte angucken, stellen wir fest, daß h(D) immer gerade ist, sobald D zwei verschiedene Primzahlen enthält. Das ist eine allgemeine Tatsache: mit Hilfe der "Geschlechtertheorie" von Gauß werden wir später (§12) sehen, daß, für D eine Fundamentaldiskriminante (positiv oder negativ),

(11) $\qquad h(D)$ ungerade $\Longleftrightarrow$ D ist Primdiskriminante

(d.h. $D = -4, +8, -8$, oder $D = \pm p \equiv 1 \pmod 4$), während die Klassenzahl einer Fundamentaldiskriminante mit t verschiedenen Primfaktoren durch 2^{t-1} teilbar ist.

Die Rechnung mit (10) ist etwas umständlicher. Wir können (10) umschreiben in die Form

$$\varepsilon_0^{h(D)} = \prod_{n=1}^{D-1}\left(\sin\frac{\pi n}{D}\right)^{-\chi_D(n)}$$

$$(12)\qquad = \frac{\prod\limits_{\substack{0<n<D\\ \chi_D(n)=-1}} \sin\frac{\pi n}{D}}{\prod\limits_{\substack{0<n<D\\ \chi_D(n)=1}} \sin\frac{\pi n}{D}} .$$

Für D = 5 ist z.B. $\varepsilon_0 = \frac{3+\sqrt{5}}{2}$ (da t = 3, u = 1 die kleinste Lösung der Pellschen Gleichung $t^2 - 5u^2 = 4$ in positiven Zahlen ist), und die rechte Seite von (12) gleich

$$\frac{\sin\frac{2\pi}{5}\sin\frac{3\pi}{5}}{\sin\frac{\pi}{5}\sin\frac{4\pi}{5}} = \left(\frac{\sin\frac{2\pi}{5}}{\sin\frac{\pi}{5}}\right)^2 = (2\cos\tfrac{\pi}{5})^2 = (\tfrac{1+\sqrt{5}}{2})^2 = \frac{3+\sqrt{5}}{2} ,$$

also h(5) = 1.

Wegen der Formel

$$L(1,\chi) = -\frac{1}{G}\sum_{n=1}^{N-1}\overline{\chi}(n)\log(1-\eta^n) \qquad (\eta = e^{2\pi i/N}) ,$$

die der Ausgangspunkt für unseren Beweis von Satz 1 war, können wir für D > 0 Formel (10) auch durch

$$h(D) = \frac{-1}{\log\varepsilon_0}\sum_{n=1}^{D-1}\chi_D(n)\log(1-\eta^n)$$

ersetzen, d.h.

$$(13)\qquad \varepsilon_0^{h(D)} = \prod_{n=1}^{D-1}(1-\eta^n)^{-\chi_D(n)} = \frac{\prod\limits_{\substack{0<n<D\\ \chi_D(n)=-1}}(1-\eta^n)}{\prod\limits_{\substack{0<n<D\\ \chi_D(n)=1}}(1-\eta^n)} ,$$

eine Formel, die fürs Rechnen vielleicht geeigneter ist. Für D = 8 finden wir z.B.

$$\varepsilon_0 = 3+\sqrt{8} ,\ \eta = e^{2\pi i/8} = \frac{1+i}{\sqrt{2}} ,\ \text{also}$$

$$(3+\sqrt{8})^{h(8)} = \frac{(1-\eta^3)(1-\eta^5)}{(1-\eta)(1-\eta^7)} = \frac{2-\eta^3-\bar{\eta}^3}{2-\eta-\bar{\eta}} = \frac{2+\sqrt{2}}{2-\sqrt{2}} = 3+\sqrt{8}$$

und daher h(8) = 1.

Was kann man über die Ausdrücke sagen, die auf der rechten Seite von (9) bzw. (10) stehen? Wie schon erwähnt, hat bisher niemand direkt nachweisen können, daß sie positiv sind. Dagegen kann man elementar zeigen, daß sie ganze Zahlen darstellen. Für D > 0 folgt das aus der Kreisteilungstheorie, mit deren Hilfe man nachweisen kann, daß die

rechte Seite von (13) eine Zahl von der Gestalt $\frac{t+u\sqrt{D}}{2}$ mit $t^2 - u^2D = 4$ ist, also auf jeden Fall eine Potenz von ε_0 ist (siehe Aufgabe 6). Für $D < 0$ kann man noch elementarer zeigen, daß die rechte Seite von (9) ganz ist. Sei z.B. $D = -p < -3$ mit p prim (also $p \equiv 3 \pmod 4$); dann ist die rechte Seite von (9) gleich

$$(14) \qquad \frac{1}{p}\,(\sum N - \sum R)\ ,$$

wobei N über alle quadratischen Nichtreste und R über alle quadratischen Reste von p im Intervall $[0,p]$ läuft. Es ist

$$\sum N + \sum R = \sum_{n=1}^{p-1} n = \frac{p(p-1)}{2} \equiv 0 \pmod p$$

$$2\sum R \equiv \sum_{n=1}^{p-1} n^2 = \frac{p(p-1)(2p-1)}{6} \equiv 0 \pmod p\ ,$$

und somit (14) eine ganze Zahl. Die Positivität von (14) bedeutet, daß die quadratischen Nichtreste im Durchschnitt größer sind als die quadratischen Reste. Wir werden jetzt eine verwandte Tatsache beweisen, ebenfalls mit Hilfe von (9): es gibt mehr quadratische Reste als quadratische Nichtreste zwischen 0 und $\frac{p}{2}$. Dies folgt aus

SATZ 4: *Für $D < -4$, D eine Fundamentaldiskriminante, gilt*

$$(15) \qquad h(D) = \frac{1}{2-\chi_D(2)} \sum_{0<k<\frac{|D|}{2}} \chi_D(k)\ ;$$

d.h. es gibt stets mehr Zahlen in dem Intervall $[0,\frac{1}{2}|D|]$ mit $\chi_D(k) = +1$ als mit $\chi_D(k) = -1$, und der Überschuß ist gleich $h(D)$, $2h(D)$ oder $3h(D)$ je nachdem, ob $D \equiv 1 \pmod 8$, $D \equiv 0 \pmod 4$ oder $D \equiv 5 \pmod 8$ ist (vgl. (5.8b)).

Beweis: Wir nehmen an, daß D ungerade ist (für D gerade s. Aufgabe 2). Sei

$$Q = \sum_{n=1}^{|D|-1} \chi_D(n)n\ .$$

Je nachdem, ob n gerade oder ungerade ist, können wir n als $2k$ mit $0 < k < \frac{|D|}{2}$ oder als $2k - |D|$ mit $\frac{|D|}{2} < k < |D|$ schreiben, also gilt

$$Q = \sum_{0<k<\frac{|D|}{2}} \chi_D(2k)\cdot 2k + \sum_{\frac{|D|}{2}<k<|D|} \chi_D(2k-|D|)(2k-|D|)$$

$$= \sum_{0<k<\frac{|D|}{2}} \chi_D(2k)\cdot 2k + \sum_{\frac{|D|}{2}<k<|D|} \chi_D(2k)(2k-|D|)$$

$$= 2\sum_{0<k<|D|} \chi_D(2k)k - |D| \sum_{\frac{|D|}{2}<k<|D|} \chi_D(2k)$$

$$= 2\chi_D(2)\,Q - |D|\,\chi_D(2) \sum_{\frac{|D|}{2}<k<|D|} \chi_D(k)\ .$$

Somit ist

$$Q = \frac{|D|\chi_D(2)}{2\chi_D(2)-1} \sum_{\frac{|D|}{2}<k<|D|} \chi_D(k)$$

oder, da $\chi_D(2) = \pm 1$ und $\sum_{0<k<|D|} \chi_D(k) = 0$ ist,

$$Q = -\frac{|D|}{2-\chi_D(2)} \sum_{0<k<\frac{|D|}{2}} \chi_D(k)\ .$$

Nach (9) ist aber $h(D) = -\frac{1}{|D|}\,Q$, womit (15) für ungerade D bewiesen ist. Unser Argument zeigt auch, daß für $D \equiv 1 \pmod 4$ und $3 \nmid D$ die rechte Seite von (9) eine ganze Zahl darstellt.

Als Beispiel für (15) haben wir für $D = -19$ in $[0,9]$ die 6 Reste $1, 4, 5, 6, 7, 9$ und die 3 Nichtreste $2, 3, 8$; es ist also $h(-19) = \frac{1}{3}(6-3) = 1$. Für $D = -23$ sind in $[0,11]$ die 7 Reste $1, 2, 3, 4, 6, 8, 9$ und die 4 Nichtreste $5, 7, 10, 11$; es ist also $h(-23) = \frac{1}{1}(7-4) = 3$ und somit 23 die erste Primzahl $p \equiv 3 \pmod 4$ mit $h(-p) > 1$.

Zum Schluß wollen wir etwas über das Wachstum von $h(D)$ erzählen. Wir haben gesehen, daß $h(D) = 1$ ist für

$$D = -3, -4, -7, -8, -11, -19\ ;$$

man findet auch $h(D) = 1$ für

$$D = -43, -67, -163\ .$$

Gauß hat $h(D)$ ausgerechnet für $0 > D > -10.000$ (!) und keine anderen Fundamentaldiskriminanten gefunden mit $h(D) = 1$. Er vermutete, daß diese neun Zahlen die einzigen Fundamentaldiskriminanten mit der Klassenzahl 1 sind (wegen (11) kommen für $D < -8$ nur Primzahlen in Frage); weiter vermutete Gauß, daß

$$h(D) \to \infty \qquad \text{für} \quad D \to -\infty\ .$$

Diese letzte Behauptung wurde erst 1934 von Heilbronn bewiesen. Im darauf folgenden Jahr wurde das Ergebnis von Siegel wesentlich verschärft, indem er zeigte, daß für $\varepsilon > 0$

$$h(D) > C|D|^{\frac{1}{2}-\varepsilon} \qquad (D < 0) \tag{16}$$

gilt für ein geeignetes (von ε abhängiges) $C > 0$. Andererseits kann man aus dem Beweis von Satz 1, §8, leicht die umgekehrte Abschätzung

$$h(D) < C'|D|^{\frac{1}{2}+\varepsilon} \qquad (D < 0) \tag{17}$$

erhalten, also läßt sich dieser Satz auch so formulieren:

$$\lim_{D\to-\infty} \frac{\log h(D)}{\log |D|} = \frac{1}{2} .$$

Die erste Vermutung von Gauß wurde 1934 von Heilbronn und Linfoot "fast" beantwortet, indem sie zeigten, daß es höchstens eine Diskriminante $D < -163$ geben kann mit $h(D) = 1$. Lange Zeit wußte man über diese eventuell vorhandene "zehnte Diskriminante" nur, daß sie $< -5\cdot 10^9$ sein müßte. Erst 1952 bewies Heegner, daß es keine zehnte Diskriminante gibt; sein Beweis erschien anderen Mathematikern lückenhaft und wurde erst von Stark "rehabilitiert", und ein ganz anderer Beweis des Satzes wurde von Baker gegeben.

Für $D > 0$ bewies Siegel an Stelle von (16) und (17) die Ungleichungen

$$C\, D^{\frac{1}{2}-\varepsilon} < h(D) \log \varepsilon_0 < C'\, D^{\frac{1}{2}+\varepsilon} \qquad (D \to \infty) \tag{18}$$

oder

$$\lim_{D\to\infty} \frac{\log(h(D) \log \varepsilon_0)}{\log D} = \frac{1}{2} .$$

(Was Siegel wirklich bewies, war, daß

$$C'|D|^{-\varepsilon} < L(1,\chi_D) < C|D|^{\varepsilon}$$

für alle D gilt, was je nach dem Vorzeichen von D entweder (16) und (17) oder (18) ergibt.) Hieraus kann man aber nicht schließen, daß $h(D)$ nach Unendlich geht, da ε_0 im Vergleich zu D sehr groß sein kann (für $D = 97$ ist z.B. $\varepsilon_0 = 62809633 + 6377352\sqrt{97}$), und in der Tat lassen die tabellierten Werte (die schon Gauß bis 3000 berechnet hatte) vermuten, daß es unendlich viele Fundamentaldiskriminanten mit Klassenzahl 1 gibt. (Diese müssen nach (11) alle Primdiskriminanten sein.) Läßt man Nichtfundamentaldiskriminanten zu, so gibt es auf jeden Fall unendlich viele D mit $h(D) = 1$ (Aufgabe 5).

Obwohl man über das genaue Wachstum von $h(D)$ bzw. $h(D) \log \varepsilon_0$ nicht sehr viel mehr als (16) - (18) weiß, kann man für die *Mittelwerte* beweisen, daß sie sich so verhalten, als ob $h(D) \sim C|D|^{1/2}$ bzw. $h(D) \log \varepsilon_0 \sim CD^{1/2}$ wäre. Man hat nämlich für $N \to \infty$

$$\sum_{\substack{0>D>-N \\ D\equiv 0 \pmod 4}} h(D) \sim \frac{\pi}{42\,\zeta(3)} N^{3/2} ;$$

$$\sum_{\substack{0<D<N \\ D\equiv 0 \pmod 4}} h(D) \log \varepsilon_0 \sim \frac{\pi^2}{42\,\zeta(3)} N^{3/2} ,$$

wo $\zeta(3) = 1.20205...$ der Wert von $\zeta(s)$ an der Stelle $s = 3$ ist. Diese Beziehungen wurden von Gauß angegeben, ihre Beweise aber erst von Mertens bzw. Siegel veröffentlicht. (Die Bedingung $D \equiv 0 \pmod 4$ rührt daher, daß Gauß nur quadratische Formen $ax^2 + bxy + cy^2$ mit b gerade studierte. Für die Summen über alle D gelten ähnliche asymptotische Formeln mit 18 statt 42.)

Aufgaben:

1. Sei χ ein beliebiger (also nicht unbedingt reeller) Dirichletscher Charakter modulo N. Man zeige, daß die zweite Summe in (4) verschwindet, falls χ gerade ist (d.h. $\chi(-1) = 1$ und die erste, falls χ ungerade ist (also $\chi(-1) = -1$). Replace n by -n in the summation.

2. Man zeige, daß $\chi_D(k + \frac{1}{2}D) = -\chi_D(k)$ für $D \equiv 0 \pmod 4$ und beweise Satz 4 sowie die Formel $h(D) = \sum_{0<k<\frac{|D|}{4}} \chi_D(k)$ $(D < 0)$ für diesen Fall.

3. Man beweise (11) für negative Fundamentaldiskriminanten mit Hilfe von Satz 4 und Aufgabe 2.

4. Man rechne $h(D)$ für $-30 < D < 15$ aus.

5. Für $i \geq 0$ gilt $h(5^{2i+1}) = 1$. (Hinweis: Man verwende Aufgabe 8 d), §8.)

6. Sei p eine Primzahl $\equiv 1 \pmod 4$, $\eta = e^{2\pi i/p}$. Seien

$$\eta_R = \sum_R \eta^R , \quad \eta_N = \sum_N \eta^N$$

wobei $\sum_R$ bzw. $\sum_N$ Summen über alle quadratischen Reste bzw. Nichtreste bezeichnen. Dann ist nach (5)

$$\eta_R + \eta_N = \sum_{k=1}^{p-1} \eta^k = -1 \ , \quad \eta_R - \eta_N = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \eta^k = \pm\sqrt{p} \ .$$

Setzen wir jetzt für jede p-te Einheitswurzel $\zeta \neq 1$

$$F_R(\zeta) = \prod_R (1 - \zeta^R) \ ,$$

wobei R über alle quadratischen Reste (mod p) läuft. Man zeige

a) $F_R(\zeta) = \sum_{r=0}^{p-1} \alpha_r \zeta^r$ mit $\alpha_r \in \mathbb{Z}$.

b) Für $\left(\frac{k}{p}\right) = 1$ ist $F_R(\zeta^k) = F_R(\zeta)$, also $\alpha_{kr} = \alpha_r$ (hier braucht man die lineare Unabhängigkeit von $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, d.h. die Irreduzibilität des Kreisteilungspolynoms $x^{p-1} + x^{p-2} + \ldots + x + 1$). Es gibt also Zahlen $\alpha_R, \alpha_N \in \mathbb{Z}$ mit

$$\alpha_r = \alpha_R \quad \text{für} \quad \left(\frac{r}{p}\right) = 1 \ , \quad \alpha_r = \alpha_N \quad \text{für} \quad \left(\frac{r}{p}\right) = -1 \ .$$

c) Man schließe

$$F_R(\eta) = \frac{S \pm T\sqrt{p}}{2}$$

(mit $S = 2\alpha_0 - \alpha_R - \alpha_N$, $T = \alpha_R - \alpha_N \in \mathbb{Z}$) und

$$\prod_N (1 - \eta^N) = F_R(\eta^{N_0}) \qquad (N_0 \text{ irgendein Nichtrest})$$

$$= \frac{S \mp T\sqrt{p}}{2} \ .$$

d) Man zeige, daß

$$\prod_{k=1}^{p-1} (1 - \eta^k) = p$$

ist (etwa aus $\frac{x^p - 1}{x-1} = \prod_{k=1}^{p-1} (x - \eta^k)$), und folgere

$$S^2 - T^2 p = 4p \ , \quad S = pU \ , \quad T^2 - pU^2 = -4$$

mit $T, U \in \mathbb{Z}$ (die Pellsche Gleichung $x^2 - py^2 = -4$ hat also eine nichttriviale Lösung!) und

$$\frac{\prod_N (1 - \eta^N)}{\prod_R (1 - \eta^R)} = \frac{t + u\sqrt{p}}{2} \quad \text{mit} \quad t, u \in \mathbb{Z}, \ t^2 - u^2 p = 4, \ u \neq 0 \ .$$

§10 Quadratische Formen und quadratische Zahlkörper

In diesem Paragraphen stellen wir die Haupttatsachen über quadratische Körper zusammen und zeigen, wie die Theorie von binären quadratischen Formen (mindestens, falls die Diskriminante eine Grundzahl ist) mit der Theorie der Ideale in solchen Körpern äquivalent ist. In §11 werden diese Ideen weiterentwickelt, indem die im letzten Paragraphen bewiesenen Sätze über Darstellungsanzahlen vom Standpunkt der Arithmetik in quadratischen Körpern interpretiert werden.

Sei K ein *quadratischer Zahlkörper*, d.h. K enthält $\mathbb{Q}$ und $[K : \mathbb{Q}] = 2$. Dann kann man

$$K = \mathbb{Q}(\sqrt{d})$$

schreiben mit $d \in \mathbb{Z}$, d keine Quadratzahl. Da $\mathbb{Q}(\sqrt{f^2 d}) = \mathbb{Q}(f\sqrt{d}) = \mathbb{Q}(\sqrt{d})$ ist, können wir d als *quadratfrei* voraussetzen. Jede Zahl in K läßt sich eindeutig schreiben als $\alpha + \beta\sqrt{d}$, mit $\alpha, \beta \in \mathbb{Q}$.

Sei $\mathfrak{O} \subset K$ der Ring der *ganzen Zahlen*, d.h. derjenigen Zahlen, die eine Gleichung mit Koeffizienten aus $\mathbb{Z}$ und höchstem Koeffizienten 1 erfüllen. Es ist leicht, $\mathfrak{O}$ zu bestimmen: ist $x = \alpha + \beta\sqrt{d} \in K$, so ist

$$x^2 - sx + n = 0$$

mit

$$s = x + x' = \mathrm{Sp}(x) \quad \text{die } \textit{Spur} \text{ von } x \text{ und}$$

$$n = xx' = N(x) \quad \text{die } \textit{Norm} \text{ von } x;$$

dabei ist $x' = \alpha - \beta\sqrt{d}$ die *Konjugierte* von x. Es ist $x \in \mathfrak{O}$ genau dann, wenn s und n in $\mathbb{Z}$ sind, d.h.

$$2\alpha \in \mathbb{Z} \ , \quad \alpha^2 - \beta^2 d \in \mathbb{Z} \ .$$

Hieraus schließt man $2\beta \in \mathbb{Z}$ (denn $(2\beta)^2 d = (2\alpha)^2 - 4(\alpha^2 - \beta^2 d) \in \mathbb{Z}$ und d ist quadratfrei), also $\alpha = \frac{a}{2}$, $\beta = \frac{b}{2}$, $x = \frac{a + b\sqrt{d}}{2}$ mit $a, b \in \mathbb{Z}$, $a^2 - b^2 d \equiv 0 \pmod 4$. Ist $d \equiv 2$ oder $d \equiv 3 \pmod 4$, so ist diese Kongruenz nur erfüllt, wenn a und b gerade, also α und β in $\mathbb{Z}$ sind; ist $d \equiv 1 \pmod 4$, so ist die Kongruenz zu $a \equiv b \pmod 2$ äquivalent. Es ist also

$$(1) \qquad \mathfrak{O} = \begin{cases} \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\sqrt{d} \ , & \text{falls } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\frac{1+\sqrt{d}}{2} \ , & \text{falls } d \equiv 1 \pmod 4 \end{cases}$$

(die Bezeichnung $M = \mathbb{Z}x + \mathbb{Z}y$ bedeutet im Folgenden, daß x und y eine $\mathbb{Z}$-Basis für M bilden). Als *Diskriminante* D von K bezeichnet man das Quadrat der Determinante von $\begin{pmatrix}\alpha & \beta\\ \alpha' & \beta'\end{pmatrix}$, wo α, β eine Basis von $\mathfrak{O}$ bilden und α', β' die Konjugierten bezeichnen (eine andere Basiswahl ändert höchstens das Vorzeichen dieser Determinante). Mit der Basis (1) finden wir

$$D = \det\begin{pmatrix}1 & \sqrt{d}\\ 1 & -\sqrt{d}\end{pmatrix}^2 = (-2\sqrt{d})^2 = 4d$$

bzw.

$$D = \det\begin{pmatrix}1 & \frac{1+\sqrt{d}}{2}\\ 1 & \frac{1-\sqrt{d}}{2}\end{pmatrix}^2 = (-\sqrt{d})^2 = d\ ,$$

also

$$D = \begin{cases}4d, & \text{falls } d \equiv 2, 3 \pmod 4\ ,\\ d, & \text{falls } d \equiv 1 \pmod 4\ .\end{cases} \tag{2}$$

Somit sind die in §5 definierten Grundzahlen oder Fundamentaldiskriminanten ($\neq 1$) genau die Diskriminanten von quadratischen Zahlkörpern, und jeder solche Körper läßt sich eindeutig als $\mathbb{Q}(\sqrt{D})$, D = Grundzahl, schreiben.

Ein *Ideal* von $\mathfrak{O}$ ist eine Untergruppe $\mathfrak{a} \subset \mathfrak{O}$ mit $\mathfrak{O}\mathfrak{a} = \mathfrak{a}$, d.h.

$$\lambda \in \mathfrak{O}\ ,\ \alpha \in \mathfrak{a} \Rightarrow \lambda\alpha \in \mathfrak{a}\ . \tag{3}$$

Wir betrachten nur Ideale $\mathfrak{a} \neq \{0\}$. Ein solches hat endlichen Index in $\mathfrak{O}$; wir definieren die *Norm* $N(\mathfrak{a})$ als $[\mathfrak{O} : \mathfrak{a}]$, d.h. als die Ordnung der endlichen Gruppe $\mathfrak{O}/\mathfrak{a}$. Die *Diskriminante* $D(\mathfrak{a})$ wird definiert als $\det\begin{pmatrix}\alpha & \beta\\ \alpha' & \beta'\end{pmatrix}^2$, wo α, β eine beliebige Basis für $\mathfrak{a}$ ist; dann gilt $D(\mathfrak{O}) = D$ und

$$D(\mathfrak{a}) = N(\mathfrak{a})^2 D\ , \tag{4}$$

wie man mit elementarer linearer Algebra zeigt. Ist $\xi \in \mathfrak{O}$, $\xi \neq 0$, so ist

$$(\xi) = \{\lambda\xi \mid \lambda \in \mathfrak{O}\}$$

offenbar ein Ideal; wir nennen (ξ) das von ξ erzeugte *Hauptideal*. Ist α, β eine Basis von $\mathfrak{O}$, so ist $\alpha\xi$, $\beta\xi$ eine Basis für (ξ), und es folgt

$$D((\xi)) = \det\begin{pmatrix}\alpha\xi & \beta\xi\\ \alpha'\xi' & \beta'\xi'\end{pmatrix}^2 = (\xi\xi')^2\cdot(\alpha\beta' - \alpha'\beta)^2 = N(\xi)^2 D\ ,$$

also nach (4)

$$N((\xi)) = |N(\xi)|\ . \tag{5}$$

Sind $\mathfrak{a}, \mathfrak{b}$ zwei Ideale, so ist das *Produktideal* $\mathfrak{a}\mathfrak{b}$ durch

$$\mathfrak{a}\mathfrak{b} = \{\sum_{i=1}^{r} a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b},\ r \in \mathbb{N}\}$$

erklärt (d.h. als das kleinste Ideal, das alle Produkte ab mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ enthält). Es gilt

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})\ . \tag{6}$$

Für ein Ideal $\mathfrak{a}$ und sein *Konjugiertes*

$$\mathfrak{a}' = \{x' \mid x \in \mathfrak{a}\}$$

besteht die Relation

$$\mathfrak{a}\mathfrak{a}' = (N(\mathfrak{a})) \tag{7}$$

(das Produkt von $\mathfrak{a}$ und $\mathfrak{a}'$ ist gleich dem von der Norm von $\mathfrak{a}$ erzeugten Hauptideal).

Es ist nützlich, auch mit *gebrochenen Idealen* zu arbeiten, d.h. mit Untergruppen von K (statt von $\mathfrak{O}$), die endlich erzeugt sind und (3) erfüllen. Für jedes gebrochene Ideal $\mathfrak{a}$ gibt es eine natürliche Zahl n, so daß $n\mathfrak{a}$ ein *ganzes Ideal*, d.h. ein Ideal im früheren Sinne ist (man wählt eine Basis α, β von $\mathfrak{a}$ und ein n mit $n\alpha \in \mathfrak{O}$, $n\beta \in \mathfrak{O}$); dann definiert man die Norm von $\mathfrak{a}$ durch

$$N(\mathfrak{a}) = \frac{1}{n^2} N(n\mathfrak{a}) \in \mathbb{Q}$$

(das ist unabhängig von der Wahl von n). Die Diskriminante $D(\mathfrak{a})$, das Konjugierte $\mathfrak{a}'$ und das Produkt von zwei gebrochenen Idealen werden wie oben definiert und die Beziehungen (4) und (6) gelten nach wie vor. Ist $\xi \in K$, $\xi \neq 0$, so ist $(\xi) = \{\lambda\xi \mid \lambda \in \mathfrak{O}\}$ ein gebrochenes Ideal und erfüllt (5). Ab jetzt bedeutet "Ideal" immer "gebrochenes Ideal" ($\neq \{0\}$), falls nicht ausdrücklich von ganzen Idealen gesprochen wird.

Die Multiplikation von Idealen erweitert die von Zahlen: sind $\xi, \eta \in K$, so ist $(\xi)(\eta) = (\xi\eta)$. Infolgedessen gilt für Zahlen $\xi, \eta \in K$

$$\xi|\eta \quad (\text{d.h. } \xi^{-1}\eta \in \mathfrak{O}) \Leftrightarrow (\eta) \subset (\xi)$$
$$\Leftrightarrow \text{es gibt ein ganzes Ideal } \mathfrak{c} \text{ mit } (\eta) = (\xi)\mathfrak{c}\ .$$

Wir können also den Begriff der Teilbarkeit von Zahlen auf Ideale übertragen, indem wir sagen, daß das Ideal $\mathfrak{a}$ das Ideal $\mathfrak{b}$ *teilt* (in Zeichen $\mathfrak{a}|\mathfrak{b}$), falls $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ gilt mit einem ganzen Ideal $\mathfrak{c}$; dies ist äquivalent zu $\mathfrak{b} \subset \mathfrak{a}$. Für eine Zahl $\xi \in K$ und ein gebrochenes Ideal $\mathfrak{a}$ gilt

$$(8) \qquad \mathfrak{a}|(\xi) \iff \xi \in \mathfrak{a} \ .$$

Wir schreiben häufig ξ anstatt (ξ) für das von ξ erzeugte Hauptideal. Der Witz an den Idealen ist, daß jedes Ideal eindeutig als Produkt von Primidealen geschrieben werden kann (ein *Primideal* ist ein ganzes Ideal, das nur durch $\mathfrak{O}$ und durch sich selbst teilbar ist), während die analoge Behauptung für Zahlen i.a. nicht stimmt. Z.B. hat die Zahl 10 im Körper $\mathbb{Q}(\sqrt{6})$ die zwei Zerlegungen

$$(9) \qquad 10 = (4 + \sqrt{6})\cdot(4 - \sqrt{6}) = 2\cdot 5 \ ,$$

wobei alle vier Faktoren $4 + \sqrt{6}$, $4 - \sqrt{6}$, 2, 5 in dem Sinne prim sind, daß sie nur als $x\cdot y$ $(x, y \in \mathfrak{O})$ geschrieben werden können, wenn x oder y eine *Einheit* ist (d.h. eine ganze Zahl, deren Inverses auch in $\mathfrak{O}$ liegt). Die Eindeutigkeit der Primzerlegung bei Idealen rührt daher, daß zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ stets einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches haben, es gilt nämlich

$$\mathfrak{c}|\mathfrak{a} \text{ und } \mathfrak{c}|\mathfrak{b} \iff \mathfrak{c}|\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \ ,$$

$$\mathfrak{a}|\mathfrak{c} \text{ und } \mathfrak{b}|\mathfrak{c} \iff \mathfrak{a} \cap \mathfrak{b}|\mathfrak{c} \ ,$$

also $(\mathfrak{a},\mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$, $[\mathfrak{a},\mathfrak{b}] = \mathfrak{a} \cap \mathfrak{b}$. Die Notwendigkeit, Ideale einzuführen, sieht man hierdurch auch: die Menge $(\xi) \cap (\eta)$ der gemeinsamen Vielfachen zweier Zahlen ξ und η ist offenbar ein Ideal, im allgemeinen aber kein Hauptideal. In (9) gilt z.B.

$$(10) \qquad \begin{aligned} 2 &= \mathfrak{p}^2 \\ 5 &= \mathfrak{q}\,\mathfrak{q}' \\ 4 + \sqrt{6} &= \mathfrak{p}\,\mathfrak{q} \\ 4 - \sqrt{6} &= \mathfrak{p}\,\mathfrak{q}' \end{aligned}$$

mit den Primidealen

$$(11) \qquad \begin{aligned} \mathfrak{p} &= (2,\ 4 + \sqrt{6}) = \mathbb{Z}\cdot 2 + \mathbb{Z}\cdot\sqrt{6} \ , \\ \mathfrak{q} &= (5,\ 4 + \sqrt{6}) = \mathbb{Z}\cdot 5 + \mathbb{Z}\cdot(4 + \sqrt{6}) \ , \end{aligned}$$

also $(5) \cap (4+\sqrt{6}) = 5\mathfrak{p} \neq$ Hauptideal. Die Frage, wie sich eine natürliche Zahl in Primideale zerlegt (z.B., warum in (10) die Zahl 2 das Quadrat eines Primideals ist, während 5 das Produkt von einem Primideal mit seinem Konjugierten ist) wird in §11 behandelt werden. Wir wollen jetzt zeigen, was Ideale mit quadratischen Formen zu tun haben. Vorerst eine Definition.

Definition: Zwei gebrochene Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen *äquivalent*, falls ein $\xi \in K$, $\xi \neq 0$, mit

$$(12) \qquad \mathfrak{a} = (\xi)\mathfrak{b}$$

existiert. Sie heißen *äquivalent im engeren Sinne*, falls es eine Zahl $\xi \in K$ mit $N(\xi) > 0$ gibt, so daß (12) gilt.

Anders ausgedrückt: die gebrochenen Ideale bilden eine Gruppe unter der Multiplikation (das inverse Ideal existiert immer, denn nach (7) ist $\mathfrak{a}^{-1} = N(\mathfrak{a})^{-1}\,\mathfrak{a}'$), und die Äquivalenzklassen (bzw. Äquivalenzklassen im engeren Sinn) von Idealen bilden den Quotienten dieser Gruppe nach der Untergruppe der Hauptideale (ξ) (bzw. der Hauptideale im engeren Sinne, d.h. der Ideale (ξ) mit $N(\xi) > 0$). Für einige Körper - z.B. $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-3})$ - ist jedes Ideal (sogar im engeren Sinn) ein Hauptideal, also zu $\mathfrak{O}$ äquivalent; in diesen Körpern ist es also gleichgültig, ob wir mit Idealen oder nur mit Zahlen arbeiten, und die Primzahlzerlegung in $\mathfrak{O}$ ist eindeutig. In anderen Körpern - z.B. in unserem Beispiel $\mathbb{Q}(\sqrt{6})$ oben - gibt es Ideale, die keine Hauptideale sind, und wir haben zwar eindeutige Primideal-, aber nicht eindeutige Primzahlzerlegung. Es wird sich aber herausstellen, daß es immer nur endlich viele Äquivalenzklassen von Idealen gibt, so daß die Abweichung von der eindeutigen Primzahlzerlegung nicht zu groß ist.

Bemerkung: Ist $d < 0$, d.h. $K = \mathbb{Q}(\sqrt{d})$ ein imaginär-quadratischer Körper, so ist für $\xi \in K$ die Konjugierte ξ' in K gleich der komplex konjugierten Zahl $\overline{\xi}$ (da $\sqrt{d}$ rein imaginär ist), also $N(\xi) = \xi\xi' = \xi\overline{\xi} = |\xi|^2$ für $\xi \neq 0$ automatisch positiv. Hier fallen also die beiden Äquivalenzbegriffe zusammen. Es gibt auch positive d mit der Eigenschaft, daß in $\mathbb{Q}(\sqrt{d})$ äquivalente Ideale stets äquivalent im engeren Sinne sind, aber es gibt ebenfalls reelle quadratische Körper, die Hauptideale haben, welche nicht als (ξ) mit $\xi\xi' > 0$ geschrieben werden können, und in diesem Fall zerfällt jede Äquivalenzklasse von Idealen in genau zwei Äquivalenzklassen im engeren Sinne.

Wir kommen jetzt zu der Korrespondenz zwischen Idealen und Formen. Ist $\mathfrak{a}$ ein (ganzes oder gebrochenes) Ideal, so ist für $\xi \in \mathfrak{a}$ wegen $\mathfrak{a} | (\xi)$

$$N(\mathfrak{a}) \mid N(\xi) \qquad (\xi \in \mathfrak{a}) , \tag{13}$$

d.h. die Funktion

$$\phi: \mathfrak{a} \to \mathbb{Q} , \qquad \phi(\xi) = \frac{\xi\xi'}{N(\mathfrak{a})} ,$$

nimmt Werte in $\mathbb{Z}$ an. Sei α, β eine Basis für $\mathfrak{a}$; dann ist $\mathfrak{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta \cong \mathbb{Z}^2$ und wir können ϕ als Funktion f auf $\mathbb{Z}^2$ auffassen:

$$f(x,y) = \phi(x\alpha + y\beta) = \frac{(x\alpha+y\beta)(x\alpha'+y\beta')}{N(\mathfrak{a})} . \tag{14}$$

Das ist eine binäre quadratische Form:

$$f(x,y) = ax^2 + bxy + cy^2 , \; a = \frac{\alpha\alpha'}{N(\mathfrak{a})} , \; b = \frac{\alpha\beta'+\alpha'\beta}{N(\mathfrak{a})} , \; c = \frac{\beta\beta'}{N(\mathfrak{a})} ; \tag{15}$$

für ihre Diskriminante finden wir

$$b^2 - 4ac = \frac{(\alpha\beta'+\alpha'\beta)^2 - 4(\alpha\alpha')(\beta\beta')}{N(\mathfrak{a})^2} = \frac{(\alpha\beta'-\alpha'\beta)^2}{N(\mathfrak{a})^2}$$
$$= \frac{D(\mathfrak{a})}{N(\mathfrak{a})^2} = D$$

nach Formel (4). Außerdem ist $a = N(\alpha)/N(\mathfrak{a})$ nach (13) ganz und ebenso c, und es folgt dann aus $b^2 - 4ac = D \in \mathbb{Z}$, daß auch b ganz ist. Also ist f eine binäre quadratische Form mit ganzzahligen Koeffizienten und Diskriminante D. Wenn wir eine andere Basis (α_1, β_1) von $\mathfrak{a}$ wählen, dann sind α_1, β_1 und α, β durch eine ganzzahlige Matrix $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ mit $ps - qr = \pm 1$ miteinander verknüpft, und die Form f_1, die man aus ϕ mit Hilfe der Basis α_1, β_1 erhält, ergibt sich aus (15), indem wir x, y durch $px + qy, rx + sy$ ersetzen. Da wir in §8 die Äquivalenz von Formen nur mit Hilfe von Matrizen der Determinante $+1$ definierten, wollen wir durch eine zusätzliche Forderung an unsere Basen erreichen, daß nur solche Matrizen bei Basiswechseln auftreten. Wir nennen eine Basis α, β von $\mathfrak{a}$ *orientiert*, falls $\frac{\alpha'\beta-\alpha\beta'}{\sqrt{D}} > 0$ ist (das ist sinnvoll, weil $(\frac{\alpha'\beta-\alpha\beta'}{\sqrt{D}})^2 = \frac{D(\mathfrak{a})}{D} = N(\mathfrak{a})^2$ reell und positiv ist); dann hat die Matrix eines Basiswechsels zwischen orientierten Basen stets die Determinante $+1$. Es folgt, daß die durch (15) definierte binäre quadratische Form bis auf Äquivalenz (im Sinne von §8) nur von $\mathfrak{a}$ und nicht von der Basiswahl abhängt,

falls man nur orientierte Basen α, β zuläßt. Wenn wir $\mathfrak{a}$ durch $(\lambda)\mathfrak{a}$ ersetzen, wobei $\lambda \in K$ und $N(\lambda) > 0$ ist, dann ist $(\lambda\alpha, \lambda\beta)$ eine orientierte Basis für $(\lambda)\mathfrak{a}$ und $N((\lambda)\mathfrak{a}) = |N(\lambda)| \, N(\mathfrak{a}) = N(\lambda)N(\mathfrak{a})$; somit ist die dem Ideal $(\lambda)\mathfrak{a}$ zugeordnete Form

$$(x,y) \mapsto \frac{N(x\lambda\alpha+y\lambda\beta)}{N((\lambda)\mathfrak{a})} = \frac{N(\lambda)\,N(x\alpha+y\beta)}{N(\lambda)\,N(\mathfrak{a})} = \frac{N(x\alpha+y\beta)}{N(\mathfrak{a})}$$

mit f identisch. Wir haben also auf eindeutige Weise *jeder Idealklasse im engeren Sinne eine Äquivalenzklasse von binären quadratischen Formen der Diskriminante* D *zugeordnet* (positiv-definit, falls $D < 0$).

Wir zeigen jetzt, daß diese Zuordnung bijektiv ist. Sei

$$f(x,y) = ax^2 + bxy + cy^2 \; ; \quad a, b, c \in \mathbb{Z} , \; b^2 - 4ac = D , \tag{16}$$

eine quadratische Form der Diskriminante D, positiv-definit falls $D < 0$. Weil D eine Fundamentaldiskriminante ist, ist $(a,b,c) = 1$. Wir setzen zunächst $a > 0$ voraus. Seien

$$w = \frac{b+\sqrt{D}}{2a} , \; w' = \frac{b-\sqrt{D}}{2a} \tag{17}$$

die Wurzeln der quadratischen Gleichung $aw^2 - bw + c = 0$, und

$$\mathfrak{a} = \mathbb{Z} + \mathbb{Z}w . \tag{18}$$

Wir behaupten, daß $\mathfrak{a}$ ein gebrochenes Ideal ist. In der Tat: ist $\lambda = \frac{u+v\sqrt{D}}{2} \in \mathfrak{D}$ $(u, v \in \mathbb{Z}, \; u \equiv vD \pmod 2)$ und $\alpha = x + yw \in \mathfrak{a}$, so ist

$$\lambda\alpha = (\tfrac{u+v\sqrt{D}}{2})(x + \tfrac{yb+y\sqrt{D}}{2a})$$
$$= \tfrac{xu}{2} + \tfrac{ybu}{4a} + \tfrac{yvD}{4a} + (\tfrac{xv}{2} + \tfrac{ybv}{4a} + \tfrac{uy}{4a})\sqrt{D}$$
$$= (x\,\tfrac{u-vb}{2} - yvc) + (xva + y\,\tfrac{u+vb}{2})\,w ,$$

was in $\mathbb{Z} + \mathbb{Z}w$ liegt ($b^2 \equiv D \pmod{4a} \Rightarrow b \equiv D \pmod 2 \Rightarrow u \equiv vD \equiv vb \pmod 2$). Wegen $\frac{w-w'}{\sqrt{D}} > 0$ ist die Basis $1, w$ orientiert. Die Diskriminante von $\mathfrak{a}$ ist

$$D(\mathfrak{a}) = \det \left(\begin{smallmatrix} 1 & w \\ 1 & w' \end{smallmatrix}\right)^2 = (w-w')^2 = D/a^2 ,$$

und wir erhalten nach (4)

$$N(\mathfrak{a}) = \frac{1}{a} .$$

Die $\mathfrak{a}$ zugeordnete quadratische Form (15) ist also gegeben durch

$$(x,y) \mapsto \frac{N(x+yw)}{N(\mathfrak{a})} = \frac{x^2 + \frac{b}{a}xy + \frac{c}{a}y^2}{\frac{1}{a}} = f(x,y) .$$

Wir haben damit ein Ideal konstruiert mit f als zugeordneter quadratischer Form. Ist umgekehrt $\mathfrak{a}$ ein Ideal mit orientierter Basis α, β und $\alpha\alpha' > 0$, so ist mit a, b, c wie in (15)

$$\frac{b+\sqrt{D}}{2a} = \frac{\alpha\beta'+\alpha'\beta+N(\mathfrak{a})\sqrt{D}}{2\alpha\alpha'}$$

$$= \frac{\alpha\beta'+\alpha'\beta+(\alpha'\beta-\alpha\beta')}{2\alpha\alpha'} = \frac{\beta}{\alpha} ,$$

also $\mathbb{Z}' + \mathbb{Z}\,\frac{b+\sqrt{D}}{2a} = \mathbb{Z} + \mathbb{Z}\,\frac{\beta}{\alpha} = (\alpha^{-1})\mathfrak{a}$ zu $\mathfrak{a}$ im engeren Sinn äquivalent.

Für Formen (16) mit $a < 0$ (dann muß nach Voraussetzung $D > 0$ sein) nehmen wir anstatt (18) das Ideal $\mathbb{Z}\lambda + \mathbb{Z}\lambda w$, wobei $\lambda \in \mathbb{Q}(\sqrt{D})$ eine Zahl mit negativer Norm ist (etwa $\lambda = \sqrt{D}$). Dann ist λ, λw eine orientierte Basis, und die diesem Ideal zugeordnete Form ist wieder f. Umgekehrt liefert jedes Ideal $\mathfrak{a}$ mit orientierter Basis α, β und $\alpha\alpha' < 0$ eine Form (16) mit $a < 0$, für die das Ideal $\mathbb{Z}\lambda + \mathbb{Z}\lambda w$ im engeren Sinne zu $\mathfrak{a}$ äquivalent ist. Wir haben also folgenden Satz bewiesen.

SATZ: *Sei $D \neq 1$ eine Fundamentaldiskriminante und $K = \mathbb{Q}(\sqrt{D})$. Dann gibt es eine bijektive Korrespondenz zwischen den Äquivalenzklassen von binären quadratischen Formen der Diskriminante D (positiv-definit, falls $D < 0$) und den Äquivalenzklassen im engeren Sinn von Idealen von K. Diese Korrespondenz ordnet dem Ideal $\mathbb{Z}\alpha + \mathbb{Z}\beta$ (mit $\frac{\alpha'\beta-\alpha\beta'}{\sqrt{D}} > 0$) die Form (15) zu und ordnet der Form $ax^2 + bxy + cy^2$ das (gebrochene) Ideal $\mathbb{Z}\cdot\lambda + \mathbb{Z}\cdot\frac{b+\sqrt{D}}{2a}\,\lambda$ zu, wobei $\lambda \in K$ so gewählt wird, daß $N(\lambda)$ dasselbe Vorzeichen wie a hat. Somit ist die Anzahl der Äquivalenzklassen von Idealen im engeren Sinne gleich der in §8 definierten Klassenzahl $h(D)$ und insbesondere endlich.*

Aufgaben:

1. Man beweise die im Text behaupteten Aussagen (4), (6), (7).

2. Man verifiziere (10) und (11) (d.h., daß die als $(2,4+\sqrt{6})$ bzw. $(5,4+\sqrt{6})$ definierten Ideale wirklich die gegebenen Basen besitzen) und auch, daß $\mathfrak{p}$ und $\mathfrak{q}$ Primideale sind und $\mathfrak{q} \neq \mathfrak{q}'$. (Hinweis: ein Ideal, dessen Norm eine Primzahl ist, ist prim. Warum?)

3. Man zeige, daß eine Matrix, die den Übergang zwischen zwei orientierten Basen beschreibt, Determinante $+1$ hat.

4. Man zeige, daß es eine Bijektion zwischen den Äquivalenzklassen von Idealen in K (nicht im engeren Sinne) und den Äquivalenzklassen im weiteren Sinne (vgl. (8.14)) von quadratischen Formen der Diskriminante D gibt.

5. a) Für $D \equiv 0$ oder $1 \pmod 4$, D kein Quadrat, sei

$$\mathfrak{O}_D = \{\tfrac{a+b\sqrt{D}}{2} \mid a, b \in \mathbb{Z},\ a \equiv bD \pmod 2\} .$$

Schreiben wir $D = D_0 r^2$ mit D_0 eine Fundamentaldiskriminante und $r \geq 1$, so ist $\mathfrak{O}_D$ ein Unterring vom Index r im Ring $\mathfrak{O} = \mathfrak{O}_{D_0}$ der ganzen Zahlen des quadratischen Körpers $K = \mathbb{Q}(\sqrt{D})$. Mit den naheliegenden Definitionen von Idealen, Hauptidealen, Äquivalenz usw. in $\mathfrak{O}_D$ gibt es dann eine bijektive Korrespondenz zwischen den Äquivalenzklassen von $\mathfrak{O}_D$-Idealen im engeren Sinne und den Äquivalenzklassen (ebenfalls im engeren Sinne) von quadratischen Formen der Diskriminante D (positiv definit, falls $D < 0$).

b) Sei K ein quadratischer Körper der Diskriminante D_0. Für jeden *Modul* $M \subset K$ (d.h. Untergruppe von Rang 2) ist der *Multiplikator*

$$\mathfrak{O}(M) = \{x \in K \mid xM \subseteq M\}$$

gleich dem in a) definierten Ring $\mathfrak{O}_D$ für ein geeignetes $D = D_0 r^2$. Im engeren Sinne äquivalente Moduln (d.h. Moduln M und ξM mit $\xi \in K$, $N(\xi) > 0$) haben denselben Multiplikator, und es gibt eine bijektive Korrespondenz zwischen den Äquivalenzklassen von Moduln M mit $\mathfrak{O}(M) = \mathfrak{O}_D$ und den Äquivalenzklassen von *primitiven* quadratischen Formen der Diskriminante D (positiv-definit, falls $D < 0$).

Bemerkung: Mit Hilfe dieser Korrespondenz kann man einen rein algebraischen Beweis der in Aufgabe 8d), §8, auf analytischem Weg bewiesenen Beziehung $h(D) = \frac{\gamma_{D_0}(r)}{\nu_r}\, h(D_0)$ geben. Dafür werden durch $M \mapsto \mathfrak{O}M$ ($\mathfrak{O} = \mathfrak{O}_{D_0}$ der Ring der ganzen Zahlen in K) Abbildungen

$$\{\text{Moduln mit Multiplikator } \mathfrak{O}_D\} \to \{\text{(gebrochene) } \mathfrak{O}\text{-Ideale}\} ,$$

$$\{\text{Hauptmoduln } \xi\mathfrak{O}_D,\ \xi \in K^*\} \to \{\text{Hauptideale } \xi\mathfrak{O},\ \xi \in K^*\}$$

definiert, welche surjektiv sind und Kerne der Ordnungen $[(\mathfrak{O}/r\mathfrak{O})^* : (\mathfrak{O}_D/r\mathfrak{O})^*]$ bzw. $[\mathfrak{O}^* : \mathfrak{O}_D^*]$ haben, wobei R^* die Gruppe der invertierbaren Elemente eines Rings R bezeichnet. (Eine Skizze des Beweises wird in den Aufgaben 6-11, §7, Kap.II, des am Ende dieses Kapitels zitierten Buchs von Borewicz und

Šafarevič gegeben.) Es ist aber $[\mathfrak{O}^* : \mathfrak{O}_D^*] = \nu_r$ und $[(\mathfrak{O}/r\mathfrak{O})^* : (\mathfrak{O}_D/r\mathfrak{O})^*] = \frac{|(\mathfrak{O}/r\mathfrak{O})^*|}{|(\mathbb{Z}/r\mathbb{Z})^*|} = \gamma_{D_0}(r)$ (s. Aufgabe 2, §11).

§11 Die Zetafunktion eines quadratischen Körpers

Die Bedeutung der Riemannschen Zetafunktion kommt von der Formel

$$(1) \qquad \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1} \qquad (\sigma > 1) ,$$

die die analytische Formulierung der Tatsache ist, daß sich jede natürliche Zahl auf eindeutige Weise als Produkt von Primzahlen darstellen läßt. Für einen quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{D})$ wissen wir, daß die entsprechende Behauptung nicht für Zahlen, wohl aber für Ideale gilt, und es ist daher sehr natürlich, dem Körper K die Dirichletsche Reihe

$$(2) \qquad \zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

zuzuordnen, wobei die Summe über alle ganzen Ideale $\mathfrak{a}$ $(\neq 0)$ von K läuft (ob diese Reihe einen nichtleeren Konvergenzbereich hat, sei für den Augenblick dahingestellt). Die Funktion (2) nennt man die *Dedekindsche Zetafunktion;* sie kann für einen beliebigen Zahlkörper definiert werden und hat viele Eigenschaften mit der Riemannschen Zetafunktion (dem Spezialfall $K = \mathbb{Q}$) gemeinsam: Konvergenzabszisse $\sigma_0 = 1$, einfacher Pol bei $s = 1$ als einzige Singularität, Funktionalgleichung unter $s \to 1 - s$, rationale Werte für $s = 0, -1, -2, \ldots$ usw. Mit demselben Beweis wie für (1) schließt man aus der eindeutigen Primidealzerlegung, daß

$$(3) \qquad \zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

(Produkt über alle Primideale $\mathfrak{p}$), falls eine der beiden Seiten der Gleichung absolut konvergiert.

Wir zeigen jetzt, daß das für $\sigma > 1$ der Fall ist. Jedes Primideal teilt eine natürliche Primzahl p (denn $\mathfrak{p}$ teilt die natürliche Zahl $N(\mathfrak{p})$, also muß $\mathfrak{p}$, da es prim ist, einen der Primteiler von $N(\mathfrak{p})$ teilen). Dann folgt aus $\mathfrak{p}|p$, daß

$$N(\mathfrak{p}) \mid N((p)) = pp' = p^2 ,$$

also $N(\mathfrak{p}) = p$ oder p^2 ($N(\mathfrak{p}) = 1$ scheidet offensichtlich aus). Wenn

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

die Primidealzerlegung von p (d.h. von dem Hauptideal (p)) in $\mathfrak{O}$ ist, so ist

$$p^2 = N(p) = N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_r) ,$$

also $r \leq 2$, und es gibt zwei Möglichkeiten: $p = \mathfrak{p}_1\mathfrak{p}_2$ mit $\mathfrak{p}_1$, $\mathfrak{p}_2$ prim und $N(\mathfrak{p}_i) = p$ oder $p = \mathfrak{p}$ mit $N(\mathfrak{p}) = p^2$. Somit ist

$$\prod_{\mathfrak{p}|p} (1-N(\mathfrak{p})^{-s})^{-1} = (1-p^{-s})^{-1} \text{ oder } (1-p^{-s})^{-2} \text{ oder } (1-p^{-2s})^{-1} ;$$

also

$$\prod_{\mathfrak{p}|p} |1 - N(\mathfrak{p})^{-s}|^{-1} \leq (1 - p^{-\sigma})^{-2} ,$$

und $\prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$ wird im Absolutbetrag durch $\zeta(\sigma)^2$ abgeschätzt, was für $\sigma > 1$ endlich ist; das Produkt (3) und somit auch die Summe (2) sind daher absolut konvergent für $\sigma > 1$.

Wir können (2) auch schreiben als

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{F(n)}{n^s}$$

mit

$$F(n) = \#\{\mathfrak{a} \mid \mathfrak{a} \text{ ein ganzes Ideal, } N(\mathfrak{a}) = n\} ,$$

$\zeta_K(s)$ ist also eine gewöhnliche Dirichletsche Reihe, deren Koeffizienten uns sagen, wie oft eine gegebene Zahl als Norm eines Ideals auftritt. Wir behaupten, daß *die Zahl* $F(n)$ *gleich der Zahl* $R(n)$ *der nichtäquivalenten Darstellungen von* n *durch quadratische Formen der Diskriminante* D *ist.* In der Tat, seien $A_1, \ldots, A_h$ ($h = h(D)$) die Äquivalenzklassen von Idealen im engeren Sinn, und sei für jedes i

$$\zeta(A_i,s) = \sum_{\substack{\mathfrak{a} \in A_i \\ \mathfrak{a} \text{ ganz}}} \frac{1}{N(\mathfrak{a})^s}$$

die *Zetafunktion der Idealklasse* A_i; dann gilt offenbar

$$\zeta_K(s) = \sum_{i=1}^{h(D)} \zeta(A_i,s)$$

und

$$\zeta(A_i,s) = \sum_{n=1}^{\infty} \frac{F_i(n)}{n^s} ,$$

$$F_i(n) = \#\{\mathfrak{a} \in A_i \mid \mathfrak{a} \text{ ganz}, N(\mathfrak{a}) = n\} .$$

Wir behaupten, daß $F_i(n)$ gleich der Darstellungsanzahl $R(n,f_i)$ der Zahl n durch die Form f_i ist, welche unter der in §10 konstruierten Korrespondenz der Idealklasse A_i entspricht. Daraus wird unsere erste Behauptung wegen $R(n) = \sum_{i=1}^{h} R(n,f_i)$ und $F(n) = \sum_{i=1}^{h} F_i(n)$ folgen.

Wir machen eine Vorbemerkung. Wegen (10.7) ist die Idealklasse A^{-1} der Inversen von Elementen aus einer Idealklasse A gleich der Idealklasse A' der Konjugierten von Elementen aus A, also

$$\zeta(A^{-1},s) = \zeta(A',s) = \sum_{\substack{\mathfrak{a}\in A' \\ \mathfrak{a}\text{ ganz}}} \frac{1}{N(\mathfrak{a})^s}$$

$$= \sum_{\substack{\mathfrak{a}\in A \\ \mathfrak{a}\text{ ganz}}} \frac{1}{N(\mathfrak{a}')^s} = \zeta(A,s)$$

(das letzte wegen $N(\mathfrak{a}') = N(\mathfrak{a})$). Sei jetzt $\mathfrak{a}$ ein Ideal, A seine Idealklasse und f die entsprechende quadratische Form. Für $\mathfrak{b} \in A^{-1}$ ist $\mathfrak{ab}$ ein Hauptideal im engeren Sinne, also $\mathfrak{ab} = (\xi)$ mit $N(\xi) > 0$; umgekehrt liegt für $\xi \in K$ mit $N(\xi) > 0$ das gebrochene Ideal $\mathfrak{b} = (\xi)\mathfrak{a}^{-1}$ in A^{-1}. Das Ideal $\mathfrak{b}$ ist genau dann ganz, wenn $\mathfrak{a} \mid \xi$, d.h. wenn $\xi \in \mathfrak{a}$ gilt. Somit ist die Abbildung

$$\begin{aligned} \{\xi \in \mathfrak{a} \mid N(\xi) > 0\} &\to \{\mathfrak{b} \in A^{-1} \mid \mathfrak{b} \text{ ganz}\} \\ \xi &\mapsto (\xi)\mathfrak{a}^{-1} \end{aligned} \tag{4}$$

wohldefiniert und surjektiv. Was ist ihr Kern? Zwei Elemente ξ und ξ_1 haben genau dann dasselbe Bild, wenn $\xi_1 \mid \xi$ und $\xi \mid \xi_1$, also $\xi_1 = \varepsilon\xi$ ist mit $\varepsilon \in \mathfrak{O}$, $\varepsilon^{-1} \in \mathfrak{O}$ und $N(\varepsilon) = N(\xi_1)/N(\xi) > 0$. Somit liefert (4) eine Bijektion

$$\{\xi \in \mathfrak{a} \mid N(\xi) > 0\}/U_+ \xrightarrow{\sim} \{\mathfrak{b} \in A^{-1},\ \mathfrak{b} \text{ ganz}\} , \tag{5}$$

wobei

$$U_+ = \{\varepsilon \in \mathfrak{O} \mid \varepsilon^{-1} \in \mathfrak{O},\ N(\varepsilon) = 1\}$$

die Gruppe der Einheiten positiver Norm ist, die in der Gruppe

$$U = \{\varepsilon \in \mathfrak{O} \mid \varepsilon^{-1} \in \mathfrak{O}\}$$

aller Einheiten den Index 1 oder 2 hat. Unter der Korrespondez (5) ist

$$N(\mathfrak{b}) = N((\xi)\mathfrak{a}^{-1}) = N(\xi)\, N(\mathfrak{a})^{-1} .$$

Daher gilt

$$\begin{aligned} \zeta(A,s) &= \zeta(A^{-1},s) \\ &= \sum_{\substack{\mathfrak{b}\in A^{-1} \\ \mathfrak{b}\text{ ganz}}} \frac{1}{N(\mathfrak{b})^s} \\ &= \sum_{\substack{\xi\in\mathfrak{a}/U_+ \\ N(\xi)>0}} \frac{N(\mathfrak{a})^s}{N(\xi)^s} , \end{aligned}$$

also wegen (10.14)

$$\zeta(A,s) = \sum_{\substack{(x,y)\in\mathbb{Z}^2/U_+ \\ f(x,y)>0}} \frac{1}{f(x,y)^s} \tag{6}$$

wobei wir $\mathfrak{a}$ durch die Wahl einer orientierten Basis mit $\mathbb{Z}^2$ identifiziert haben; die induzierte Operation von U_+ auf $\mathbb{Z}^2$ ist dann genau die, unter der wir zwei Lösungen von $f(x,y) = n$ $(n \in \mathbb{N})$ in §8 als äquivalent erklärten. Die rechte Seite von (6) ist also gleich

$$\sum_{n=1}^{\infty} \frac{R(n,f)}{n^s} ,$$

und die Behauptung ist bewiesen.

Wir werden jetzt für die Zetafunktion von K einen elementaren Ausdruck geben; wegen (3) genügt es, für jede natürliche Primzahl p den Faktor $\prod_{\mathfrak{p}\mid p} (1 - N(\mathfrak{p})^{-s})^{-1}$ der Eulerschen Produkt-Entwicklung zu kennen. Wir müssen also untersuchen, wie sich eine Primzahl p in Primideale zerlegt.

Wir hatten schon überlegt, daß grundsätzlich zwei Fälle vorkommen können - das in $\mathbb{Z}$ prime Ideal $p\mathbb{Z}$ bleibt entweder in $\mathfrak{O}$ prim, also

$$p = \mathfrak{p} , \qquad N(\mathfrak{p}) = p^2 ,$$

(eine solche Primzahl p nennt man *träge*), oder es zerfällt in der Form

$$p = \mathfrak{p}_1\mathfrak{p}_2 , \ N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p .$$

Diesen Fall werden wir weiter unterteilen je nachdem, ob $\mathfrak{p}_1 = \mathfrak{p}_2$ ist, also

$$p = \mathfrak{p}^2 , \qquad N(\mathfrak{p}) = p$$

(eine solche Primzahl nennt man *verzweigt*), oder ob $\mathfrak{p}_1 \neq \mathfrak{p}_2$ (dann heißt p *zerlegt*). In beiden Fällen ist $\mathfrak{p}_2 = \mathfrak{p}_1'$ (das folgt aus der allgemeinen Beziehung $\mathfrak{a}' = N(\mathfrak{a})\,\mathfrak{a}^{-1}$). Welcher der drei Fälle vorliegt, hängt von dem Wert von $\chi_D(p)$ ab, wo D die Diskriminante von K und χ_D der in §5 definierte primitive Charakter ist:

SATZ 1: *Sei K ein quadratischer Körper und p eine rationale Primzahl. Dann wird die Zerlegung von p im Ring $\mathfrak{O}$ der ganzen Zahlen von K wie folgt gegeben:*

$$(7) \qquad p = \mathfrak{p}\mathfrak{p}' , \ \mathfrak{p} \neq \mathfrak{p}' \Leftrightarrow \chi_D(p) = 1 ,$$

$$(8) \qquad p = \mathfrak{p}^2 \Leftrightarrow \chi_D(p) = 0 ,$$

$$(9) \qquad p = \mathfrak{p} \Leftrightarrow \chi_D(p) = -1 .$$

KOROLLAR: *Die Zetafunktion von K hat die Zerlegung*

$$(10) \qquad \zeta_K(s) = \zeta(s)\, L(s,\chi_D) .$$

Die Anzahl der Darstellungen einer natürlichen Zahl n als Norm eines Ideals in $\mathfrak{O}$ ist gegeben durch

$$(11) \qquad F(n) = \sum_{m|n} \chi_D(m) .$$

Beweis: Sei $p \neq 2$ (für den Fall $p = 2$ siehe Aufgabe 1). Dann ist $\chi_D(p)$ gleich dem Legendre-Symbol $(\frac{D}{p})$.

Sei zunächst p eine verzweigte Primzahl, $p = \mathfrak{p}^2$, $\mathfrak{p} = \mathfrak{p}'$, $N(\mathfrak{p}) = p$. Wegen $\mathfrak{p}^2 \neq \mathfrak{p}$ gibt es eine Zahl $x = \frac{a+b\sqrt{D}}{2}$, die durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist. Dann ist x' durch $\mathfrak{p}' = \mathfrak{p}$ teilbar, also auch $a = x + x'$ und $b\sqrt{D} = x - x'$. Aber

$$\mathfrak{p}|a \Rightarrow p = \mathfrak{p}^2|a^2 \Rightarrow p|a ,$$

und

$$\mathfrak{p}|b\sqrt{D} \Rightarrow p = \mathfrak{p}^2|(b\sqrt{D})^2 = b^2D \Rightarrow p|b \text{ oder } p|D .$$

Da p nicht a *und* b teilen kann (sonst wäre ja x durch $p = \mathfrak{p}^2$ teilbar), folgt hieraus $p|D$, d.h. $\chi_D(p) = 0$.

Ist umgekehrt p ein Primteiler der Diskriminante, so ist p verzweigt: Da D oder $D/4$ quadratfrei ist, gilt $p^2 \nmid D$, d.h. $D = pD_1$ mit $p \nmid D_1$. Dann folgt aus

$$(\sqrt{D})^2 = (D) = (p)(D_1)$$

und $(p,D_1) = 1$, daß die Ideale (p) und (D_1) beide Quadrate sind. Somit ist (8) bewiesen.

Sei jetzt p zerlegt, also $p = \mathfrak{p}\mathfrak{p}'$ mit $\mathfrak{p}' \neq \mathfrak{p}$. Nach dem eben Bewiesenen teilt p die Diskriminante nicht. Da $N(\mathfrak{p}) = p$ prim ist, ist der Quotientenring $R = \mathfrak{O}/\mathfrak{p}$ von $\mathfrak{O}$ nach dem Ideal $\mathfrak{p}$ ein Körper der Ordnung p, und die Gruppe $R^\times$ der invertierbaren Elemente von R hat die Ordnung $p - 1$. Somit gilt $x^{p-1} = 1$ für jedes $x \in R$, $x \neq 0$, d.h.

$$x \in \mathfrak{O} , \ \mathfrak{p} \nmid x \Rightarrow x^{p-1} \equiv 1 \pmod{\mathfrak{p}}$$

(Analogon zum kleinen Fermatschen Satz). Da $p \nmid D$ und daher $\mathfrak{p} \nmid \sqrt{D}$ gilt, können wir diese Formel auf $x = \sqrt{D}$ anwenden und erhalten somit

$$D^{\frac{p-1}{2}} = (\sqrt{D})^{p-1} \equiv 1 \pmod{\mathfrak{p}} .$$

Für $a \in \mathbb{Z}$ ist aber $\mathfrak{p}|a$ zu $p|a$ äquivalent ($\mathfrak{p}|a \Rightarrow p = N(\mathfrak{p}) | N(a) = a^2 \Rightarrow p|a$), also gilt auch

$$D^{\frac{p-1}{2}} \equiv 1 \pmod{p} ,$$

was nach einem bekannten Kriterium zu $(\frac{D}{p}) = 1$ äquivalent ist.

Ist umgekehrt p eine Primzahl mit $(\frac{D}{p}) = 1$, so wählen wir eine Zahl $x \in \mathbb{Z}$ mit $x^2 \equiv D \pmod{p}$. Wäre $x - \sqrt{D}$ durch p teilbar, so müßte p auch das Konjugierte $x + \sqrt{D}$ und daher auch die Differenz $2\sqrt{D}$ dieser beiden Elemente teilen, im Widerspruch zu den Voraussetzungen $p \neq 2$ und $p \nmid D$. Es gilt also $p \nmid (x - \sqrt{D})$ und entsprechend $p \nmid (x + \sqrt{D})$. Andererseits ist das Produkt $(x - \sqrt{D})(x + \sqrt{D}) = x^2 - D$ dieser beiden Zahlen nach Voraussetzung durch p teilbar. Es folgt, daß p mindestens zwei Primidealfaktoren enthält. Da wir aber schon gesehen haben, daß $p = \mathfrak{p}^2 \Rightarrow \chi_D(p) = 0$, bleibt nur die Möglichkeit, daß p zerlegt ist. Damit ist (7) bewiesen.

Da es für die Primidealzerlegung von p sowie für den Wert von $\chi_D(p)$ jeweils genau drei Möglichkeiten gibt, ist (9) eine Konsequenz von (7) und (8). Damit ist Satz 1 (für $p \neq 2$) bewiesen.

Das Korollar ist jetzt leicht zu beweisen. Wegen der in §2 angegebenen Regel für die Multiplikation von Dirichletschen Reihen sind die Aussagen (10) und (11) äquivalent. Da $F(n)$ und $\sum_{m|n} \chi_D(m)$ beide multiplikativ sind, brauchen wir (11) nur für Primzahlpotenzen $n = p^k$ nachzuweisen. Es gibt drei Fälle:

i) Ist $\chi_D(p) = 1$, so ist $p = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p}' \neq \mathfrak{p}$, $N(\mathfrak{p}) = N(\mathfrak{p}') = p$, und

$$p^k = N(\mathfrak{p}^k) = N(\mathfrak{p}^{k-1}\,\mathfrak{p}') = N(\mathfrak{p}^{k-2}\,\mathfrak{p}'^2) = \ldots = N(\mathfrak{p}'^k)$$

läßt sich auf genau $k+1$ verschiedene Weisen als Norm darstellen, also

$$F(p^k) = k+1 = \underbrace{1+1+\ldots+1}_{k+1} = \sum_{i=0}^{k} \chi_D(p^i) .$$

ii) Ist $\chi_D(p) = 0$, so ist $p = \mathfrak{p}^2$, $N(\mathfrak{p}) = p$, und $p^k = N(\mathfrak{p}^k)$ hat genau eine Darstellung als Norm, also

$$F(p^k) = 1 = \underbrace{1+0+\ldots+0}_{k+1} = \sum_{i=0}^{k} \chi_D(p^i) .$$

iii) Ist $\chi_D(p) = -1$, so ist $p = \mathfrak{p}$, $N(\mathfrak{p}) = p^2$ und $p^{2k} = N(\mathfrak{p}^k)$, während p^{2k+1} gar keine Norm ist, also

$$F(p^k) = \begin{cases} 1 & (k \text{ gerade}) \\ 0 & (k \text{ ungerade}) \end{cases} = \underbrace{1-1+\ldots\pm 1}_{k+1} = \sum_{i=0}^{k} \chi_D(p^i) .$$

Somit ist (11) in allen drei Fällen bewiesen.

Wir können auch (10) direkt beweisen mit Hilfe der Euler-Produkte der beiden Seiten. Wie oben (als wir zeigten, daß $\zeta_K(s)$ für $\sigma > 1$ konvergiert), schreiben wir

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{p} \left(\prod_{\mathfrak{p}\mid p} \frac{1}{1-N(\mathfrak{p})^{-s}} \right) ,$$

wobei $\mathfrak{p}$ über die Primideale in $\mathfrak{o}$ und p über die gewöhnlichen Primzahlen läuft. Mit Satz 1 haben wir:

$$\chi_D(p) = 1 \Rightarrow p = \mathfrak{p}\mathfrak{p}' \,,\ \mathfrak{p} \neq \mathfrak{p}' \,,\ N(\mathfrak{p}) = N(\mathfrak{p}') = p$$

$$\Rightarrow \prod_{\mathfrak{p}\mid p} \frac{1}{1-N(\mathfrak{p})^{-s}} = \frac{1}{(1-p^{-s})^2} ,$$

$$\chi_D(p) = 0 \Rightarrow p = \mathfrak{p}^2 \,,\ N(\mathfrak{p}) = p \Rightarrow \prod_{\mathfrak{p}\mid p} \frac{1}{1-N(\mathfrak{p})^{-s}} = \frac{1}{1-p^{-s}} ,$$

$$\chi_D(p) = -1 \Rightarrow p = \mathfrak{p} \,,\ N(\mathfrak{p}) = p^2 \Rightarrow \prod_{\mathfrak{p}\mid p} \frac{1}{1-N(\mathfrak{p})^{-s}} = \frac{1}{1-p^{-2s}} ,$$

also in allen drei Fällen

$$\prod_{\mathfrak{p}\mid p} \frac{1}{1-N(\mathfrak{p})^{-s}} = \frac{1}{1-p^{-s}} \cdot \frac{1}{1-\chi_D(p)p^{-s}} .$$

Wenn wir diese Gleichungen für alle rationalen Primzahlen p miteinander multiplizieren, erhalten wir (10).

Da wir am Anfang des Paragraphen bewiesen haben, daß die Gesamtanzahl $R(n)$ der Darstellungen einer Zahl n durch Formen der Diskriminante D gleich dem n-ten Koeffizienten $F(n)$ der Dirichletschen Reihe $\zeta_K(s)$ ist, erhalten wir aus dem Korollar die Formel

$$R(n) = \sum_{m\mid n} \chi_D(m) , \tag{12}$$

die in §8 als Satz 2 bewiesen wurde. (Umgekehrt hätten wir Satz 1 aus (12) ableiten können.) In §8 zeigten wir, wie man die Klassenzahlformel

$$h(D) = \frac{1}{\kappa} L(1,\chi_D) \tag{13}$$

mit

$$\kappa = \begin{cases} \frac{1}{w} \cdot \frac{2\pi}{\sqrt{|D|}} \,, & \text{falls } D < 0 \\ \frac{\log \varepsilon_0}{\sqrt{D}} \,, & \text{falls } D > 0 \end{cases} \tag{14}$$

(w die Ordnung der Einheitengruppe U, ε_0 die Grundeinheit) aus (12) erhalten kann, indem man aus (12) schließt, daß der Mittelwert der Zahlen $R(n)$ gleich $L(1,\chi_D)$ ist, während man durch geometrische Methoden direkt zeigt, daß der Mittelwert der Zahlen $R(n,f)$ für jede Form f der Diskriminante D gleich κ ist. Man kann aber (13) auch aus dem Korollar zu Satz 1 gewinnen, ohne die Theorie von quadratischen Formen zu verwenden. Denn aus (10) und den in §4 und §6 bewiesenen Eigenschaften der Zetafunktion und der L-Reihen folgt sofort, daß die Funktion $\zeta_K(s)$, die für $\sigma > 1$ durch (2) definiert ist, eine meromorphe Fortsetzung auf die ganze komplexe Ebene besitzt mit einem einfachen Pol vom Residuum $L(1,\chi_D)$ an der Stelle $s = 1$ als einziger Singularität. Andererseits ist aber $\zeta_K(s)$ die Summe der $h(D)$ Funktionen $\zeta(A,s)$, wo A über die verschiedenen Idealklassen von $\mathfrak{o}$ (im engeren Sinne) läuft. Die Beziehung (13) ist dann eine unmittelbare Folge des folgenden Satzes:

SATZ 2: *Sei* K *ein quadratischer Körper der Diskriminante* D *und* A *eine Idealklasse (im engeren Sinne) von* K. *Dann hat die für* $\sigma > 1$ *durch*

$$\zeta(A,s) = \sum_{\substack{\mathfrak{a}\in A \\ \mathfrak{a} \text{ ganz}}} \frac{1}{N(\mathfrak{a})^s} \tag{15}$$

definierte Zetafunktion von A *eine meromorphe Fortsetzung auf die Halbebene* $\sigma > \frac{1}{2}$ *mit einem einfachen Pol an der Stelle* $s = 1$ *als einziger Singularität. Es gilt*

(16) $$\operatorname{res}_{s=1} \zeta(A,s) = \kappa \ ,$$

wobei κ *die durch (14) definierte Zahl bezeichnet, welche von* K, *aber nicht von der Idealklasse* A *abhängt.*

Wenn wir diesen Beweis der Klassenzahlformel (13) mit dem Beweis in §8 vergleichen, so sehen wir, daß die Grundidee in beiden dieselbe ist, nur daß wir jetzt mit dem Residuum einer Dirichletschen Reihe $\sum a_n n^{-s}$ an der Stelle $s = 1$ statt mit dem Mittelwert $\lim_{N\to\infty} \frac{1}{N}(a_1 + \dots + a_N)$ ihrer Koeffizienten arbeiten; für die von uns betrachteten Dirichletschen Reihen sind diese Werte aber gleich (vgl. Aufgabe 3). Wir bemerken auch, daß sich $\zeta(A,s) - \frac{\kappa}{s-1}$ tatsächlich auf die ganze komplexe Ebene holomorph fortsetzen läßt; wir haben in Satz 2 nur die Fortsetzbarkeit auf die Halbebene $\sigma > \frac{1}{2}$ behauptet, weil dies sich aus dem schon Bewiesenen leicht herleiten läßt (Aufgabe 4).

Sei jetzt

$$C = \{\text{gebrochene Ideale von } K\}/\{\text{Hauptideale}\}$$

die Gruppe der Idealklassen von K (im engeren Sinne); dies ist eine endliche Gruppe der Ordnung $|C| = h = h(D)$. Ein *Idealklassencharakter* von K ist ein Charakter auf C im Sinne von §5 oder, was dasselbe ist, eine komplexwertige Funktion χ auf den (gebrochenen) Idealen von K mit den beiden Eigenschaften

a) $\chi(\mathfrak{a}\mathfrak{b}) = \chi(\mathfrak{a})\,\chi(\mathfrak{b})$ für alle Ideale $\mathfrak{a}, \mathfrak{b}$;

b) $\chi((\alpha)) = 1$ für $\alpha \in K$, $N(\alpha) > 0$.

Einem solchen Charakter ordnen wir die L-Reihe

$$L_K(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

zu, wobei die Summe wie in (2) über die ganzen Ideale $\mathfrak{a} \neq 0$ von K läuft. Wegen der Multiplikativität a) hat diese L-Reihe eine Euler-Produktentwicklung

$$L_K(s,\chi) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} .$$

Andererseits ist

(17) $$L_K(s,\chi) = \sum_{A\in C} \sum_{\mathfrak{a}\in A} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{A\in C} \chi(A)\ \zeta(A,s)$$

und nach der Orthogonalitätsrelation für Charaktere (der Verallgemeinerung des Korollars zu Satz 3, §5, auf Charaktere auf beliebigen endlichen abelschen Gruppen, deren Beweis wir dem Leser überlassen) umgekehrt

(18) $$\zeta(A,s) = \frac{1}{h} \sum_{\chi} \overline{\chi}(A)\ L_K(s,\chi)$$

(Summe über alle Idealklassencharaktere χ). Es ist also gleichbedeutend, die Funktionen $\zeta(A,s)$ oder die L-Reihen $L_K(s,\chi)$ zu studieren; die ersteren sind häufig für analytische und die letzteren für arithmetische Untersuchungen geeigneter.

Aus (17) und Satz 2 folgt, daß $L_K(s,\chi)$ eine meromorphe Fortsetzung auf $\sigma > \frac{1}{2}$ hat und dort mit der eventuellen Ausnahme eines einfachen Pols bei $s = 1$ holomorph ist. Wegen (16) und der genannten Orthogonalitätsrelationen ist

$$\operatorname{res}_{s=1} L_K(s,\chi) = \sum_{A\in C} \chi(A)\ \kappa = \begin{cases} h\kappa & (\chi = \chi_0) \\ 0 & (\chi \neq \chi_0) \end{cases}$$

(χ_0 = Hauptcharakter), d.h. $L_K(s,\chi)$ ist für $\chi \neq \chi_0$ holomorph, während $L_K(s,\chi_0) = \zeta_K(s)$ einen Pol mit Residuum $h\kappa$ bei $s = 1$ hat. Es gilt dann

SATZ 3: *Für jeden nichttrivialen Idealklassencharakter* χ *ist* $L_K(1,\chi) \neq 0$.

Der Beweis ist analog zu dem in §6 gegebenen Beweis für Dirichletsche Charaktere: zunächst ist die Funktion

$$F(s) = \prod_{\chi\in\hat{C}} L_K(s,\chi) = \zeta_K(s) \prod_{\chi\neq\chi_0} L_K(s,\chi)$$

wegen

$$\log F(s) = h \sum_{\substack{\mathfrak{p}\ \text{Primideal} \\ r\geq 1 \\ \mathfrak{p}^r\ \text{Hauptideal}}} \frac{1}{r} N(\mathfrak{p})^{-rs}$$

für reelles $s > 1$ reell und ≥ 1, woraus folgt, daß $L_K(1,\chi)$ für höchstens einen nichttrivialen Charakter χ verschwinden kann, welcher reell sein muß; für χ reell leitet man aus $L_K(1,\chi) = 0$ mit Hilfe der Funktion $\frac{\zeta_K(s)\,L_K(s,\chi)}{\zeta_K(2s)}$ einen Widerspruch her (in §12 werden wir für reelle χ eine Formel für $L_K(s,\chi)$ angeben, woraus $L_K(1,\chi) \neq 0$ ebenfalls folgt).

Wir erwähnen, daß, genau wie im Falle $K = \mathbb{Q}$, die Werte $L_K(1,\chi)$

in die Formeln für die Klassenzahlen gewisser Erweiterungen von K (der sog. Klassenkörper) eingehen.

KOROLLAR: *Sei* D *eine Fundamentaldiskriminante. Dann stellt jede quadratische Form der Diskriminante* D *unendlich viele Primzahlen dar.*

(Das Korollar gilt für beliebige primitive Formen, deren Diskriminante kein Quadrat ist, aber für den allgemeinen Beweis muß man statt Idealklassencharakteren die sog. Ringklassencharaktere benutzen.)

Beweis: Wieder wegen der Orthogonaltitätsrelationen ist

$$\sum_{\mathfrak{p}^r \in A} \frac{1}{r} N(\mathfrak{p})^{-rs} = \frac{1}{h} \sum_{\chi \in \hat{C}} \overline{\chi}(A) \log L_K(s,\chi) \qquad (\mathrm{Re}(s) > 1)$$

für jedes $A \in C$. Wegen des Satzes sind die Glieder mit $\chi \neq \chi_0$ auf der rechten Seite für $s \to 1$ beschränkt, während

$$\log L_K(s,\chi_0) = \log \zeta_K(s) = \log \frac{1}{s-1} + O(1) \qquad (s \to 1) .$$

Andererseits ist auf der linken Seite die Summe über alle $\mathfrak{p}$ und r mit $r > 1$ oder $N(\mathfrak{p}) = p^2$ wegen $\sum_{n=1}^{\infty} n^{-2} < \infty$ ebenfalls für $s \to 1$ beschränkt, also

$$\sum_{\substack{\mathfrak{p} \in A \\ N(\mathfrak{p}) \text{ prim}}} N(\mathfrak{p})^{-s} = \frac{1}{h} \log \frac{1}{s-1} + O(1) \qquad (s \to 1) .$$

Für eine rationale Primzahl p ist aber die Anzahl der $\mathfrak{p} \in A$ mit $N(\mathfrak{p}) = p$ gleich der Anzahl der Darstellungen von p durch die Form f, die unter der Korrespondenz von §10 der Idealklasse A entspricht. Damit haben wir nicht nur das Korollar, sondern die schärfere Aussage

$$\sum_{p} R(p,f)\, p^{-s} = \frac{1}{h} \log \frac{1}{s-1} + O(1)$$

need p unramified

bewiesen. Ist p durch f darstellbar, so ist $R(p,f)$ gleich 1 oder 2 je nachdem, ob $A = A'$ oder nicht, d.h. je nachdem, ob die Form $f(x,y) = ax^2 + bxy + cy^2$ unter $SL_2(\mathbb{Z})$ zu der Form $ax^2 - bxy + cy^2$ äquivalent ist (solche Formen heißen *ambig*) oder nicht. Definieren wir die *Dirichletsche Dichte* einer Menge $\mathfrak{P}$ von Primzahlen als

$$\delta(\mathfrak{P}) = \lim_{s \to 1} \left(\sum_{p \in \mathfrak{P}} p^{-s} \right) \Big/ \left(\log \frac{1}{s-1} \right)$$

(falls der Limes existiert), so können wir das Ergebnis etwas bildhafter so formulieren: die Menge der Primzahlen, die durch f darstellbar sind, besitzt eine Dirichletsche Dichte, und zwar $\frac{1}{2h(D)}$

oder $\frac{1}{h(D)}$ je nachdem, ob f ambig ist oder nicht.

Aufgaben:

1. Man beweise Satz 1 für $p = 2$, d.h. 2 ist zerlegt, falls $D \equiv 1 \pmod 8$, träge, falls $D \equiv 5 \pmod 8$, und verzweigt, falls $D \equiv 0 \pmod 4$.

   Hinweis: Ist $D = 4d$ mit $d \equiv 2$ bzw. $3 \pmod 4$, so ist $x = \sqrt{d}$ bzw. $x = 1 + \sqrt{d}$ in $\mathfrak{O}$ und $2 \mid x^2$, $2 \nmid x$; also ist 2 verzweigt. Ist umgekehrt $2 = \mathfrak{p}^2$ verzweigt, aber $D \equiv 1 \pmod 4$, so kann man aus $\mathfrak{p} \mid x$ und $2 \nmid x$ wie im Falle einer ungeraden Primzahl einen Widerspruch herleiten. Ist $D \equiv 5 \pmod 8$, so kann man aus $2 \mid N(x)$ auch $2 \mid x$ ableiten, also ist 2 träge. Ist aber $D \equiv 1 \pmod 8$, so ist $\frac{1+\sqrt{D}}{2}$ nicht durch 2 teilbar, hat aber gerade Norm, und 2 kann nicht träge sein.

2. Sei K ein quadratischer Körper der Diskriminante D, $\mathfrak{O}$ der Ring der ganzen Zahlen in K und r eine natürliche Zahl. Dann ist die Ordnung der Gruppe $(\mathfrak{O}/r\mathfrak{O})^*$ der invertierbaren Elemente des Restklassenrings $\mathfrak{O}/r\mathfrak{O}$ durch

   $$|(\mathfrak{O}/r\mathfrak{O})^*| = \phi(r)\, \gamma_D(r)$$

   gegeben, wo $\phi(r) = |(\mathbb{Z}/r\mathbb{Z})^*|$ die Eulersche Funktion ist und $\gamma_D(r) = r \prod_{p \mid r} \left(1 - \frac{\chi_D(p)}{p}\right)$. (Vgl. die Bemerkung zu Aufgabe 5, §10.)

3. Sei $\sum_{n=1}^{\infty} c_n n^{-s}$ eine Dirichletsche Reihe mit Konvergenzabszisse $\sigma_0 < 1$. Dann ist das Produkt von $\sum c_n n^{-s}$ mit $\zeta(s)$ eine Dirichletsche Reihe mit folgender Eigenschaft: der Mittelwert der Koeffizienten existiert und ist gleich dem Residuum an der Stelle $s = 1$ der meromorphen Fortsetzung der durch diese Reihe definierten Funktion, also gleich $\sum \frac{c_n}{n}$. (Vgl. den Beweis vom Satz 4, §8, wo $c_n = \chi_D(n)$, $\sigma_0 = 0$.)

4. Man beweise Satz 2, indem man die Beziehung $\zeta(s,A) = \sum_{n=1}^{\infty} \frac{R(n,f)}{n^s}$ (f die Form, die A entspricht) benutzt und den Beweis von Satz 4, §8, verfeinert, um die Formel

   $$\sum_{n=1}^{N} R(n,f) \sim \kappa N$$

durch die präzisere Formel

$$\sum_{n=1}^{N} R(n,f) = \kappa N + O(\sqrt{N})$$

zu ersetzen.

§12 Geschlechtertheorie

In §8 haben wir binäre quadratische Formen studiert. Dabei nannten wir zwei Formen äquivalent, falls sie durch eine ganzzahlige Matrix der Determinante 1 ineinander übergeführt werden können, und sahen, daß es im allgemeinen mehrere (allerdings nur endlich viele) Äquivalenzklassen von Formen mit einer gegebenen Diskriminante D gibt, und daß deren Anzahl h(D) eine gar nicht leicht zu bestimmende Zahl ist. Zu den schönsten Entdeckungen von Gauß gehört die Erkenntnis, daß das entsprechende Problem für *rationale* Äquivalenz leichter ist und vollständig gelöst werden kann. Man sagt, daß zwei Formen, die rational äquivalent sind (d.h. durch eine Matrix von rationalen Zahlen mit der Determinante 1 ineinander überführbar sind) zum selben *Geschlecht* gehören. Gauß hat eine vollständige Beschreibung der Geschlechter der Formen mit Diskriminante D mit Hilfe von gewissen quadratischen Charakteren gegeben und gezeigt, daß ihre Anzahl gleich 2^{t-1} ist, wo t die Anzahl der in D enthaltenen Primfaktoren bezeichnet. Insbesondere ist h(D) stets durch 2^{t-1} teilbar, eine Tatsache, die wir schon in §9 erwähnten. Daß die Einteilung in Geschlechter wirklich grober ist als die vorher von uns betrachtete Klasseneinteilung, sieht man anhand des folgenden Beispiels: die Formen

$$f(x,y) = x^2 + xy + 6y^2$$
$$g(x,y) = 2x^2 + xy + 3y^2$$

der Diskriminante -23 sind sicherlich nicht äquivalent, da f die Zahl 1 ganzzahlig darstellt (mit x = 1, y = 0) und g das nicht tut ($g(x,y) = 2(x + \frac{1}{4}y)^2 + \frac{23}{8}y^2 > 1$ für x, y ganz und nicht beide 0), aber man kann f in g überführen durch Anwendung der Transformation $\begin{pmatrix} 1/2 & 1/2 \\ -3/2 & 1/2 \end{pmatrix}$ der Determinante 1.

Wir wollen in diesem Paragraphen die Hauptresultate der Gaußschen Geschlechtertheorie herleiten, wobei wir mit Idealklassen statt mit

Formen arbeiten. Hierbei wählen wir eine andere Definition der Geschlechter als die oben angegebene (für die Äquivalenz der beiden Definitionen s. Aufgabe 1). Wir führen alle Überlegungen für beliebige quadratische Körper - reell sowie imaginär - durch.

Sei also K ein quadratischer Körper der Diskriminante D und C die Gruppe der Idealklassen von K. (Wir fassen Idealklassen immer im engeren Sinne auf.) Wir hatten am Ende von §11 gemerkt, daß die multiplikativen, komplexwertigen Funktionen auf Idealen, welche auf der Hauptidealklasse den Wert 1 annehmen, genau die Charaktere von C sind, d.h. die Homomorphismen $\chi: C \to \mathbb{C}^*$. Unter diesen Funktionen zeichnen wir die aus, die *reellwertig* sind, d.h. die Homomorphismen

$$\chi: C \to \{\pm 1\} ,$$

und nennen sie die *Geschlechtscharaktere*. Wir sagen, daß zwei Idealklassen A_1 und A_2 zu demselben *Geschlecht* gehören, falls $\chi(A_1) = \chi(A_2)$ für alle Geschlechtscharaktere χ. Da offensichtlich

$$\begin{aligned} \chi(C) \subset \{\pm 1\} &\iff \chi(A)^2 = 1 \quad \text{für alle } A \in C \\ &\iff \chi(A^2) = 1 \quad \text{für alle } A \in C \\ &\iff \chi(A_1A_2^2) = \chi(A_1) \quad \text{für alle } A_1A_2 \in C \end{aligned} \tag{1}$$

ist diese Definition zur folgenden äquivalent: zwei Klassen $A_1, A_2 \in C$ gehören zum gleichen Geschlecht genau dann, wenn A_1 und A_2 sich um ein Quadrat in der Gruppe C unterscheiden. Die Geschlechter bilden also eine Gruppe, die zu C/C^2 isomorph ist, wo C^2 die Untergruppe $\{A^2 | A \in C\}$ von C bezeichnet; die Geschlechtscharaktere bilden die hierzu duale Gruppe $\widehat{C/C^2}$ (vgl. §5). Insbesondere ist die Anzahl der Geschlechter gleich der Anzahl der Geschlechtscharaktere und ist eine Potenz von 2. Das Einselement der Gruppe der Geschlechter nennt man das *Hauptgeschlecht;* nach (1) besteht dieses Geschlecht aus den Quadraten der Idealklassen, d.h. ein Ideal $\mathfrak{a}$ gehört genau dann zum Hauptgeschlecht, wenn $\mathfrak{a} = (\lambda)\,\mathfrak{b}^2$ für ein geeignetes Ideal $\mathfrak{b}$ und eine Zahl $\lambda \in K$ mit $N(\lambda) > 0$.

Diese Definition der Geschlechter als Äquivalenzklassen von Idealklassen modulo den Quadraten wirkt vielleicht etwas künstlich. Daß der Begriff doch sehr natürlich ist, sieht man aus folgendem Ergebnis.

SATZ 1: i) *Zwei (gebrochene) Ideale* $\mathfrak{a}, \mathfrak{b}$ *gehören genau dann zum gleichen Geschlecht, wenn es eine Zahl* $\lambda \in K$ *positiver Norm gibt mit*

$$N(\mathfrak{a}) = N(\lambda)\, N(\mathfrak{b}) . \tag{2}$$

Example of $K=\mathbb{Q}(\sqrt{-6})$. Integers form a UFD. $N((\sqrt{-6}))=6$. But no $\lambda \in K$ has norm 6, since $a^2+6b^2=6c^2$ has no solution. (Assume $(a,b,c)=1$, $3|a \Rightarrow 3|b^2,c^2 \Rightarrow 3|b$ and $3|c$). So $(\sqrt{-6})$ not in principal genus

ii) *Eine natürliche Zahl* n *ist genau dann Norm einer Zahl aus* K, *wenn* n *die Norm eines ganzen Ideals aus dem Hauptgeschlecht ist.*

Beweis: i) Die Behauptung in einer Richtung ist trivial: Sind $\mathfrak{a}$ und $\mathfrak{b}$ in demselben Geschlecht, so ist nach dem oben Gesagten

$$\mathfrak{a} = (\mu)\mathfrak{c}^2\mathfrak{b}$$

mit $\mathfrak{c}$ ein Ideal aus K und $\mu \in K$ eine Zahl positiver Norm; dann ist

$$N(\mathfrak{a}) = |N(\mu)|\, N(\mathfrak{c})^2\, N(\mathfrak{b}) = N(\mu N(\mathfrak{c}))\, N(\mathfrak{b}) ,$$

also gilt (2) mit $\lambda = \mu N(\mathfrak{c})$. Nehmen wir jetzt umgekehrt an, daß (2) gilt; wir wollen zeigen, daß $\mathfrak{a}$ im Geschlecht von $\mathfrak{b}$ liegt. Indem wir $\mathfrak{a}$ durch $\mathfrak{a}\mathfrak{b}^{-1}$ ersetzen, können wir $\mathfrak{b} = (1)$ annehmen, d.h. es genügt, die Implikation

$$(3) \qquad N(\mathfrak{a}) = N(\lambda) \quad (\lambda \in K) \quad \Rightarrow \quad \mathfrak{a} \in \text{Hauptgeschlecht}$$

nachzuweisen. Ersetzen wir $\mathfrak{a}$ durch $(\lambda^{-1})\mathfrak{a}$, so können wir sogar $\lambda = 1$ annehmen, d.h. $N(\mathfrak{a}) = 1$. Wir behaupten:

$$(4) \qquad N(\mathfrak{a}) = 1 \Rightarrow \exists \text{ ganzes Ideal } \mathfrak{b} \text{ mit } \mathfrak{a} = \mathfrak{b}/\mathfrak{b}' .$$

Dies impliziert dann (3), da $\mathfrak{b}/\mathfrak{b}' = N(\mathfrak{b})^{-1}\,\mathfrak{b}^2$ offensichtlich zum Hauptgeschlecht gehört.

Um (4) einzusehen, schreiben wir die Primidealzerlegung des (gebrochenen) Ideals $\mathfrak{a}$ hin, wobei wir zwischen den Primfaktoren $\mathfrak{p}_i$ mit $\mathfrak{p}_i' \neq \mathfrak{p}_i$ (d.h. $N(\mathfrak{p}_i) = p_i$ mit p_i eine zerfallende Primzahl) und den Primfaktoren $\mathfrak{q}_j$ mit $\mathfrak{q}_j = \mathfrak{q}_j'$ (d.h. $N(\mathfrak{q}_j) = q_j^{i_j}$ mit q_j verzweigt und $i_j = 1$ oder q_j träge und $i_j = 2$) unterscheiden:

$$\mathfrak{a} = \Big(\prod_i \mathfrak{p}_i^{a_i}\,\mathfrak{p}_i'^{b_i}\Big)\Big(\prod_j \mathfrak{q}_j^{c_j}\Big) \qquad (a_i, b_i, c_j \in \mathbb{Z}) .$$

Dann folgt aus $1 = N(\mathfrak{a}) = \prod p_i^{a_i+b_i} \prod q_j^{i_j c_j}$ und der eindeutigen Primzahlzerlegung in $\mathbb{Q}$, daß $a_i + b_i = 0$ für alle i und $c_j = 0$ für alle j, und somit ist (4) mit $\mathfrak{b} = \prod_{a_i>0} \mathfrak{p}_i^{a_i} \prod_{b_i>0} \mathfrak{p}_i'^{b_i}$ bewiesen.

ii) Wieder ist eine Richtung trivial: Ist $n = N(\mathfrak{a})$ mit $\mathfrak{a}$ im Hauptgeschlecht, so ist nach (2) mit $\mathfrak{b} = (1)$ auch n die Norm einer Zahl $\lambda \in K$. Ist umgekehrt $n = N(\lambda)$, $\lambda \in K$, so schreibt man (λ) als $\mathfrak{a}/\mathfrak{b}$ mit $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde ganze Ideale aus K; dann folgt aus

$N(\mathfrak{b})|N(\mathfrak{a})$ und $(\mathfrak{a},\mathfrak{b}) = 1$ mit demselben Argument wie für (4), daß $\mathfrak{b}'|\mathfrak{a}$, also $\mathfrak{a} = \mathfrak{b}'\mathfrak{c}$ ist mit $\mathfrak{c}$ ganz. Dann ist

$$n = N(\lambda) = N(\mathfrak{a}/\mathfrak{b}) = N(\mathfrak{b}'\mathfrak{c}/\mathfrak{b}) = N(\mathfrak{c})$$

und $\mathfrak{c}$ liegt wegen (3) im Hauptgeschlecht.

Für spätere Zwecke schreiben wir gleich das Analogon von (4) für Zahlen:

$$(5) \qquad \lambda \in K ,\ N(\lambda) = 1 \quad \Rightarrow \quad \exists\, \mu \in \mathfrak{O} \text{ mit } \lambda = \mu/\mu' .$$

Der Beweis ist einfach: man wählt $\mu = \lambda + 1$.

Der eben bewiesene Satz soll den Unterschied zwischen Idealklassen (im engeren Sinne) und Geschlechtern verdeutlichen: Für Ideale $\mathfrak{a}, \mathfrak{b}$ hat man

$\mathfrak{a}, \mathfrak{b}$ in derselben Idealklasse $\Leftrightarrow \mathfrak{a} = (\lambda)\mathfrak{b}$, $N(\lambda) > 0$,

$\mathfrak{a}, \mathfrak{b}$ in demselben Geschlecht $\Leftrightarrow N(\mathfrak{a}) = N((\lambda)\mathfrak{b})$, $N(\lambda) > 0$;

für $n \in \mathbb{N}$ hat man $n = N((a+\sqrt{5})) = 2$, but $2c^2 \neq a^2 + 5b^2$ (assume $(a,b,c)=1$ and check mod 5) If $N(\lambda)<0$ does λ unit with $N=-1$? No, see $\mathfrak{a}(\sqrt{5})$

$n = N(\mathfrak{a})$, $\mathfrak{a}$ ganz, $\mathfrak{a} \in$ Hauptidealklasse $\Leftrightarrow n = |N(\lambda)|$, $\lambda \in \mathfrak{O}$

$n = N(\mathfrak{a})$, $\mathfrak{a}$ ganz, $\mathfrak{a} \in$ Hauptgeschlecht $\Leftrightarrow n = N(\lambda)$, $\lambda \in K$.

Wir kommen jetzt zum Hauptergebnis dieses Paragraphen, der Klassifikation aller Geschlechtscharaktere. Wir erinnern an einige Tatsachen aus Teil I: Jeder Fundamentaldiskriminante D ist ein reeller, primitiver Charakter χ_D (modulo $|D|$) zugeordnet. Jede Diskriminante D läßt sich eindeutig als Produkt von Primdiskriminanten schreiben, d.h. von Fundamentaldiskriminanten, die nur eine Primzahl enthalten. Ist $D = D_1 \ldots D_t$ die Zerlegung von D als Produkt von Primdiskriminanten, so ist χ_D das Produkt der entsprechenden χ_{D_i}. Wir bezeichnen die L-Reihe $L(s,\chi_D)$ mit $L_D(s)$; für $D = 1$ ist χ_D trivial und $L_D(s) = \zeta(s)$, während man für $D \neq 1$, also D die Diskriminante eines quadratischen Körpers K, die Beziehung

$$(6) \qquad \zeta_K(s) = \zeta(s)\, L_D(s)$$

hat. Mit dieser Terminologie gilt:

SATZ 2: *Sei* D *die Diskriminante des quadratischen Körpers* K. *Es gibt eine bijektive Korrespondenz zwischen den Geschlechtscharakteren von* K *und den Zerlegungen* $D = D' \cdot D''$ *von* D *als Produkt von zwei Fundamentaldiskriminanten* (wo-

bei die Zerlegungen $D = D' \cdot D''$ und $D = D'' \cdot D'$ als gleich angesehen werden, und die Zerlegungen $D = 1 \cdot D$ bzw. $D = D \cdot 1$ erlaubt sind). *Der der Zerlegung* $D = D' \cdot D''$ *entsprechende Geschlechtscharakter ist für Primideale durch*

$$\chi(\mathfrak{p}) = \begin{cases} \chi_{D'}(N\mathfrak{p}) \text{ , falls } (N\mathfrak{p}, D') = 1 \text{ ,} \\ \chi_{D''}(N\mathfrak{p}) \text{ , falls } (N\mathfrak{p}, D'') = 1 \text{ ,} \end{cases} \tag{7}$$

und für beliebige Ideale durch

$$\chi(\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}) = \chi(\mathfrak{p}_1)^{n_1} \cdots \chi(\mathfrak{p}_k)^{n_k} \quad (\mathfrak{p}_i \text{ Primideale, } n_i \in \mathbb{Z}) \text{ ,} \tag{8}$$

definiert. Die L-Reihe von χ *ist durch die Formel*

$$L_K(s,\chi) = L_{D'}(s)\, L_{D''}(s) \tag{9}$$

gegeben.

Für $D' = 1$, $D'' = D$ ist $\chi = \chi_0$ und $L(s,\chi) = \zeta_k(s)$; in diesem Fall reduziert sich (9) auf (6).

KOROLLAR: *Die Gruppe* C/C^2 *ist zu* $(\mathbb{Z}/2\mathbb{Z})^{t-1}$ *isomorph, wo* t *die Anzahl der verschiedenen Primteiler von* D *bezeichnet. Insbesondere ist die Klassenzahl* $h(D)$ *durch* 2^{t-1} *teilbar, und* $h(D)$ *ist genau dann ungerade, wenn* D *eine Primdiskriminante ist.*

Beweis des Korollars: Sei $D = D_1 \cdots D_t$ die Zerlegung von D als Produkt von Primdiskriminanten; dann hat D genau 2^{t-1} Zerlegungen als $D' \cdot D''$, da diese genau den Zerlegungen der Menge $\{D_1, \ldots, D_t\}$ als disjunkte Vereinigung von zwei Mengen (ohne Rücksicht auf die Reihenfolge dieser Mengen) entsprechen. Andererseits wissen wir, daß die Anzahl der Geschlechtscharaktere gleich der Ordnung der Gruppe C/C^2 ist; da diese Gruppe abelsch ist und den Exponenten 2 hat, ist sie zu $(\mathbb{Z}/2\mathbb{Z})^r$ isomorph für ein geeignetes r, und dann gilt $2^r \mid h(D)$ und $r > 0 \iff 2 \mid h(D)$ $(h(D) = |C|)$. Nach dem Satz gibt es aber gleich viele Geschlechtscharaktere wie Diskriminantenzerlegungen, also ist $r = t - 1$.

Beweis des Satzes: Nachzuweisen ist,

i) daß die durch (7) und (8) definierte Funktion auf Idealen wohldefiniert und ein Geschlechtscharakter ist,
ii) daß für diesen Charakter die Beziehung (9) gilt,
iii) daß die 2^{t-1} so konstruierten Charaktere verschieden sind, und

iv) daß sämtliche Geschlechtscharaktere auf diese Weise entstehen.

i) Wenn $\mathfrak{p}$ ein Primideal und $D = D' \cdot D''$ ein Zerlegung wie im Satz ist, so ist $N(\mathfrak{p})$ eine Primzahlpotenz und $(D', D'') = 1$, also gilt $(N\mathfrak{p}, D') = 1$ oder $(N\mathfrak{p}, D'') = 1$ (oder beides). Wir müssen verifizieren, daß die beiden Werte in (7) übereinstimmen, falls $(N\mathfrak{p}, D') = 1$ und $(N\mathfrak{p}, D'') = 1$, d.h., falls $N(\mathfrak{p})$ zu D teilerfremd ist. Dann gibt es nach Satz 1, §11, zwei Möglichkeiten: entweder ist $N\mathfrak{p} = p^2$, $\chi_D(p) = -1$, oder $N\mathfrak{p} = p$, $\chi_D(p) = +1$. Im ersten Fall ist

$$\chi_{D'}(N\mathfrak{p}) = \chi_{D'}(p^2) = \chi_{D'}(p)^2 = 1 = \chi_{D''}(N\mathfrak{p})$$

und die beiden Definitionen (7) stimmen überein; im zweiten Fall ist

$$\chi_{D'}(N\mathfrak{p})\chi_{D''}(N\mathfrak{p}) = \chi_{D'}(p)\chi_{D''}(p) = \chi_D(p) = 1 \text{ ,}$$

also $\chi_{D'}(N\mathfrak{p}) = \chi_{D''}(N\mathfrak{p})$, und wieder ist (7) widerspruchsfrei. Wegen der eindeutigen Primidealzerlegung in K definiert dann (8) die Funktion χ eindeutig für alle Ideale $\mathfrak{a} \neq 0$. Es bleibt nur zu zeigen, daß $\chi(\mathfrak{a}) = 1$ für ein Hauptideal $\mathfrak{a}$, d.h.

$$\chi((\lambda)) = 1 \qquad (\lambda \in K,\ N(\lambda) > 0) \text{ ;} \tag{10}$$

da χ offensichtlich multiplikativ ist und nur die Werte ± 1 annimmt, ist es dann ein Geschlechtscharakter.

In (10) können wir $\lambda \in \mathfrak{o}$ annehmen, da jede Zahl aus K Quotient zweier ganzer Zahlen ist. Wir beweisen (10) erst unter der Annahme, daß $N(\lambda)$ zu D' (oder D'') teilerfremd ist. Dann folgt aus (7) und (8), daß

$$\chi((\lambda)) = \chi_{D'}(N(\lambda)) \text{ .}$$

Sei $D' = \prod_i D_i$ die Zerlegung der Fundamentaldiskriminante in Primdiskriminanten. Dann ist $\chi_{D'}$ das Produkt der Charaktere χ_{D_i} (das soll der Leser verifizieren!), also genügt es, für jedes i

$$\chi_{D_i}(N(\lambda)) = 1 \qquad (\lambda \in \mathfrak{o},\ \lambda \text{ zu } D_i \text{ teilerfremd})$$

zu zeigen. Hierbei ist entweder $D_i = \pm p \equiv 1 \pmod 4$ mit p prim, oder $D_i = -4$, 8 oder -8 (siehe Teil I, §5). Im ersten Fall ist

$$\lambda = \frac{a + b\sqrt{D}}{2} \qquad (a, b \in \mathbb{Z})$$

$$N(\lambda) = \frac{a^2 - b^2 D}{4} \equiv \frac{a^2}{4} \pmod{p} \ , \ p \nmid a \ ,$$

also

$$\chi_{D_i}(N(\lambda)) = \chi_{D_i}\left(\frac{a^2}{4}\right) = 1 \ .$$

Falls $D_i = -4$ bzw. 8 bzw. -8 ist, schreiben wir D als $4d$ mit $d \equiv 3 \pmod 4$ bzw. $d \equiv 2 \pmod 8$ bzw. $d \equiv 6 \pmod 8$ und λ als $m + n\sqrt{d}$ mit $m, n \in \mathbb{Z}$. Dann erhalten wir:

$$D_i = -4 \Rightarrow N(\lambda) = m^2 - n^2 d \ , \ d \equiv 3 \pmod 4$$
$$\Rightarrow N(\lambda) \equiv 0 \ , \ 1 \ , \ 2 \pmod 4$$
$$\Rightarrow N(\lambda) \equiv 1 \pmod 4$$
$$\Rightarrow \chi_{-4}(N(\lambda)) = 1 \ .$$

$$D_i = 8 \Rightarrow N(\lambda) = m^2 - n^2 d \ , \ d \equiv 2 \pmod 8$$
$$\Rightarrow N(\lambda) \equiv 0 \ , \ 1 \ , \ 2 \ , \ 4 \ , \ 6 \ , \ 7 \pmod 8$$
$$\Rightarrow N(\lambda) \equiv 1 \ , \ 7 \pmod 8$$
$$\Rightarrow \chi_{8}(N(\lambda)) = 1 \ ,$$

$$D_i = -8 \Rightarrow N(\lambda) = m^2 - n^2 d \ , \ d \equiv 6 \pmod 8$$
$$\Rightarrow N(\lambda) \equiv 0 \ , \ 1 \ , \ 2 \ , \ 3 \ , \ 4 \ , \ 6 \pmod 8$$
$$\Rightarrow N(\lambda) \equiv 1 \ , \ 3 \pmod 8$$
$$\Rightarrow \chi_{-8}(N(\lambda)) = 1 \ ,$$

wobei wir $2 \nmid N(\lambda)$ benutzt haben. Damit ist (10) bewiesen, falls das Ideal (λ) zu D' oder D'' teilerfremd ist.

Sei jetzt $\lambda \in \mathfrak{O}$ beliebig: wir schreiben (λ) als

$$(\lambda) = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{b} \ ,$$

wobei die Primideale $\mathfrak{p}_j$ Teiler von D sind und $\mathfrak{b}$ zu D teilerfremd ist. Für jedes j wählen wir ein Ideal $\mathfrak{a}_j$ in der Idealklasse von $\mathfrak{p}_j^{-1}$, das zu D teilerfremd ist (dies ist immer möglich: s. Aufgabe 2). Dann ist für jedes j das Produkt $\mathfrak{p}_j \mathfrak{a}_j$ ein Hauptideal, das entweder zu D' oder zu D'' teilerfremd ist (da es nur einen Primfaktor enthält, der in D aufgeht), also ist nach dem bereits Bewiesenen

$$\chi(\mathfrak{p}_j \mathfrak{a}_j) = 1 \qquad (j = 1, \ldots, r) \ .$$

Wegen

$$(\lambda) = (\mathfrak{p}_1 \mathfrak{a}_1) \cdots (\mathfrak{p}_r \mathfrak{a}_r)(\mathfrak{b}\mathfrak{a}_1^{-1} \cdots \mathfrak{a}_r^{-1})$$

ist auch $\mathfrak{b}\mathfrak{a}_1^{-1} \cdots \mathfrak{a}_r^{-1}$ ein Hauptideal, und weil dieses Ideal zu D teilerfremd ist, gilt

$$\chi(\mathfrak{b}\mathfrak{a}_1^{-1} \cdots \mathfrak{a}_r^{-1}) = 1 \ .$$

Die Behauptung (10) folgt aus den letzten drei Gleichungen.

ii) Wir wollen jetzt Gleichung (9) beweisen. Das Euler-Produkt von $L_K(s,\chi)$ liefert

$$L_K(s,\chi) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \prod_{p} \prod_{\mathfrak{p} \mid p} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} \tag{12}$$

(das erste Produkt läuft über alle rationalen Primzahlen p, das zweite über Primideale $\mathfrak{p}$, die p teilen). Die Euler-Produkte von $L_{D'}$ und $L_{D''}$ geben

$$L_{D'}(s)L_{D''}(s) = \prod_{p} \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{D''}(p)}{p^s}\right)^{-1} \ . \tag{13}$$

Wir zeigen, daß für jede Primzahl p die entsprechenden Faktoren in (12) und (13) übereinstimmen.

Fall 1: $\chi_D(p) = 1$, $p = \mathfrak{p}\mathfrak{p}'$. Hier ist $\mathfrak{p}$ zu D' und zu D'' teilerfremd. Nach (7) gilt

$$\chi(\mathfrak{p}) = \chi_{D'}(N\mathfrak{p}) = \chi_{D'}(p) = \chi_{D''}(p)$$

und ebenfalls $\chi(\mathfrak{p}') = \chi_{D''}(p)$, also

$$\prod_{\mathfrak{p} \mid p} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{D''}(p)}{p^s}\right)^{-1} \ .$$

Fall 2: $\chi_D(p) = -1$, $p = \mathfrak{p}$. Hier ist $N(\mathfrak{p}) = p^2$, also $\chi(\mathfrak{p}) = 1$; andererseits ist $\chi_{D'}(p)\,\chi_{D''}(p) = \chi_D(p) = -1$, also ist eine der Zahlen $\chi_{D'}(p)$, $\chi_{D''}(p)$ gleich $+1$ und die andere gleich -1, also

$$\prod_{\mathfrak{p} \mid p} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \left(1 - \frac{1}{p^{2s}}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1}$$
$$= \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{D''}(p)}{p^s}\right)^{-1} \ .$$

Fall 3: $\chi_D(p) = 0$, $p = \mathfrak{p}^2$. Hier teilt p entweder D' oder D''. Wenn etwa $p|D''$, ist $(p,D') = 1$, also nach (7) ist $\chi(\mathfrak{p}) = \chi_{D'}(p)$. Dann gilt

$$\prod_{\mathfrak{p}|p}\left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1}$$

$$= \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1}\left(1 - \frac{\chi_{D''}(p)}{p^s}\right)^{-1},$$

das letztere wegen $\chi_{D''}(p) = 0$.

iii) Sei $D = D_1 \ldots D_t$ die Zerlegung von D in Primdiskriminanten und χ_i der der Zerlegung $D = D_i \cdot D_1 \ldots D_{i-1} D_{i+1} \ldots D_t$ zugeordnete Charakter. Dann ist für eine allgemeine Zerlegung $D = D' \cdot D''$ mit $D'' = D_{i_1} \ldots D_{i_s}$ der entsprechende Charakter χ gleich $\chi_{i_1} \cdots \chi_{i_s}$. Mit anderen Worten, die Charaktere, die wir schon konstruiert haben, bilden eine Gruppe, die von $\chi_1, \ldots, \chi_t$ erzeugt wird, wobei die Relationen $\chi_i^2 = 1$ und $\chi_1 \cdots \chi_t = 1$ gelten. Wir müssen zeigen, daß es zwischen den χ_i keine weiteren Relationen gibt, d.h., daß der Charakter χ, den wir einer Zerlegung $D = D'D''$ zugeordnet haben, nur dann der triviale Charakter ist, wenn $D' = 1$ oder $D'' = 1$. Aber das folgt unmittelbar aus (9): wenn D' und D'' beide $\neq 1$ sind, so sind die Funktionen $L_{D'}(s)$ und $L_{D''}(s)$ an der Stelle $s = 1$ holomorph, also hat $L_K(s,\chi)$ nach (9) auch keinen Pol bei $s = 1$ und χ kann nicht der triviale Charakter sein.

iv) Wie wir schon im Beweis des Korollars gesehen haben, gibt es genau 2^r Geschlechtscharaktere, wo $2^r = |C/C^2|$. Wir müssen also zeigen, daß $r \leq t - 1$.

Sei $Sq: C \to C$ die Abbildung, die eine Idealklasse auf ihr Quadrat schickt, dann hat man die exakte Folge

$$0 \to I \to C \xrightarrow{Sq} C \to C/C^2 \to 0$$

mit $I = \mathrm{Ker}(Sq)$. Da die Gruppen alle endlich sind, folgt $|I| = |C/C^2|$, d.h. es gibt gleich viele Idealklassen, deren Quadrat trivial ist, wie es Äquivalenzklassen modulo Quadraten gibt. Für $A \in C$ hat man wegen $A^{-1} = A'$

$$A \in I \iff A^2 = 1 \iff A = A^{-1} \iff A = A' .$$

Die Idealklassen, die gleich ihren konjugierten Klassen sind, nennt man *ambig* (sie entsprechen den am Ende von §11 definierten ambigen

Formen). Wir wollen zeigen, daß es höchstens 2^{t-1} solche Idealklassen gibt.

Zunächst bemerken wir, daß jede ambige Idealklasse ein Ideal $\mathfrak{a}$ mit $\mathfrak{a}' = \mathfrak{a}$ enthält. Dies folgt aus (5): Sei zunächst $\mathfrak{a} \in A$ beliebig; dann ist $\mathfrak{a}' \in A' = A$ in derselben Idealklasse wie $\mathfrak{a}$, also $\mathfrak{a}' = (\lambda)\mathfrak{a}$ mit $\lambda \in K$, $N(\lambda) = 1$. Nach (5) ist dann $\lambda = \mu/\mu'$ mit $\mu \in \mathfrak{o}$, wobei wir auch $N(\mu) > 0$ erreichen können (ist K imaginär, so ist dies sowieso erfüllt; ist K reell, so wählen wir λ positiv, also $\mu\mu' = \lambda\mu'^2 > 0$). Dann ist das Ideal $(\mu)\mathfrak{a} \in A$ gleich seinem Konjugierten.

Wir wählen also in der ambigen Idealklasse A ein Ideal $\mathfrak{a}$ mit $\mathfrak{a}' = \mathfrak{a}$. Durch Multiplikation mit einer geeigneten rationalen Zahl können wir erreichen, daß $\mathfrak{a}$ ein ganzes Ideal und außerdem *primitiv* ist (d.h. durch keine natürliche Zahl > 1 teilbar). Aber es gibt in K überhaupt nur 2^t ganze, primitive, ambige Ideale, nämlich die Produkte

$$\mathfrak{p}_1^{i_1} \ldots \mathfrak{p}_t^{i_t} \qquad (i_1, \ldots, i_t \in \{0,1\}) , \tag{14}$$

wobei $\mathfrak{p}_i$ $(i = 1, \ldots, t)$ das (eindeutig bestimmte) Primideal bezeichnet, das in D_i aufgeht. In der Tat: ein solches Ideal $\mathfrak{a}$ ist weder durch ein Primideal $\mathfrak{p}$ mit $\mathfrak{p} = (p)$, p träge, teilbar (weil dann $\mathfrak{a}$ durch die natürliche Zahl p teilbar wäre), noch kann in $\mathfrak{a}$ ein Primideal $\mathfrak{p}$ mit $\mathfrak{p} \neq \mathfrak{p}'$, $\mathfrak{p}\mathfrak{p}' = (p)$ vorkommen (da dann aus $\mathfrak{p}' | \mathfrak{a}' = \mathfrak{a}$ auch $p = \mathfrak{p}\mathfrak{p}' | \mathfrak{a}$ folgen würde, im Widerspruch zur Primitivität von $\mathfrak{a}$). Somit enthält $\mathfrak{a}$ lauter verzweigte Primideale und zwar jeweils höchstens zur ersten Potenz ($\mathfrak{p}^2 = p \Rightarrow \mathfrak{p}^2 \nmid \mathfrak{a}$). Jede ambige Idealklasse $A \in I$ enthält also mindestens eins der 2^t Ideale (14). Hieraus folgt schon, daß $2^r \leq 2^t$ ist; wenn wir unter den 2^t Idealen (14) ein einziges Ideal $\mathfrak{a} \neq 1$ finden können, das in der Hauptidealklasse liegt, so folgt sogar $2^r < 2^t$ und wir sind fertig. (Da wir schon wissen, daß $2^r \geq 2^{t-1}$ ist, kann es natürlich unter den Idealen (14) auch nicht mehr als ein solches $\mathfrak{a}$ geben.)

Ist $D < 0$, so folgt aus

$$\mathfrak{p}_1^2 \ldots \mathfrak{p}_t^2 = \prod_{p|D} p = \begin{cases} D, & \text{falls } D \equiv 1 \pmod 4 \\ 2d, & \text{falls } D = 4d,\ d \equiv 3 \pmod 4 \\ d, & \text{falls } D = 4d,\ d \equiv 2 \pmod 4, \end{cases}$$

daß man die Relation

$$(15)\qquad \begin{aligned} (\sqrt{D}) &= \mathfrak{p}_1 \dots \mathfrak{p}_t, && \text{falls } D \equiv 1 \pmod 4 \\ (\sqrt{d}) &= \mathfrak{p}_2 \dots \mathfrak{p}_t, && \text{falls } D = 4d,\ d \equiv 3 \pmod 4 \\ (\sqrt{d}) &= \mathfrak{p}_1 \dots \mathfrak{p}_t, && \text{falls } D = 4d,\ d \equiv 2 \pmod 4 \end{aligned}$$

hat, wobei wir im zweiten Fall die $\mathfrak{p}_i$ so numeriert haben, daß $\mathfrak{p}_1$ der Primteiler von 2 ist. Da die linke Seite von (15) jeweils ein Hauptideal ist, haben wir unsere nichttriviale Relation unter den $\mathfrak{p}_i$ in C gefunden.

Für $D > 0$ gelten die Gleichungen (15) auch, aber die linke Seite braucht kein Hauptideal im engeren Sinne mehr zu sein, da $\sqrt{D}$ (bzw. $\sqrt{d}$) negative Norm hat. Falls die Grundeinheit ε von K negative Norm hat, ist das Hauptideal $(\sqrt{D})$ bzw. $(\sqrt{d})$ durch die Zahl $\varepsilon\sqrt{D}$ bzw. $\varepsilon\sqrt{d}$ erzeugt, welche positive Norm hat; somit liefert (15) wieder die verlangte Relation. Falls der Körper K reell ist und die Grundeinheit ε *positive* Norm hat (also $\varepsilon\varepsilon' = 1$), setzen wir $\mu = (\varepsilon - 1)\sqrt{D}$ und finden

$$\mu' = -\varepsilon'\sqrt{D} + \sqrt{D} = (1 - \varepsilon^{-1})\sqrt{D} = \varepsilon^{-1}\mu ,$$

also $(\mu') = (\mu)$. Wir schreiben (μ) als $n\mathfrak{a}$, wobei n eine natürliche Zahl und $\mathfrak{a}$ primitiv ist. Wegen $\mathfrak{a}' = \mathfrak{a}$ muß sich $\mathfrak{a}$ unter den Idealen (14) befinden. Aber $\mathfrak{a}$ kann nicht 1 sein, denn aus $(\mu) = (n)$ würde

$$\mu = \pm n\varepsilon^r \qquad (r \in \mathbb{Z})$$

und daher

$$\varepsilon = \frac{\mu}{\mu'} = \frac{n\varepsilon^r}{n\varepsilon^{-r}} = \varepsilon^{2r}$$

folgen, ein Widerspruch. Die Gleichung $\mathfrak{a} = (n^{-1}\mu)$ liefert die gesuchte nicht-triviale Relation unter den Idealklassen $\mathfrak{p}_1, \dots, \mathfrak{p}_t$. Damit ist Satz 2 bewiesen.

Aus $C/C^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$ und dem Strukturatz für endliche abelsche Gruppen folgt, daß die Gruppe C/C^4 ($C^4 = \{A^4,\ A \in C\}$) zu $(\mathbb{Z}/2\mathbb{Z})^{t-1-s} \times (\mathbb{Z}/4\mathbb{Z})^s$ isomorph ist, wobei die Zahl s zwischen 0 und $t - 1$ liegt und durch

$$2^s = \#\{A \in C \mid A^2 = 1,\ A = B^2 \text{ für ein } B \in C\}$$

bestimmt wird, d.h. 2^s = Ordnung von $\mathrm{Ker}(Sq) \cap \mathrm{Im}(Sq)$. Für die Gruppen $\mathrm{Ker}(Sq)$ und $\mathrm{Im}(Sq)$ haben wir aber eine genaue Beschreibung gefunden: die Idealklassen aus $\mathrm{Ker}(Sq)$ werden durch die Ideale (14)

vertreten, und zwar jeweils genau zweimal, während $\mathrm{Im}(Sq)$ aus den $A \in C$ mit $\chi(A) = 1$ für alle Geschlechtscharaktere χ (oder nur $\chi_i(A) = 1$ für alle i) besteht. Wir können also s bestimmen, indem wir die Werte der χ_i auf den Idealen (14) berechnen. Das Ergebnis läßt sich wie folgt formulieren: sei $\varepsilon_{ij} \in \mathbb{Z}/2\mathbb{Z}$ für $1 \le i, j \le t$ durch

$$(-1)^{\varepsilon_{ij}} = \chi_i(\mathfrak{p}_j) = \begin{cases} \chi_{D_i}(p_j), & \text{falls } i \neq j \\ \prod\limits_{k \neq i} \chi_{D_k}(p_i), & \text{falls } i = j \end{cases}$$

($p_j = N(\mathfrak{p}_j)$) definiert; dann ist $t - 1 - s$ der Rang der Matrix $(\varepsilon_{ij})_{1 \le i,j \le t}$ über dem Körper $\mathbb{Z}/2\mathbb{Z}$.

Aufgaben:

1. Man zeige mit Hilfe von Satz 1: unter der Korrespondenz zwischen Idealklassen in K und Äquivalenzklassen von quadratischen Formen der Diskriminante D gehören zwei Idealklassen genau dann demselben Geschlecht an, wenn die entsprechenden Formen rational (d.h. durch eine Matrix aus $SL_2(\mathbb{Q})$) ineinander überführbar sind.

2. Man beweise: in jeder Idealklasse gibt es Ideale, die zu einem vorgegebenen Ideal teilerfremd sind. (Dies folgt natürlich aus der am Ende von §11 bewiesenen Existenz unendlich vieler Primideale in jeder Idealklasse, soll hier aber elementar gezeigt werden.)

3. Man verifiziere die am Ende des Paragraphen gemachten Behauptungen über C/C^4 und folgere:

$$\begin{aligned} h(D) &\equiv \pm 1 \pmod 4 \iff D = -4, +8, -8, +p, -q, \\ h(D) &\equiv 2 \pmod 4 \iff D = +4q, \pm 8p \quad (p \equiv 5 \pmod 8), +8q, \\ &\qquad\qquad -8q \quad (q \equiv 3 \pmod 8), \\ &\qquad\qquad +pp' \quad (\left(\tfrac{p'}{p}\right) = -1), \\ &\qquad\qquad -pq \quad (\left(\tfrac{q}{p}\right) = -1), +qq', \\ h(D) &\equiv 0 \pmod 4 \quad \text{sonst,} \end{aligned}$$

wobei p bzw. q Primzahlen $\equiv 1$ bzw. $\equiv 3 \pmod 4$ bezeichnen. Damit ist $h(D)$ modulo 4 in allen Fällen außer $D = +p$, $D = -q$ bestimmt.

Bemerkung: Wegen des Wilsonschen Satzes ist $[(\frac{q-1}{2})!]^2 \equiv 1 \pmod q$ für $q \equiv 3 \pmod 4$, also $(\frac{q-1}{2})! \equiv \pm 1 \pmod q$, während $[(\frac{p-1}{2})!]^2 \equiv -1 \pmod p$ für $p \equiv 1 \pmod 4$, also $(\frac{p-1}{2})! \equiv \pm t_0/2 \pmod p$, wobei (t_0,u_0) die kleinste positive Lösung von $t^2 - pu^2 = -4$ ist. Die Bestimmung von $h(D)$ modulo 4 wird dann durch

$$h(-q) \equiv 1 \pmod 4 \iff (\tfrac{q-1}{2})! \equiv -1 \pmod q \quad \text{oder} \quad q = 3$$

(Mordell, Amer. Math. Monthly 68 (1961), 145-146) bzw.

$$h(+p) \equiv 1 \pmod 4 \iff (\tfrac{p-1}{2})! \equiv -t_0/2 \pmod p$$

(Chowla, Proc. Nat. Acad. Sci. USA 47 (1961), 878) vervollständigt. Der Leser mag versuchen, die erste dieser Gleichungen mit Hilfe von Satz 4, §9, zu beweisen.

§13 Reduktionstheorie

In §§8-9 bestimmten wir die Anzahl der Äquivalenzklassen von Formen mit gegebener Diskriminante sowie die Anzahl der inäquivalenten Darstellungen einer natürlichen Zahl durch die Gesamtheit dieser Formen (nicht aber durch die einzelnen Formen). Neben diesen Anzahlen will man aber effektive Algorithmen haben, um

a) eine endliche Menge von Formen mit gegebener Diskriminante anzugeben, welche mindestens einen Vertreter jeder Äquivalenzklasse enthält,

b) zu entscheiden, ob zwei gegebene Formen äquivalent sind,

c) eine endliche Menge von Darstellungen einer gegebenen Zahl durch eine gegebene Form anzugeben, welche mindestens einen Vertreter jeder Äquivalenzklasse von Darstellungen enthält, und

d) zu entscheiden, ob zwei gegebene Darstellungen einer Zahl durch eine Form äquivalent sind.

Frage a) wurde in §8, Satz 1, beantwortet, indem gezeigt wurde, daß man von einer beliebigen Form durch Anwendung von Transformationen der Gestalt

$$(1) \qquad S_n = \begin{pmatrix} n & 1 \\ -1 & 0 \end{pmatrix} : ax^2+bxy+cy^2 \to (an^2-bn+c)x^2+(2an-b)xy+ay^2$$

nach endlich vielen Schritten zu einer Form $ax^2+bxy+cy^2$ mit

$$(2) \qquad -|a| < b \le |a| \le |c|$$

gelangt und daß es nur endlich viele solche Formen mit gegebener Diskriminante gibt.

Im Falle $D < 0$ können wir die Absolutbetragszeichen in (2) weglassen (da wir nur positiv difinite Formen betrachten) und außerdem im Falle $a = c$ annehmen, daß $b \ge 0$ ist (da $ax^2+bxy+ay^2$ zu $ax^2-bxy+ay^2$ äquivalent ist). Wir nennen eine positiv definite Form $ax^2+bxy+cy^2$ *reduziert*, falls

$$(3) \qquad -a < b \le a < c \quad \text{oder} \quad 0 \le b \le a = c \ ;$$

dann ist jede positiv definite Form zu einer reduzierten äquivalent. Umgekehrt behaupten wir, daß *die reduzierten positiv definiten Formen paarweise inäquivalent sind*; dies gibt nicht nur einen praktischen Weg zur Berechnung der Klassenzahlen negativer Diskriminanten, sondern auch eine Antwort auf Frage b) für definite Formen, nämlich, daß zwei definite Formen genau dann äquivalent sind, wenn sie zur selben reduzierten Form führen. Um die Behauptung zu beweisen, bemerken wir erst, daß für eine reduzierte Form f und $x,y \in \mathbb{Z}$, $(x,y) \neq (0,0)$,

$$(4) \qquad f(x,y) = ax^2 + bxy + cy^2 \ge a(x^2-|xy|+y^2) \ge a$$

gilt, also ist der erste Koeffizient a von f die kleinste durch f dargestellte Zahl. Eine Matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ führt aber f in eine Form f' mit erstem Koeffizienten $a' = f(\alpha,\gamma)$ über; ist also f' auch reduziert, so muß a' gleich a sein und daher (wenn man die Fälle mit Gleichheit in (4) betrachtet)

$$\begin{array}{lll} (\text{falls } c>a) & \alpha=\pm 1\ , & \gamma=0 \\ (\text{falls } c=a>b) & \alpha=\pm 1\ , & \gamma=0 \quad \text{oder} \quad \alpha=0\ , \ \gamma=\pm 1 \\ (\text{falls } c=a=b) & \alpha=\pm 1\ , & \gamma=0 \quad \text{oder} \quad \alpha=0\ , \ \gamma=\pm 1 \quad \text{oder} \quad \alpha\gamma=-1\ . \end{array}$$

Im ersten Fall ist $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \pm\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$, also ist der zweite Koeffizient b' von f' gleich $b + 2\beta a$, und aus $-a < b$, $b' \le a$ folgt $\beta = 0$ und $f' = f$. In den anderen zwei Fällen sieht man ebenfalls leicht, daß $f' = f$; in diesen Fällen braucht die Matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ nicht unbedingt gleich $\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ zu sein, da die reduzierten Formen $ax^2 + ay^2$ und $ax^2 + axy + ay^2$ zusätzliche Automorphismen haben.

Für definite Formen sind die Fragen c) und d) auch sehr leicht zu beantworten. Wegen der Identitäten

$$f(x,y) = a(x + \frac{b}{2a}y)^2 + \frac{|D|}{4a}y^2 = \frac{|D|}{4c}x^2 + c(\frac{b}{2c}x + y)^2$$

haben wir nämlich die a priori Schranken $|x| \le \sqrt{4nc/|D|}$ und $|y| \le \sqrt{4na/|D|}$ für die Lösungen von $f(x,y) = n$, womit c) beantwortet

ist, und d) ist vollkommen trivial, weil f (außer in den genannten Spezialfällen) überhaupt keine Automorphismen außer ±Id hat.

Im Falle von indefiniten Formen sind die Probleme a)-d) viel schwieriger, weil man keine a priori Schranken für die Koeffizienten der Übergangsmatrizen zwischen zwei gegebenen Formen oder für die Argumente in der Darstellung einer gegebenen Zahl durch eine gegebene Form hat. Zwar liefern die Formen, deren Koeffizienten (2) erfüllen, wieder eine Antwort auf a), aber diese ist jetzt unbefriedigend, weil man die Äquivalenzen zwischen diesen Formen nicht leicht beschreiben kann. Um eine befriedigende Antwort auf a) und b) zu erhalten, muß man andere Ungleichungen als (2) oder (3) wählen, um reduzierte Formen zu definieren. Dann erhält man zwar immer noch nicht - wie im definiten Fall - genau einen reduzierten Vertreter für jede Äquivalenzklasse (dies ist durch Ungleichungen für die Koeffizienten gar nicht zu erreichen), wohl aber eine vollständige Beschreibung der Äquivalenzen zwischen reduzierten Formen. Um das Ergebnis zu formulieren, definieren wir eine Transformation T von der Gesamtheit aller indefiniten Formen in sich selbst durch

$$(5) \qquad Tf = S_n f \ , \ n \in \mathbb{Z} \ , \ n > \frac{b+\sqrt{D}}{2a} > n - 1 \ ,$$

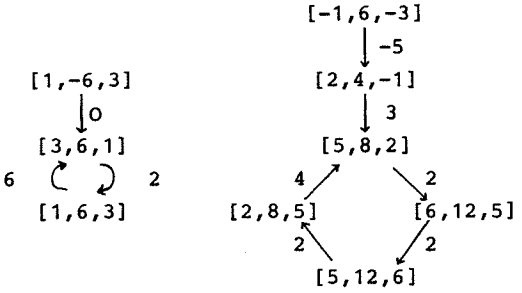
mit S_n wie in (1), wobei a, b, c die Koeffizienten von f sind und $\sqrt{D}$ die positive Wurzel von $D = b^2 - 4ac$ bezeichnet. Wir nennen eine indefinite Form $ax^2 + bxy + cy^2$ *reduziert*, falls

$$(6) \qquad a > 0 \ , \ c > 0 \ , \ b > a + c \ .$$

Dann gilt:

SATZ 1: *Sei* $D > 0$, D *kein Quadrat. Dann gibt es nur endlich viele reduzierte Formen der Diskriminante* D. *Jede Form der Diskriminante* D *wird durch endlich viele Anwendungen der Transformation* T *in eine reduzierte Form überführt. Die Transformation* T *führt reduzierte Formen in reduzierte über; somit zerfällt die Menge der reduzierten Formen in disjunkte Zykel. Jede Äquivalenz zwischen reduzierten Formen erhält man durch Iteration von* T; *insbesondere sind zwei reduzierte Formen dann und nur dann äquivalent, wenn sie zum selben Zykel gehören.*

Beispiel: Um festzustellen, ob die Form $x^2 - 6xy + 3y^2$ der Diskriminante 24 zu ihrer Negativen äquivalent ist, wenden wir die Transformation T wiederholt auf beide an und erhalten



wobei wir die Form $ax^2 + bxy + cy^2$ mit $[a,b,c]$ bezeichnet haben und $f \xrightarrow{n} f^*$ bedeutet, daß $f^* = Tf = S_n f$. Da wir in verschiedenen Zykeln landen, sind die Formen inäquivalent. Außerdem kann man nachprüfen, daß sich alle reduzierten Formen der Diskriminante 24 in einem der beiden Zykel befinden, also $h(24) = 2$.

Beweis des Satzes: Sei $[a,b,c]$ eine reduzierte Form und $k = b - 2a$. Dann ist

$$D - k^2 = b^2 - 4ac - (b-2a)^2 = 4a(b-a-c) > 0 \ .$$

Die reduzierten Formen sind also die Formen

$$(7) \quad [a,k+2a,k+a-\frac{D-k^2}{4a}] \ \text{ mit } \ |k|<\sqrt{D} \ , \ k^2 \equiv D \pmod 4 \ , \ a \Big| \frac{D-k^2}{4} \ , \ a > \frac{\sqrt{D}-k}{2} \ ,$$

und dies ist offenbar eine endliche Menge. Damit ist die erste Behauptung bewiesen.

Sei jetzt $f = [a,b,c]$ eine beliebige Form der Diskriminante D und $Tf = f^* = [a^*,b^*,c^*]$ ihr Bild unter T, also

$$(8) \qquad a^* = an^2 - bn + c \ , \ b^* = 2an - b \ , \ c^* = a$$

mit

$$(9) \qquad \frac{b+\sqrt{D}}{2a} = n - \theta \ , \ 0 < \theta < 1 \ .$$

Durch Substitution von (9) in (8) erhält man

$$(10) \qquad a^* = a\theta^2 + \theta\sqrt{D} \ , \ b^* = 2a\theta + \sqrt{D} \ , \ c^* = a \ .$$

Aus den ersten dieser Gleichungen folgt

$$a \geq 0 \Rightarrow a^* > 0 \ , \ a < 0 \Rightarrow a^* > a \ ,$$

d.h. unter wiederholter Anwendung von T wächst a so lange, bis es positiv wird, und bleibt dann positiv; wegen $c^* = a$ wird c nach höchstens einer weiteren Anwendung von T ebenfalls positiv. Da es nur endlich viele natürliche Zahlen unter einer gegebenen Zahl gibt, gelangt man nach endlich vielen weiteren Anwendungen von T zu einer Form $f = [a,b,c]$, für deren Nachfolger $a^* \geq a$ gilt. Für diese Form folgt aus (10)

$$0 \leq a^* - a = \theta\sqrt{D} - a(1-\theta^2)$$
$$< (1+\theta)(\sqrt{D}-a(1-\theta)) = \frac{1+\theta}{1-\theta}\,(b^*-a^*-c^*) ,$$

also ist der Nachfolger f^* von f reduziert und die zweite Behauptung des Satzes bewiesen.

Die dritte Behauptung beweist man analog: für eine reduzierte Form $f = [a,b,c]$ haben wir schon gesehen, daß $|b-2a| < \sqrt{D}$, also

$$\frac{b+\sqrt{D}}{2a} > 1 \ , \ \frac{b-\sqrt{D}}{2a} < 1 \ . \tag{11}$$

Somit ist die Zahl n in (9) mindestens 2 und es gilt

$$\frac{\sqrt{D}}{a} = n - \theta - \frac{b-\sqrt{D}}{2a} > 1 - \theta ,$$

also

$$b^* - a^* - c^* = (1-\theta)(\sqrt{D}-a(1-\theta)) > 0 ;$$

da wir schon wissen, daß a^* und c^* positiv sind, ist die Form $Tf = [a^*,b^*,c^*]$ wieder reduziert. Da die Menge der reduzierten Formen endlich ist, folgt, daß diese Menge unter der Operation von T in Zykel zerfällt. Es bleibt nur noch zu zeigen, daß es genau einen Zykel zu jeder Äquivalenzklasse von Formen gibt und daß sämtliche Äquivalenzen zwischen reduzierten Formen aus demselben Zykel durch Iteration von T entstehen.

Seien also $f = [a,b,c]$ und $f' = [a',b',c']$ zwei reduzierte Formen der Diskriminante D und $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ eine Matrix, die f in f' überführt. Aus der Formel (8.6) für die Koeffizienten von f' erhält man

$$a' = f(\alpha,\gamma) \ , \ c' = f(\beta,\delta) \ , \ a' + c' - b' = f(\alpha-\beta,\gamma-\delta) .$$

Da f' reduziert ist, sind die ersten beiden Zahlen positiv und die letzte negativ. Insbesondere ist $\gamma \neq \delta$ (sonst wäre $f(\alpha-\beta,\gamma-\delta)$ positiv); indem wir ggf. A durch $-A$ ersetzen, können wir annehmen, daß

$$\delta > \gamma . \tag{12}$$

Wir unterscheiden jetzt drei Fälle, je nach dem Vorzeichen von γ.

Fall I: $\gamma = 0$. Dann ist f' gleich f und $A = Id$. Aus $1 = \alpha\delta - \beta\gamma = \alpha\delta$ und (12) folgt nämlich $\alpha = \delta = 1$, also

$$f(\beta,1) = f(\beta,\delta) > 0 > f(\alpha-\beta,\gamma-\delta) = f(\beta-1,1) .$$

Diese Ungleichungen implizieren aber $\beta = 0$, denn für ein quadratisches Polynom $\phi(x)$ kann es höchstens eine ganze Zahl n mit $\phi(n-1) < 0 < \phi(n)$ geben.

Fall II: $\gamma < 0$. In diesem Fall behaupten wir, daß f' aus f durch wiederholte Anwendung von T entsteht und daß A das Produkt der entsprechenden Matrizen S_n ist. Sei nämlich $f^* = S_n f$ (n wie in (5)) das Bild von f unter T und

$$A^* = \begin{pmatrix} \alpha^* & \beta^* \\ \gamma^* & \delta^* \end{pmatrix} = S_n^{-1}A = \begin{pmatrix} -\gamma & -\delta \\ \alpha+n\gamma & \beta+n\delta \end{pmatrix}$$

die Matrix, die f^* in f' überführt. Die Matrix A^* erfüllt wieder (12) (es ist nämlich $\alpha^* - \beta^* = \delta - \gamma > 0$, und wegen $f(\alpha^*-\beta^*,\gamma^*-\delta^*) < 0$ haben $\alpha^* - \beta^*$ und $\gamma^* - \delta^*$ entgegengesetzte Vorzeichen). Wenn wir zeigen können, daß $\gamma < \gamma^* \leq 0$, so folgt unsere Behauptung mit vollständiger Induktion: in der Folge $\gamma < \gamma^* < \gamma^{**} < \ldots \leq 0$ muß irgendwann ein $\gamma^{*\cdots*}$ Null sein, und dann ist nach Fall I $f^{*\cdots*} = f'$ und die entsprechende Übergangsmatrix $A^{*\cdots*}$ die Identität. Wir müssen also die Ungleichungen $\gamma < \alpha + n\gamma \leq 0$ oder

$$n - 1 < \frac{\alpha}{-\gamma} \leq n \tag{13}$$

beweisen. Wegen $f(\alpha,\gamma) > 0 > f(\alpha-\beta,\gamma-\delta)$ hat das Polynom $f(x,-1) = ax^2 - bx + c$ bei $\frac{\alpha}{-\gamma}$ einen positiven und bei $\frac{\alpha-\beta}{-\gamma+\delta}$ einen negativen Wert; außerdem ist $\frac{\alpha}{-\gamma}$ größer als $\frac{\alpha-\beta}{-\gamma+\delta}$. Es folgt, daß die größere Wurzel von $f(x,-1) = 0$ zwischen diesen Zahlen liegt, also

$$\frac{\alpha-\beta}{-\gamma+\delta} < \frac{b+\sqrt{D}}{2a} < \frac{\alpha}{-\gamma} .$$

Wegen $n - 1 < \frac{b+\sqrt{D}}{2a}$ folgt hieraus sofort die erste der Ungleichungen (13). Für die zweite bemerken wir, daß aus $\frac{\alpha}{-\gamma} > n$ und $n > \frac{b+\sqrt{D}}{2a}$ die Ungleichungen $\frac{\alpha-\beta}{-\gamma+\delta} < n < \frac{\alpha}{-\gamma}$ folgen würden, also $-\alpha\gamma + \beta\gamma < n\gamma(\gamma-\delta) < -\alpha\gamma + \alpha\delta$, im Widerspruch zur Bedingung $\alpha\delta - \beta\gamma = 1$.

Fall III: $\gamma > 0$. In diesem Fall behaupten wir, daß f aus f' durch wiederholte Anwendung von T entsteht (d.h. man muß den Zykel im anderen Sinn durchlaufen) und daß A das Produkt der entsprechenden Matrizen S_n^{-1} ist. Da $A^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ einen negativen dritten Ko-

$S_n = \begin{pmatrix} 0 & 1 \\ -1 & n \end{pmatrix}$. by part 2, $S_n = \pm$ reduced, since $\frac{b+\sqrt{D}}{2a} > 1$ (see above) $\Rightarrow n \geq 2$

effizienten hat, folgt dies unmittelbar aus Fall II, wenn wir nachweisen, daß A^{-1} wieder (12) erfüllt, d.h. daß $\alpha > -\gamma$. Dies ist aber leicht: wegen $\frac{\alpha}{-\gamma} < \frac{\alpha-\beta}{-\gamma+\delta}$ und $f(\frac{\alpha}{-\gamma},-1) > 0 > f(\frac{\alpha-\beta}{-\gamma+\delta},-1)$ ist $\frac{\alpha}{-\gamma}$ kleiner als die kleinere Wurzel von $f(-x,1) = 0$, also mit (11)

$$\frac{\alpha}{-\gamma} < \frac{b-\sqrt{D}}{2a} < 1 \ , \ \alpha > -\gamma \ .$$

Damit ist die letzte Behauptung des Satzes bewiesen.

Satz 1 und sein Beweis sind sehr eng mit der Theorie der Kettenbrüche verbunden. Wir beschreiben jetzt diesen Zusammenhang.

Seien $n_0, n_1, n_2, \ldots$ ganze Zahlen mit $n_1, n_2, \ldots \geq 2$. Wir bezeichnen mit $[[n_0,n_1,\ldots,n_s]]$ den endlichen Kettenbruch

$$[[n_0,n_1,\ldots,n_s]] = n_0 - \cfrac{1}{n_1 - \cfrac{1}{n_2 - \ddots - \cfrac{1}{n_s}}}$$

und mit $[[n_0,n_1,n_2,\ldots]]$ den Limes $\lim_{s\to\infty}[[n_0,n_1,\ldots,n_s]]$, dessen Existenz leicht nachzuweisen ist. Dieser Limes ist eine reelle Zahl; umgekehrt hat jede reelle Zahl w eine eindeutige Kettenbruchentwicklung $w = [[n_0,n_1,n_2,\ldots]]$ mit $n_i \in \mathbb{Z}$ und $n_1, n_2, \ldots \geq 2$, indem man $n_0 = [w] + 1$, $w_1 = \frac{1}{n_0 - w}$ und induktiv $n_i = [w_i] + 1$, $w_{i+1} = \frac{1}{n_i - w_i}$ setzt. Somit gibt es eine eindeutige Korrespondenz zwischen der Menge der reellen Zahlen w und der Menge der Folgen $n_0, n_1, \ldots$ mit $n_0 \in \mathbb{Z}$, $n_1, n_2, \ldots \in \{2,3,\ldots\}$. Unter dieser Korrespondenz gilt:

i) $w \in \mathbb{Q} \iff$ ab einem bestimmten Punkt sind alle n_i gleich 2;

ii) w erfüllt eine quadratische Gleichung mit Koeffizienten in $\mathbb{Z} \iff$ ab einem bestimmten Punkt wiederholen sich die n_i periodisch (d.h. es gibt Zahlen $r \geq 1$ und $i_0 \geq 0$, so daß $n_{i+r} = n_i$ für alle $i \geq i_0$);

iii) w ist die größere Wurzel der quadratischen Gleichung $ax^2 - bx + c = 0$, wobei $[a,b,c]$ eine reduzierte quadratische Form positiver Diskriminante ist $\iff$ die Kettenbruchentwicklung von w ist rein periodisch (d.h. $n_{i+r} = n_i$ für alle $i \geq 0$).

Die erste Behauptung ist leicht zu beweisen (in der Richtung "$\Leftarrow$" sogar trivial, da $[[2,2,2,\ldots]]=1$). Die Richtung "$\Rightarrow$" der Behauptungen ii) und iii) ist in Satz 1 enthalten. Sei nämlich $f = [a,b,c]$ eine quadratische Form der Diskriminante $D > 0$ und

$$w = \frac{b+\sqrt{D}}{2a} \ , \ w' = \frac{b-\sqrt{D}}{2a} \tag{14}$$

die Wurzeln von $f(x,-1) = 0$. Ist $f^* = S_n f$ das Bild von f unter der Transformation T und w^* analog zu w definiert, so ist $n = [w] + 1$ und $w = n - \frac{1}{w^*}$, womit wir den Anfang der Kettenbruchentwicklung von w haben: ist $f_i = [a_i,b_i,c_i]$ $(i \geq 0)$ das Bild von f unter T^i, also $f_0 = f$, $f_1 = f^*$, $f_{i+1} = Tf_i = S_{n_i} f_i$ mit $n_i = \left[\frac{b_i+\sqrt{D}}{2a_i}\right] + 1 = [w_i]+1$, dann gilt $w_i = n_i - \frac{1}{w_{i+1}}$ und folglich $w = w_0 = [[n_0,n_1,n_2,\ldots]]$. Satz 1 sagt, daß es ein i_0 mit f_{i_0} reduziert gibt und daß die f_i für $i \geq i_0$ alle reduziert sind und sich periodisch wiederholen, insbesondere also $n_{i+r} = n_i$ für ein geeignetes r und alle $i \geq i_0$. Bevor wir die andere Richtung von ii) und iii) beweisen, bemerken wir, daß auch der letzte Teil von Satz 1, über die Äquivalenzen zwischen reduzierten Formen, sich gut in die Sprache der Kettenbrüche übertragen läßt: ist z.B. $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit $\delta > \gamma$ und $\gamma < 0$ eine Matrix in $SL_2(\mathbb{Z})$, welche die reduzierte Form f in eine reduzierte Form f' überführt, so gilt für ein geeignetes s (vgl. Fall II des Beweises oben)

$$f' = T^{s+1} f \ , \ A = S_{n_0} S_{n_1} \ldots S_{n_s} \ , \ \frac{\alpha}{-\gamma} = [[n_0,n_1,\ldots,n_s]] \ .$$

Für eine allgemeine, d.h. nicht notwendig reduzierte Form f, deren zugehörige Wurzel w die Kettenbruchentwicklung

$$w = [[n_0,n_1,\ldots,n_{i_0-1},\overline{n_{i_0},n_{i_0+1},\ldots,n_{i_0+r-1}}]] \tag{15}$$

besitzt (wobei der Strich über $n_{i_0}, \ldots, n_{i_0+r-1}$ bedeutet, daß die Zahlen sich periodisch wiederholen und daß r die kürzeste Periode ist), so folgt aus Satz 1, daß die Automorphismengruppe von f durch

$$U_f = \{\pm S_{n_0} S_{n_1} \ldots S_{n_{i_0-1}} (S_{n_{i_0}} \ldots S_{n_{i_0+r-1}})^N S_{n_{i_0-1}}^{-1} \ldots S_{n_0}^{-1} \mid N \in \mathbb{Z}\} \tag{16}$$

gegeben ist.

Wir beweisen jetzt die Richtung "$\Leftarrow$" der Behauptungen ii) und iii) oben. Die erste ist leicht. Hat nämlich die reelle Zahl w die Kettenbruchentwicklung (15) und ist $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ eine beliebige Matrix aus der Menge (16) mit $N \neq 0$ (also $A \neq \pm \mathrm{Id}$), so gilt $w = \frac{\alpha w-\beta}{-\gamma w+\delta}$, d.h. w ist eine Wurzel der quadratischen Gleichung $\gamma w^2+(\alpha-\delta)w-\beta = 0$. Die zweite ist eine formale Konsequenz von der ersten und von Satz 1. Ist nämlich w eine Zahl mit einer rein periodischen Kettenbruchentwicklung der Länge r, so ist w Wurzel einer quadratischen Form f; für

genügend großes N ist nach Satz 1 die Form $T^{Nr}f$ reduziert, hat aber eine Wurzel mit derselben Kettenbruchentwicklung wie w. Wir geben aber einen anderen, kettenbruchtheoretischen Beweis, der auf einer Tatsache von unabhängigem Interesse basiert: ist w eine Zahl mit einer reinperiodischen Kettenbruchentwicklung und w' die konjugierte Zahl (wir wissen bereits, daß w quadratisch ist), so gilt

$$(17) \qquad w = [[\overline{n_0,\dots,n_{r-1}}]] \quad \frac{1}{w'} = [[\overline{n_{r-1},\dots,n_0}]] \ .$$

Wegen $n_i \geq 2$ folgen aus (17) für eine Zahl w mit rein periodischer Kettenbruchentwicklung die Ungleichungen

$$(18) \qquad w > 1 \ , \ 0 < w' < 1 \ ,$$

die damit äquivalent sind, daß die quadratische Form mit den Wurzeln w und w' reduziert ist (vgl. (11)). Um (17) einzusehen, setzen wir die Folge $\{n_i\}$ durch $n_{i+r} = n_i$ $(\forall i \in \mathbb{Z})$ periodisch fort und setzen für alle i

$$x_i = 1/[[\overline{n_{i-1},n_{i-2},\dots,n_{i-r}}]] \ .$$

Dann gilt $\frac{1}{x_{i+1}} = n_i - x_i$ oder $x_i = n_i - \frac{1}{x_{i+1}}$, also erfüllt x_0 die quadratische Gleichung

$$x_0 = n_0 - \cfrac{1}{n_1 - \cfrac{1}{\ddots - \cfrac{1}{n_{r-1} - \cfrac{1}{x_0}}}} \ .$$

Dies ist aber dieselbe Gleichung, die w erfüllt, und da x_0 wegen $x_0 < 1 < w$ nicht gleich w sein kann, muß $x_0 = w'$ gelten, was zu beweisen war.

Wir haben diesen Paragraphen mit vier Fragen über quadratische Formen und Darstellungen von Zahlen durch Formen begonnen, die im definiten Fall alle leicht zu lösen waren. Für den indefiniten Fall wurden die beiden Fragen nach einem Verfahren zur Bestimmung der Äquivalenzklassen von Formen durch Satz 1 beantwortet. Die Antwort auf die beiden Fragen (nach der Beschreibung der Äquivalenzklassen von Darstellungen einer natürlichen Zahl durch eine indefinite Form) wird durch den folgenden Satz gegeben, der sich im Unterschied zu Satz 1 nicht in der klassischen Literatur zu befinden scheint.

SATZ 2: *Sei* $\{f_1,\dots,f_r\}$ *der in Satz 1 konstruierte Zykel der reduzierten Formen in der Äquivalenzklasse einer indefiniten quadratischen Form* f *und sei* n *eine natürliche Zahl. Dann ist jede Darstellung von* n *durch* f *zu genau einer Darstellung* $n = f_i(x,y)$ *mit* $1 \leq i \leq r$, $x > 0$, $y \geq 0$ *äquivalent.* (Hierbei bedeutet Äquivalenz von Darstellungen $n = f(x,y) = f'(x',y')$ durch verschiedene Formen f und f', daß es eine Matrix gibt, die f in f' und (x,y) in (x',y') überführt; um einen vollen Satz von Darstellungen von n durch f selbst zu erhalten, müssen wir auf jede Darstellung im Satz eine Matrix anwenden, welche f_i in f überführt.)

Wir bemerken, daß die Koeffizienten von $f_i = [a_i,b_i,c_i]$ positiv sind und daher für eine Darstellung $n = f_i(x,y)$ mit x und y nichtnegativ die a priori Abschätzungen $x \leq \sqrt{n/a_i}$, $y \leq \sqrt{n/c_i}$ bestehen; es gibt also nur endlich viele solche Darstellungen, und diese lassen sich effektiv (und sogar leicht) bestimmen.

Beweis: Wir numerieren die f_i so, daß $f_{i+1} = Tf_i = S_{n_i}f_i$, also $f_i(x,y) = a_i(x+yw_i)(x+yw_i')$ mit

$$w_i = \frac{b_i+\sqrt{D}}{2a_i} = [[\overline{n_i,n_{i+1},\dots,n_{i+r-1}}]] = n_i - \frac{1}{w_{i+1}}$$

(hierbei ist i modulo r zu verstehen, also $f_{i+r} = f_i$, $n_{i+r} = n_i$, $w_{i+r} = w_i$ für alle $i \in \mathbb{Z}$). O.B.d.A. können wir annehmen, daß f gleich f_0 $(=f_r)$ ist. Von einer gegebenen Darstellung

$$n = f(x_0,y_0)$$

ausgehend erhalten wir unendlich viele äquivalente Darstellungen

$$(19) \qquad n = f_i(x_i,y_i) \quad (i \in \mathbb{Z})$$

mit $\begin{pmatrix} x_i \\ y_i \end{pmatrix} = S_{n_i}\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix}$. Sei $\xi_i = x_i + y_iw_i$; dann ist (19) zu $n = a_i\xi_i\xi_i'$ $(\xi_i'$ die Konjugierte von $\xi_i)$ äquivalent. Insbesondere haben ξ_i und ξ_i' dasselbe Vorzeichen, das wegen

$$(20) \qquad \xi_i = x_i + y_i(n_i - \frac{1}{w_{i+1}}) = \frac{1}{w_{i+1}}\,\xi_{i+1}$$

von i unabhängig ist. Da $(x,y) \mapsto (-x,-y)$ ein Automorphismus von f ist und wir uns nur für die Äquivalenzklassen von Darstellungen interessieren, können wir annehmen, daß dieses Vorzeichen positiv ist, also $\xi_i, \xi_i' > 0$. Wegen (20) und $w_i > 1 > w_i' > 0$ gilt

$$\frac{\xi_i}{\xi_i'} < \frac{\xi_{i+1}}{\xi_{i+1}'} \ , \ \lim_{i\to\infty} \frac{\xi_i}{\xi_i'} = \infty \ , \ \lim_{i\to-\infty} \frac{\xi_i}{\xi_i'} = 0 \ ,$$

also gibt es genau ein $i \in \mathbb{Z}$ mit

$$\frac{\xi_i}{\xi_i'} \geq 1 > \frac{\xi_{i-1}}{\xi_{i-1}'} \ . \tag{21}$$

Aber $\xi_i - \xi_i'$ ist gleich $y_i(w_i - w_i')$ und $w_i - w_i'$ ist positiv, also ist $\xi_i/\xi_i' \geq 1$ zu $y_i \geq 0$ äquivalent und entsprechend $\xi_{i-1}/\xi_{i-1}' < 1$ zu $x_i = -y_{i-1} > 0$. Somit ist $n = f_i(x_i,y_i)$ für das durch (21) definierte i die zu $n = f(x_0,y_0)$ äquivalente Darstellung, deren Existenz im Satz behauptet wird. Die Eindeutigkeit folgt aus der Eindeutigkeit von i in (21) und der Tatsache, daß die volle Automorphismengruppe von f von $-Id$ und $\prod_{i=1}^{r} S_{n_i}$ erzeugt wird. Damit ist Satz 2 bewiesen.

Die Aussage von Satz 2 gibt die Formel

$$R(n,f) = \sum_{i(\mathrm{mod}\ r)} \sum_{\substack{x,y\in\mathbb{Z} \\ x>0,y>0 \\ f_i(x,y)=n}} 1 \qquad (n \in \mathbb{N})$$

für die in §8 betrachteten Darstellungsanzahlen $R(n,f)$. Aus §10 wissen wir, daß $\sum_{n=1}^{\infty} R(n,f)n^{-s} = \zeta(A,s)$, wobei A die Idealklasse ist, die unter der dort aufgestellten Korrespondenz der Form f entspricht. Satz 2 ist also zu der Identität

$$\zeta(A,s) = \sum_{i(\mathrm{mod}\ r)} \sum_{\substack{x,y\in\mathbb{Z} \\ x>0,y\geq 0}} \frac{1}{f_i(x,y)^s} \qquad (\mathrm{Re}(s) > 1)$$

äquivalent. Es wird sich als bequemer herausstellen, die Bedingungen an x und y durch die symmetrischeren Bedingungen

$$x \geq 0 \ , \ y \geq 0 \ , \ (x,y) \neq (0,0)$$

zu ersetzen; da die Dastellungen $n = f_i(x,0)$ und $n = f_{i+1}(0,x)$ aber äquivalent sind, werden die Darstellungen mit $x = 0$ oder $y = 0$ dadurch zweimal gezählt. Satz 2 ist also zu folgendem Satz über Dirichletsche Reihen äquivalent:

SATZ 2': *Sei A eine Idealklasse in einem reell-quadratischen Körper. Dann gilt*

$$\zeta(A,s) = \sum_{f} Z_f(s) \qquad (s \in \mathbb{C},\ \mathrm{Re}(s) > 1) \ ,$$

wobei die Summation über den Zykel von reduzierten Formen f läuft, welcher der Klasse A entspricht, und $Z_f(s)$ durch

$$Z_f(s) = \sum_{x,y>0} \frac{1}{f(x,y)^s} + \frac{1}{2} \sum_{x>0} \frac{1}{f(x,0)^s} + \frac{1}{2} \sum_{y>0} \frac{1}{f(0,y)^s} \qquad (\mathrm{Re}(s) > 1) \tag{22}$$

definiert wird.

Dieser Satz wird im nächsten Paragraphen benutzt werden, um $\zeta(A,0)$ zu berechnen.

Aufgaben:

1. Man beweise das Analogon zu Satz 1 für Äquivalenzklassen im weiteren Sinne von indefiniten Formen, wobei "reduziert" jetzt durch die Ungleichungen

$$w > 1 \ , \ 0 > w' > -1 \qquad \left(w = \frac{b+\sqrt{D}}{2a}\right) \tag{23}$$

(statt (17)) definiert wird und T durch die Transformation

$$T^+f = S_m^+ f \ , \ S_m^+ = \begin{pmatrix} m & -1 \\ -1 & 0 \end{pmatrix} \ , \ m < \frac{b+\sqrt{D}}{2a} < m+1 \tag{24}$$

zu ersetzen ist. Man führe dieses Reduktionsverfahren für das Beispiel nach Satz 1 (also Äquivalenz von $[1,-6,3]$ und $[-1,6,-3]$, jetzt im weiteren Sinne) aus.

2. Man zeige die Äquivalenz des Reduktionsverfahrens von Aufgabe 1 mit der Entwicklung von w in einen Kettenbruch der Gestalt

$$w = [[m_0,m_1,\ldots]]^+ := m_0 + \cfrac{1}{m_1 + \cfrac{1}{m_2 + \ddots}}$$

mit $m_i \in \mathbb{Z}$, $m_i \geq 1$ für $i \geq 1$: Die Folge $\{m_i\}$ ist für jede quadratische Irrationalität w nach einem bestimmten Punkt periodisch und ist genau dann rein periodisch, wenn w (23) erfüllt.

3. Man zeige, daß der Übergang zwischen den beiden Sorten von Kettenbrüchen durch

$$[[m_0,m_1,m_2,\ldots]]^+ = [[m_0+1,\underbrace{2,\ldots,2}_{m_1-1},m_2+2,\underbrace{2,\ldots,2}_{m_3-1},m_4+2,\ldots]]$$

$$(m_i \in \mathbb{Z},\ m_1,m_2,\ldots \geq 1)$$

gegeben wird.

4. Man zeige mit Hilfe von Aufgabe 3, daß eine Idealklasse im weiteren Sinne gleich einer Idealklasse im engeren Sinne ist oder in zwei solche zerfällt, je nachdem, ob die Länge s der zugehörigen Kettenbruchperiode $[[\overline{m_1,m_2,\dots,m_s}]]^+$ ungerade oder gerade ist.

5. Man bestimme die Zykel von reduzierten Formen (im engeren sowie im weiteren Sinne) für alle positiven Diskriminanten < 30.

§14 Werte von Zetafunktionen bei $s = 0$, Kettenbrüche und Klassenzahlen

Das Ziel dieses Paragraphen ist der Beweis der beiden folgenden Ergebnisse, die als schöne Anwendung eine Beziehung zwischen Klassenzahlen imaginärquadratischer Zahlkörper und Kettenbruchentwicklungen reellquadratischer Zahlen haben werden.

SATZ 1: *Sei* $f(x,y)$ *eine indefinite quadratische Form mit positiven Koeffizienten und* $Z_f(s)$ *die für* $\mathrm{Re}(s) > 1$ *durch Gleichung (22), §13, definierte Zetafunktion. Dann läßt sich* $Z_f(s)$ *auf die Halbebene* $\mathrm{Re}(s) > -\frac{1}{2}$ *bis auf einen einfachen Pol bei* $s = 1$ *holomorph fortsetzen und es gilt:*

$$Z_f(0) = \frac{1}{24}\left(\frac{b}{a} + \frac{b}{c} - 6\right).$$

SATZ 2: *Sei* A *eine Idealklasse in einem reellquadratischen Zahlkörper und* $n_1,\dots,n_r$ $(n_i \geq 2)$ *die Zahlen aus der minimalen Periode der Kettenbruchentwicklung der größeren Wurzel irgendeiner Form aus der Äquivalenzklasse, welche* A *entspricht. Dann gilt für die Zetafunktion der Idealklasse* A

$$\zeta(A,0) = \frac{1}{12}\sum_{i=1}^{r}(n_i - 3).$$

Satz 2 ist eine leichte Folgerung aus Satz 1 und der Ergebnissen von §13. Aus letzteren folgt nämlich, daß (bei passender Numerierung) die reduzierten Formen aus der der Idealklasse A entsprechenden Äquivalenzklasse von Formen durch

$$f_i(x,y) = a_ix^2+b_ixy+c_iy^2\ ,\ \frac{b_i+\sqrt{D}}{2a_i} = [[\overline{n_i,n_{i+1},\dots,n_{i+r-1}}]]$$

gegeben werden (wir denken uns die Numerierung periodisch fortgesetzt, also $n_{i+r} = n_i$, $f_{i+r} = f_i$). Aus Satz 3 von §13 und Satz 1 folgt dann unter Verwendung der Periodizität

$$\begin{aligned}\zeta(A,0) &= \sum_{i=1}^{r} Z_{f_i}(0)\\ &= \frac{1}{24}\sum_{i=1}^{r}\left(\frac{b_i}{a_i} + \frac{b_i}{c_i} - 6\right)\\ &= \frac{1}{24}\sum_{i=1}^{r}\left(\frac{b_i}{a_i} + \frac{b_{i+1}}{c_{i+1}} - 6\right)\end{aligned}$$

Wegen $f_{i+1} = S_{n_i}f_i$ ist aber $c_{i+1} = a_i$, $b_{i+1} = 2n_ia_i - b_i$ (vgl. §13, (1)), also $\frac{b_i}{a_i} + \frac{b_{i+1}}{c_{i+1}} = 2n_i$, womit Satz 2 bewiesen ist.

Zum Beweis von Satz 1 verwenden wir das allgemeine Ergebnis über analytische Fortsetzung und spezielle Werte von Dirichletschen Reihen, das in §7 als Satz 1 formuliert wurde (bzw. die in der zweiten Bemerkung danach formulierte Ergänzung, falls die Koeffizienten von f nicht ganz, sondern nur reell sind). Dieser Satz besagt in unserem Fall: falls die Funktion

$$V_f(t) = \sum_{x,y>0} e^{-f(x,y)t} + \frac{1}{2}\sum_{x>0} e^{-f(x,0)t} + \frac{1}{2}\sum_{y>0} e^{-f(0,y)t} \qquad (t > 0)$$

für $t \to 0$ eine asymptotische Entwicklung der Gestalt

$$(1) \qquad V_f(t) \sim \frac{C}{t} + C_0 + C_1t + \dots \qquad (t \to 0)$$

besitzt, so ist $Z_f(s)$ meromorph auf ganz $\mathbb{C}$ fortsetzbar, $Z_f(s) - \frac{C}{s-1}$ ist ganz und $Z_f(-n) = (-1)^n n!C_n$ $(\forall\, n \geq 0)$. Aus seinem Beweis sehen wir allerdings, daß es für die schwächere Aussage von Satz 1 (analytische Fortsetzbarkeit nur bis $\mathrm{Re}(s) = -\frac{1}{2}$ und Wert bei $s = 0$) genügt, die schwächere asymptotische Formel

$$(2) \qquad V_f(t) = \frac{C}{t} + C_0 + \mathbf{O}(t^{\frac{1}{2}})$$

mit irgendeinem C und mit $C_0 = \frac{1}{24}\left(\frac{b}{a} + \frac{b}{c} - 6\right)$ zu beweisen. In der Tat gilt (1); da wir uns aber nur für den Wert von $Z_f(0)$ interessieren, werden wir uns mit dem schwächeren Resultat (2) begnügen.

Um die volle asymptotische Formel für $V_f(t)$ zu erhalten, benutzt man die sogenannte Euler-Maclaurin Summationsformel, oder vielmehr eine Verallgemeinerung von ihr auf Funktionen von zwei Variablen, welche ein allgemeines Rezept zur Berechnung von Summen der Gestalt $\sum_{x,y>0} F(x,y)$ liefert. Da wir aber nur das schwächere Ergebnis (2) im Sinne haben, werden wir nur die ersten Glieder aus dieser Summations-

formel benutzen, wodurch unser Beweis allerdings einen etwas künstlichen Aspekt erhalten wird.

Sei also $F(u,v)$ irgendeine glatte und im Unendlichen sehr kleine Funktion auf $[0,\infty)\times[0,\infty)$. Für $x, y \geq 1$ bilden wir den Ausdruck

$$G(x,y) = \frac{1}{4}[F(x,y)+F(x-1,y)+F(x,y-1)+F(x-1,y-1)] - \int_{x-1}^{x}\int_{y-1}^{y} F(u,v)dudv$$

$$+ \frac{1}{12}\int_{x-1}^{x}[F_v(u,y-1)-F_v(u,y)]du + \frac{1}{12}\int_{y-1}^{y}[F_u(x-1,v)-F_u(x,v)]dv \quad (3)$$

wobei $F_u(u,v) = \frac{\partial F}{\partial u}(u,v)$, $F_v(u,v) = \frac{\partial F}{\partial v}(u,v)$. Die Koeffizienten in diesem Ausdruck sind so gewählt, daß $G(x,y)$ gleichzeitig besonders klein und besonders leicht summierbar ist. Entwickelt man nämlich $F(u,v)$ in dem Viereck $x-1 \leq u \leq x$, $y-1 \leq v \leq y$ in eine Taylorreihe, so sieht man, daß die Ableitungen von F bis zur zweiten Ordnung in (3) wegfallen (z.B. ist G identisch 0, falls F ein Polynom vom Grad ≤ 2 ist); andererseits haben wir

$$\sum_{x=1}^{\infty}\sum_{y=1}^{\infty} G(x,y) = \frac{1}{4}F(0,0) + \frac{1}{2}\sum_{x>0} F(x,0) + \frac{1}{2}\sum_{y>0} F(0,y) + \sum_{x,y>0} F(x,y)$$

$$- \int_0^\infty\int_0^\infty F(u,v)dudv + \frac{1}{12}\int_0^\infty F_v(u,0)du + \frac{1}{12}\int_0^\infty F_u(0,v)dv .$$

Wendet man diese Formel auf die Funktion $F_t(u,v) = e^{-f(u,v)t}$ an, so findet man für die entsprechende Funktion G_t

$$\sum_{x,y>0} G_t(x,y) = \frac{1}{4} + V_f(t) - \int_0^\infty\int_0^\infty e^{-f(u,v)t}dudv$$

$$- \frac{bt}{12}\left(\int_0^\infty ue^{-au^2t}du + \int_0^\infty ve^{-cv^2t}dv\right)$$

$$= V_f(t) - \frac{C}{t} - C_0$$

mit $C = \int_0^\infty\int_0^\infty e^{-f(u,v)}dudv$ und $C_0 = \frac{1}{24}(\frac{b}{a}+\frac{b}{c}) - \frac{1}{4}$. Um (2) zu beweisen, müssen wir also nur noch zeigen, daß $\sum_{x,y>0} G_t(x,y) = \mathbf{O}(t^{-\frac{1}{2}})$ für $t \to 0$.

Dies ist aber sehr leicht. Nach dem Taylorschen Satz (in zwei Veränderlichen) haben wir nämlich für feste $x, y \geq 1$ eine Zerlegung $F = P + \tilde{F}$, wobei P ein Polynom vom Grad ≤ 2 in u und v ist und $\tilde{F}$ sowie ihre beiden ersten Ableitungen in dem Viereck

$x-1 \leq u \leq x$, $y-1 \leq v \leq y$ durch absolute Konstanten mal

$$M_F^{(3)}(x,y) = \max_{\substack{x-1\leq u\leq x\\ y-1\leq v\leq y}} \max_{0\leq i\leq 3} \left|\frac{\partial^3 F(u,v)}{\partial u^i \partial v^{3-i}}\right|$$

abgeschätzt werden. (Wählt man für P z.B. den quadratischen Anteil der Taylorentwicklung von F im Punkt $(x-\frac{1}{2},y-\frac{1}{2})$, so gilt $|\tilde{F}| \leq \frac{1}{6}M_F^{(3)}$, $|\tilde{F}_u|$, $|\tilde{F}_v| \leq \frac{1}{2}M_F^{(3)}$ in dem Viereck.) Andererseits ist, wie schon bemerkt, der Ausdruck (3) so beschaffen, daß er für quadratische Polynome identisch verschwindet. (Der Leser kann dies schnell verifizieren, indem er diesen Ausdruck für die 6 Monome vom Grad ≤ 2 berechnet; für $F(u,v) = u^2$ ist z.B. $G(x,y) = \frac{1}{2}[x^2+(x-1)^2] - \frac{1}{3}[x^3-(x-1)^3] + \frac{1}{6}[(x-1)-x] = 0$. Tatsächlich verschwindet G für alle Polynome F vom Grad ≤ 3, wie man ebenso leicht verifiziert; diese stärkere Aussage würde (2) mit $\mathbf{O}(t)$ statt $\mathbf{O}(t^{\frac{1}{2}})$ und damit die analytische Fortsetzung von Z_f bis $\mathrm{Re}(s) = -1$ liefern.) Hieraus folgt, daß $G(x,y)$ ebenfalls durch eine absolute Konstante ($\frac{1}{2}$, falls man P wie oben wählt) mal $M_F^{(3)}(x,y)$ abgeschätzt wird. Wir wenden dies auf die spezielle Funktion $F_t(u,v) = e^{-f(u,v)t} = F_1(u\sqrt{t},v\sqrt{t})$ an. Dann haben die dritten Ableitungen von F_1 die Gestalt

$$(\text{Polynom von Grad} \leq 3 \text{ in } u,v) \times F_1$$

und daher die von F_t die Gestalt

$$t^{\frac{3}{2}} \times (\text{Polynom vom Grad} \leq 3 \text{ in } u\sqrt{t},\ v\sqrt{t}) \times F_t ,$$

also

$$M_{F_t}^{(3)}(x,y) \leq K \max_{i+j\leq 3} x^i y^j t^{\frac{3+i+j}{2}} e^{-f(x-1,y-1)t}$$

mit einer nur von f abhängigen Konstanten K. Es gilt aber

$$t^{\frac{3}{2}+\frac{i+j}{2}} \sum_{x,y>0} x^i y^j e^{-f(x-1,y-1)t} = \mathbf{O}\left(t^{\frac{3}{2}+\frac{i+j}{2}} \int_0^\infty\int_0^\infty x^i y^j e^{-f(x,y)t}dxdy\right)$$

$$= \mathbf{O}(t^{\frac{1}{2}}) .$$

Damit ist Satz 1 bewiesen.

Wir schließen mit einem Ergebnis, das rein arithmetisch ist, in dessen Beweis aber sämtliche algebraischen und analytischen Hilfsmittel, die in diesem Buch entwickelt wurden, eingehen.

SATZ 3: *Sei*

$$\sqrt{p} = n_0 - \cfrac{1}{n_1 - \cfrac{1}{n_2 - \ddots - \cfrac{1}{n_r - \cfrac{1}{n_1 - \cfrac{1}{n_2 - \ddots}}}}}$$

(minimale Periode)

die Kettenbruchentwicklung der Quadratwurzel einer Primzahl $p \equiv 3 \pmod 4$, $p \neq 3$, *für die die Klassenzahl im weiteren Sinne von* $\mathbb{Q}(\sqrt{p})$ *gleich* 1 *ist. Dann ist die Klassenzahl von* $\mathbb{Q}(\sqrt{-p})$ *gleich* $\frac{1}{3}(n_1 + \ldots + n_r) - r$.

Als Beispiele für den Satz haben wir

$$\sqrt{7} = [[3,\overline{3,6}]] \ , \ h(-7) = \tfrac{1}{3}(3+6) - 2 = 1 \ ,$$

$$\sqrt{11} = [[4,\overline{2,2,8}]] \ , \ h(-11) = \tfrac{1}{3}(2+2+8) - 3 = 1 \ ,$$

$$\sqrt{163} = [[13,\overline{5,2,2,4,3,2,2,2,2,2,2,3,2,2,2,2,2,2,2,2,2,2,2,3,2,2,2,2,2,2,3,4,2,2,5,26}]],$$

$$h(-163) = \tfrac{1}{3}(5+2+2+4+3+6\times 2+3+10\times 2+3+10\times 2+3+6\times 2+3+4+2+2+5+26) - 35 = 1 \ .$$

Wie in §9 erwähnt, ist die Primzahl 163 die größte Zahl p mit $h(-p) = 1$; dagegen ist die Klassenzahl von $\mathbb{Q}(\sqrt{+p})$ vermutlich für unendlich viele, jedenfalls für viele Tausende Primzahlen $p \equiv 3 \pmod 4$ gleich 1, so daß der Satz nicht leer ist. Daß die Kettenbruchentwicklung von $\sqrt{p}$ die im Satz behauptete Gestalt hat (also rein periodisch nach dem ersten Glied, übrigens mit $n_r = 2n_0$) folgt daraus, daß die Zahl $w = \sqrt{p} + n_0 = \sqrt{p} + [\sqrt{p}] + 1$ die Ungleichungen (18) aus §13 erfüllt.

Beweis des Satzes: Wir werden Satz 2 auf Geschlechtscharaktere anwenden. Ist χ irgendein Charakter auf der Idealklassengruppe C (im engeren Sinne) eines reellquadratischen Körpers K, so liefert Satz 2 die analytische Fortsetzung von der L-Reihe

$$L_K(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{A \in C} \chi(A)\, \zeta(A,s) \qquad (\mathrm{Re}(s) > 1)$$

auf die punktierte Halbebene $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > -\frac{1}{2},\ s \neq 1\}$ und gibt ihren Wert bei $s = 0$ als eine endliche Summe

$$(4) \qquad L_K(0,\chi) = \frac{1}{12} \sum_{A \in C} \chi(A) \sum_{i=1}^{r(A)} (n_i(A) - 3)$$

an, wobei $\{n_i(A)\}_{1 \le i \le r(A)}$ der A zugehörige Zykel ist. Wenn aber χ ein Geschlechtscharakter ist, haben wir schon einen Ausdruck für $L_K(0,\chi)$: nach dem Hauptsatz von §12 entspricht χ einer Zerlegung der Diskriminante von K als Produkt zweier Diskriminanten D' und D'' und es gilt $L_K(s,\chi) = L_{D'}(s) L_{D''}(s)$, andererseits wurden $L_{D'}(0)$ und $L_{D''}(0)$ in §7 berechnet. Falls D' und D'' positiv sind, ist nach dem Korollar in §7 mindestens einer der Werte $L_{D'}(0)$ und $L_{D''}(0)$ gleich Null (beide, falls D' und D'' ungleich 1 sind) und wir haben $L_K(0,\chi) = 0$. (Dies folgt allerdings auch aus (4), denn in diesem Fall gilt $\chi(\theta) = +1$ und daher $\chi(A\theta) = \chi(A)$, wobei $\theta \in C$ die aus den Hauptidealen (λ) mit $N(\lambda) < 0$ bestehende Idealklasse bezeichnet. Beim Übergang von A nach θA ändert sich aber das Vorzeichen der Invarianten $\sum_{i=1}^{r(A)} (n_i(A)-3)$; s. Aufgabe 3.) Falls dagegen D' und D'' negativ sind, so haben wir aus Gleichung (8) von §7 und Gleichung (9) (Satz 3) von §9

$$L_{D'}(0) = -\frac{1}{|D'|} \sum_{n=1}^{|D'|-1} \chi_{D'}(n) n = \frac{h(D')}{\frac{1}{2}w(D')} \ ,$$

wobei $h(D')$ die Klassenzahl und

$$w(D') = \begin{cases} 6 & (D' = -3) \\ 4 & (D' = -4) \\ 2 & (D' < -4) \end{cases}$$

die Anzahl der Einheiten des Körpers $\mathbb{Q}(\sqrt{D'})$ bezeichnen, also

$$(5) \qquad L_K(0,\chi) = \frac{h(D')}{\frac{1}{2}w(D')} \cdot \frac{h(D'')}{\frac{1}{2}w(D'')} \ .$$

Die Gleichheit der rechten Seiten von (4) und (5) ist der eigentliche Inhalt von Satz 3, wovon die gegebene Formulierung nur einen besonders einfachen Spezialfall darstellt. Um ihn zu gewinnen, bemerken wir erst, daß für p wie im Satz die Diskriminante von $\mathbb{Q}(\sqrt{p})$ gleich $4p$ und die Idealklassenzahl im engeren Sinne gleich 2 ist (nach Voraussetzung ist nämlich $h_0(p) = 1$, und es gilt immer $h = h_0$ oder $h = 2h_0$; hier ist die Möglichkeit $h = h_0$ dadurch ausgeschlossen, daß die Pellsche Gleichung $x^2 - py^2 = -4$ für $p \equiv 3 \pmod 4$ keine Lösung hat, oder auch dadurch, daß $h(4p)$ nach dem Korollar in §12 gerade sein muß). Seien E (= Hauptklasse) und θ die Elemente der Idealklassengruppe. Auf dieser Gruppe gibt es nur zwei Charaktere, den trivialen Charakter χ_0 und den Charakter χ_1 mit $\chi_1(E) = 1$, $\chi_1(\theta) = -1$; da es nach dem Hauptsatz von §12 auch zwei Geschlechts-

charaktere gibt, welche den Zerlegungen $4p = 1 \times 4p$ und $4p = -4 \times -p$ entsprechen, müssen diese χ_0 bzw. χ_1 sein und wir haben

$$\zeta(E,s) + \zeta(\theta,s) = L_K(s,\chi_0) = \zeta(s)\, L_{4p}(s) ,$$

$$\zeta(E,s) - \zeta(\theta,s) = L_K(s,\chi_1) = L_{-4}(s)\, L_{-p}(s) ,$$

als nach dem bereits Gesagten

$$\zeta(E,0) + \zeta(\theta,0) = 0 ,$$

$$\zeta(E,0) - \zeta(\theta,0) = \frac{h(-4)}{\frac{1}{2}\cdot 4} \cdot \frac{h(-p)}{\frac{1}{2}w(-p)} = \frac{1}{2}\, h(-p)$$

(hier brauchen wir $p \neq 3$!). Es gilt also $h(-p) = 4\zeta(E,0)$, und nach Satz 2 ist dies gleich $\frac{1}{3}\sum_{i=1}^{r}(n_i-3)$ mit n_i wie in der Formulierung von Satz 3. Damit ist der Beweis von Satz 3 zu Ende. Vergleicht man allerdings die Bemerkungen nach Satz 3 in §9, so sieht man, daß (5) zwar richtig, von uns aber nur bis aufs Vorzeichen bewiesen worden ist (weil das Vorzeichen der Gaußschen Summe nie bestimmt wurde). Dasselbe gilt also auch für die Formel in Satz 3 hier, die allerdings dadurch nichts an Nützlichkeit einbüßt, weil Klassenzahlen ja von Natur aus positiv sind; wir wollten aber nicht durch Absolutbetragszeichen um den Ausdruck $\frac{1}{3}\sum_{i=1}^{r} n_i - r$ die Schönheit des Satzes beeinträchtigen.

Aufgaben:

1. Man zeige, daß das Residuum von $Z_f(s)$ ($f = ax^2 + bxy + cy^2$, $a, b, c > 0$, $D = b^2 - 4ac > 0$) an der Stelle $s = 1$ gleich $\frac{1}{2\sqrt{D}} \log \frac{w}{w'}$ ist, wobei $w, w' = \frac{b \pm \sqrt{D}}{2a}$ die Wurzeln von $ax^2 - bx + c = 0$ sind.

2. Sei A eine Idealklasse in einem reellquadratischen Zahlkörper K und seien $w_1, \ldots, w_r$ die größeren Wurzeln der reduzierten Formen aus dem entsprechenden Zykel. Man zeige, daß $\prod_{i=1}^{r} w_i = \varepsilon$, wobei ε die Grundeinheit (mit Norm +1) von K bezeichnet. Zusammen mit Aufgabe 1 und Satz 3 von §13 liefert dies einen neuen Beweis von Satz 2, §10.

3. Sei x eine reelle Zahl mit der Kettenbruchentwicklung

$$x = [[a_1+3, \underbrace{2,\ldots,2}_{a_2\text{-mal}}, a_3+3, \underbrace{2,\ldots,2}_{a_4\text{-mal}}, \ldots]] \qquad (a_i \geq 0) .$$

Man zeige, daß die Zahl $\frac{x-1}{x-2}$ die Kettenbruchentwicklung

$$\frac{x-1}{x-2} = [[\underbrace{2,\ldots,2}_{a_1\text{-mal}}, a_2+3, \underbrace{2,\ldots,2}_{a_3\text{-mal}}, a_4+3, \ldots]]$$

hat und folgere aus dieser Aussage und Satz 2 die Gleichung

$$\zeta(A,0) = -\zeta(A\theta,0) ,$$

wobei A eine Idealklasse im engeren Sinne in einem reellquadratischen Körper K ist und $A\theta$ die aus allen Idealen

$$(\lambda)\mathfrak{a} \qquad (\mathfrak{a} \in A ,\ \lambda \in K ,\ N(\lambda) < 0)$$

bestehende Idealklasse bezeichnet. Insbesondere verschwindet $\zeta(A,0)$ für alle A, falls die Idealklasseneinteilungen im engeren Sinne zusammenfallen, d.h. falls K eine Einheit der Norm -1 besitzt.

Literatur zu Teil II

Fast die ganze Theorie, die im zweiten Teil dieses Buchs entwickelt wurde, geht (mindestens im Prinzip) auf Gauß' *Disquisitiones Arithmeticae* (*Arithmetische Untersuchungen*) zurück; ihre deutsche Übersetzung sowie der Aufsatz *Über den Zusammenhang zwischen der Anzahl der Klassen, in welche die binären Formen zweiten Grades zerfallen, und ihrer Determinante* sind in

C.F. Gauß, *Untersuchungen über höhere Arithmetik*, Göttingen 1889 (Neuauflage Chelsea 1965)

enthalten. Man soll sie unbedingt angucken. Modernere Darstellungen verschiedener Teile dieser Theorie findet man in

S.I. Borewicz, I.R. Šafarevič, *Zahlentheorie*, Birkhäuser Verlag, Basel und Stuttgart, 1966

E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923 (Neuauflage Chelsea 1970)

E. Landau, *Vorlesungen über Zahlentheorie* (3 Bände), Leipzig 1927 (Neuauflage Chelsea 1969)

A. Scholz, B. Schoeneberg, *Einführung in die Zahlentheorie*, Sammlung Göschen, Band 1131, Walter de Gruyter, Berlin 1961

sowie in den am Ende von Teil I angeführten Büchern von Davenport und Siegel (Teil II), und zwar im Einzelnen wie folgt:

	Quadratische Formen (§8)	Klassenzahlformel (§§8,9)	Zusammenhang mit quadratischen Körpern (§§10,11)	Geschlechtertheorie (§12)
Borewicz-Šafarewič	Kap. II, §7	Kap. V, §4	Kap. III, §8	Kap. III, §8.4
Davenport	§§5-6	§1, §6		
Gauß	Disq. Arith. Art. 153-308	De nexu inter multitudinem...		Disq. Arith. Art. 228-287
Hecke		§§50-52	§§29,44-45,53	§§47-48
Landau	4. Teil, Kap. 1-4	4. Teil, Kap. 5-9	11. Teil	
Scholz-Schoeneberg	Kap. IV			
Siegel		§§13-14		§§24-25

Die Reduktionstheorie und ihr Zusammenhang mit periodischen Kettenbrüchen gehen auch auf Gauß zurück (Art. 183-205 der *Disquisitiones*) und wird auch in §31-32 von Scholz-Schoeneberg behandelt. Die hier gegebene Darstellung (§13) weicht von der üblichen ab.

Die am Ende von §13 beschriebene Zerlegung der Zetafunktion einer Idealklasse in einem reellquadratischen Körper mit Hilfe der Reduktionstheorie wurde in der Arbeit

D. Zagier, *A Kronecker limit formula for real quadratic fields*, Math. Ann. 213 (1975) 153-184

eingeführt und ihre Anwendung auf die Berechnung der Werte dieser Zetafunktionen bei $s = 0$ (Sätze 1 und 2 von §14) in

D. Zagier, *Valeurs des fonctions zêta des corps quadratiques réels aux entiers négatifs*, Journées Arithmétiques de Caen, Astérisque 41-42 (1977) 135-151

angegeben, wo auch die Werte an negativen ganzzahligen Stellen bestimmt werden. Für die Übertragung dieser Methode auf Zetafunktionen beliebiger total-reeller Zahlkörper siehe

T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. U. Tokyo 23(1976) 393-417.

Die Werte von $\zeta(A,0)$ im quadratischen Fall kannte man schon vorher durch die Arbeiten von C. Meyer, der sie mit Hilfe einer auf Hecke zurückgehenden Integraldarstellung von $\zeta(A,s)$ mittels sog. Dedekindscher Summen ausgedrückt hat. Über diese Arbeiten wird im o.a. Artikel *A Kronecker limit formula* ... sowie im ersten Kapitel von

C.L. Siegel, *Lectures on Advanced Analytic Number Theory*, Tata Institute, Bombay 1961

berichtet. Der Zusammenhang zwischen den in Meyers Formel auftretenden Dedekindschen Summen und Kettenbrüchen wurde von F. Hirzebruch und dem Autor bemerkt; insbesondere wurde Satz 3, §14, von Hirzebruch als Korollar des Meyerschen Satzes entdeckt. Siehe hierzu den Bericht

D. Zagier, *Nombres de classes et fractions continues*, Journées Arithmétiques de Bordeaux, Astérisque 24-25 (1975) 81-97.

Sachverzeichnis

Symbolverzeichnis

P. Ribenboim

13 Lectures on Fermat's Last Theorem

1979. 1 portrait, 3 tables. XVI, 302 pages.
Cloth DM 48,–
ISBN 3-540-90432-8

This book, based on the author's lectures at the Institut Henri Poincaré, gives a fully understandable mathematical description of the various highly ingenious attempts to prove Fermat's last theorem. All significant approaches are covered, including such modern methods as the use of class field theory and estimates based on diophantine approximation. The book is a unique testimonial to the multi-facetness of a single mathematical problem and the incredible variety of methods used in attempting to solve it. Number theorists will find the **13 Lectures** an inspiring account of an important part of the history of their subject. The book is, however, accessible to the non-specialist as well, particularly as the freshness of the style of the original lectures has been preserved in the printed version.

Springer-Verlag
Berlin
Heidelberg
New York