Quadratische Zahlenkörper

22. April 2005

Inhaltsverzeichnis

1 Einleitung

Das Klassenzahlproblem, in der Form in der es heutzutage behandelt wird, besteht im wesentlichen daraus, für den Ring der ganzen Zahlen eines algebraischen Zahlkörpers die Anzahl der Klassen äquivalenter Ideale zu bestimmen. Von besonderem Interesse sind in diesem Zusammenhang jene Zahlkörper, für die die Klassenzahl 1 ist, da in diesem Fall der Ring der ganzen Zahlen ein faktorieller Ring ist.

Der Ursprung des Problems liegt jedoch nicht in der Betrachtung algebraischer Zahlkörper, sondern in der quadratischer Formen. Einer der Ersten, die sich mit diesem Problem beschäftigten, war C. F. Gauß, der es im fünften Kapitel seiner Disquisitiones Arithmeticae behandelte. Allerdings betrachtet Gauß quadratische Formen der Bauart

$$f(x, y) = ax^2 + 2bxy + cy^2$$

im Gegensatz zu der allgemeineren Form

$$g(x, y) = dx^2 + exy + fy^2.$$

Bezeichnet man nun zwei "Gauß'sche" Formen $f_1(x, y)$ und $f_2(x, y)$ als äquivalent, wenn es eine ganzzahlige Matrix $\mathcal{A}$ mit Determinante ± 1 gibt, sodass

$$(\mathcal{A}f_1)(x, y) := f_1(Ax + By, Cx + Dy) = f_2(x, y),$$

wobei

$$\mathcal{A} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

gilt, so stellt sich heraus, dass alle quadratischen Formen der selben Äquivalenzklasse auch die selbe Determinante $D(f) := b^2 - ac$ besitzen. Da es darüber hinaus zu einer gegebenen Determinante nur endlich viele Äquivalenzklassen gibt, ist es möglich die Klassenzahl $H(D)$ als die Anzahl der Äquivalenzklassen quadratischer Formen mit Determinante D, für die der größte gemeinsame Teiler von a, $2b$ und c eins ist und die im Falle von negativen D, positiv definit sind, zu definieren, wie es bereits Gauß getan hat.

Betrachtet man nun allgemeine quadratische Formen, wie es bereits J. L. Lagrange und L. Kronecker getan haben, so ergibt sich für die Diskriminante $d(f) := b^2 - 4ac$, das heißt für den Spezialfall einer Gauß'schen Form gilt $d(f) = 4D(f)$ und man kann weiters feststellen, dass alle quadratischen Formen mit einer durch vier teilbaren Determinante Gauß'sch sind. Die obige Definition der Klassenzahl, kann direkt auf den allgemeinen Fall übertragen werden, wobei hier nun Formen mit $(a, b, c) = 1$ betrachtet werden, die im

Falle von negativem d positiv definit sind. Die Klassenzahl wird nun mit $h(d)$ bezeichnet.

Nun stellt sich die Frage, wie groß die Klassenzahl einer gegebenen Determinante d ist. Bereits Gauß listete einige kleine negative Determinante auf, für die $H(d)$ klein ist und wie D. Shanks zeigte ist die Aussage, dass Gauß's Liste der Determinanten D für die $H(D) = 1$ oder $= 3$ gilt, komplett ist, äquivalent dazu, dass für negatives d $h(d)$ genau dann eins ist, wenn $-d$ gleich einer der Zahlen $3, 4, 7, 8, 11, 19, 43, 67$ oder 163 ist. Der tatsächliche Beweis für die Vollständigkeit dieser Liste, sollte jedoch erst Mitte des letzten Jahrhunderts erfolgen und für positive Determinanten ist das Problem bis heute ungelöst, das heißt es ist ungeklärt ob es unendlich viele reelle quadratische Zahlkörper mit Klassenzahl 1 gibt.

Den nächsten wichtigen Beitrag zur Erforschung der Klassenzahl lieferte P. G. Lejeune Dirichlet, indem er eine Formel für die Klassenzahl fand, die sogenannte Dirichletsche Klassenzahlformel

$$h(d) = \begin{cases} \frac{\varepsilon(d)|d|^{1/2}}{2\pi} L_d(1) & \text{für } d < 0 \\ \frac{d^{1/2}}{2 \log \varepsilon} L_d(1) & \text{für } d > 0 \end{cases} \tag{1.1}$$

bzw.

$$h(d) = \begin{cases} \frac{\varepsilon(d)}{2d} \sum_{n=1}^{|d|} \left(\frac{d}{n}\right) n & \text{für } d < 0 \\ \frac{-1}{log \varepsilon} \sum_{0<n<\frac{d}{2}} \left(\frac{d}{n}\right) log \left(sin \frac{\pi n}{d}\right) & \text{für } d > 0. \end{cases} \tag{1.2}$$

Die ersten Ansätze zur Bestimmung einer explizite Formel zur Berechnung der Klassenzahl, finden sich bereits bei Gauß, in dessen Nachlaß sich ein unvollendetes Manuskript befand, in dem bereits das richtige Ergebnis für Formen mit negativer Diskriminante und der Ansatz zu einem Beweis enthalten war. Obwohl es sehr wahrscheinlich ist, dass Dirichlet, als Freund und Schüler Gauß' mit dessen Ideen vertraut war, unterscheidet sich seine Vorgehensweise doch grundlegend von der Gauß'. Für sich allein genommen stellt die Klassenzahlformel schon ein bemerkenswertes Ergebis dar, das wahre Ausmaß ihrer Bedeutung wird aber erst klar, wenn man ihre Anwendug in dem Beweis eines anderen wichtigen Satzes des Dirichletschen Primzahlsatezes berücksichtigt. Dieser Satz besagt im wesentlichen, dass jede Folge der Form $kn + h$, $n = 0, 1, 2, \ldots$ mit $(k, h) = 1$ unendlich viele Primzahlen enthält. Die Schlüsselstelle im Beweis dieses Satzes ist es zu zeigen, dass $L_d(1) \neq 0$ gilt. Kennt man nun Formel (1.1) so folgt das unmittelbar, da die Klassenzahl nie Null sein kann. Ganz in der Tradition Gauß' betrachtete Dirichlet nur quadratische Formen mit geradem Mittelkoeffizienten, der Beweis

für allgemeine quadratische Formen geht auf L. Kronecker zurück. Obwohl Dirichlet Klassenzahlen nur aus der Blickwinkel der quadratischen Formen betrachtete, stellte sich später heraus, dass sich die Formel auch auf Abelsche Körper verallgemeinern lässt.

Der nächste wesentliche Schritt in der Entwicklung der Theorie der Klassenzahlen war die Einführung von Idealen und die Ausweitung des Begriffes auf Idealklassen algebraischer Zahlkörper. Diese Entwicklung ist vor allem einem Schüler Gauß' und insbesondere Dirichlets R. Dedekind zu verdanken. In Anlehung an Dirichlets Arbeiten beschäftigte sich Dedekind mit algebraischen Zahlkörpern und führte den Begriff des Ideals für den Ring der ganzen Zahlen ein. Viele wichtige Sätze gehen auf Dedekind zurück, so zum Beispiel der Satz, dass jeder algebraische Zahlkörper eine Ganzheitsbasis besitzt, oder die Tatsache, dass jedes Ideal in dem Ring der ganzen Zahlen eine eindeutige Faktorisierung in Primideale besitzt, weiters definierte er auch Norm und Spur eines algebraischen Zahlkörpers. Außerdem gelang es Dedekind ein Verbindung zwischen den Klassen quadratischer Formen und den Idealklassen eines imaginär quadratischen Zahlkörpers herzustellen. Ist nämlich $d < 0$ die Diskriminante eines imaginär quadratischen Körpers $K = \mathbb{Q}(\sqrt{d})$, so kann man für jedes Ideal $I \trianglelefteq O_K$, dargestellt in der From $I = \mathbb{Z}a_1 + \mathbb{Z}a_2$, wobei man o.B.d.A annehmen kann, dass $\Im(a_1\overline{a}_2 - \overline{a}_1 a_2) > 0$ ist, eine quadratische Form

$$f_{a_1 a_2}(x, y) = \frac{1}{N(I)} N_{K/\mathbb{Q}}(a_1 x + a_2 y) \tag{1.3}$$

definieren, für die folgende drei Eigenschaften gelten:

(i) $f_{a_1 a_2}(x, y)$ ist eine primitive, positiv definite quadratische Form mit ganzzahligen Koeffizienten und Diskriminante d.

(ii) Zwei Ideale $I = \mathbb{Z}a_1 + \mathbb{Z}a_2$ und $J = \mathbb{Z}b_1 + \mathbb{Z}b_2$ sind genau dann in derselben Idealklasse, wenn die quadratischen Formen $f_{a_1 a_2}(x, y)$ und $f_{b_1 b_2}(x, y)$ äquivalent sind.

(iii) Die Zuordung $f_{a_1 a_2} \mapsto$ (Klasse von $I = \mathbb{Z}a_1 + \mathbb{Z}a_2$) induziert eine Bijektion zwischen der Menge aller Klassen primitiver, positiv definiter quadratischer Formen mit Diskriminante d und der Idealklassengruppe $H(K)$.

Eine unmittelbare Folgerung aus diesem Satz ist, dass die Klassenzahl imaginär quadratischer Zahlkörper mit Diskriminante d mit der Klassenzahl quadratischer Formen mit der Diskriminante d übereinstimmt.

Viele der Resultate Dedekinds bezüglich des Ringes der ganzen Zahlen eines algebraischen Zahlkörpers, lassen sich auch allgemeiner anwenden. Allerdings fehlte Dedekind das Konzept des Ringes, das in seiner heute gebräuchlichen Form erstmals durch A. Fränkel 1916 eingeführt wurde. Weiterentwickelt und verallgemeinert wurden Dedekinds Ideen vorallem von D. Hilbert und E. Noether. Im besonderen Emmy Noether erweiterte die Theorie indem sie sogenannte Dedekindsche Ringe definierte, das sind Ringe, die Noethersch sind, das heißt, dass jede aufsteigende Idealkette endlich ist und darüber hinaus ganz algebraisch abgeschlossen und deren Primideale alle maximal sind. Der Ring der ganzen Zahlen eines algebraischen Zahlkörpers ist ein spezieller Dedekindscher Ring. Insbesondere gilt für alle Dedekindschen Ring, dass ihre Ideale eine eindeutige Zerlegung in Primideale besitzten und dass jedes ihrer Ideale invertierbar ist.

Bedingt durch die Ergebnisse Dedekinds bezüglich dem Zusammenhang zwischen imaginär quadratischen Zahlkörpern und quadratischen Formen, war es möglich das Klassenzahlenproblem für solche Zahlkörper zu lösen. Den ersten Schritt in diese Richtung unternahmen H. Heilbronn und E. Linfoot indem sie zeigten, dass es außer den neun bereits von Gauß gefunden Diskriminanten, maximal noch eine zehnte geben könne, für die die Klassenzahl eins ist. 1967 gelang es schließlich H. M. Stark zu beweisen, dass eine solche Diskriminante nicht existiert nachdem er bereits ein Jahr zuvor gezeigt hatte, dass für diese zehnte Diskriminante d, $|d| \geq 2.2 \cdot 10^7$ gelten müßte. Der Vollständigkeit halber sollte noch erwähnt werden, dass K. Heegner bereits 1952 einen Beweis für die Nichtexistenz einer zehnten Diskriminante erbrachte, der allerdings nicht als vollständig angesehen wurde. Erst später wurde klar dass Heegners Ansatz richtig war.

Wie bereits erwähnt ist das Klassenzahlproblem für reell quadratische Zahlkörper bis heute ungelöst. Das größte Hindernis stellt hier die Tatsache dar, dass die Einheitengruppe in diesem Fall unendlich ist und die Klassenzahlformel von der fundamentalen Einheit des Zahlkörpers abhängt. Daher ist es wichtig die fundamentale Einheit explicit zu bestimmen, was in eingigen Fällen mit Hilfe von Kettenbruchentwicklungen gelungen ist.

2 Klassenzahl Algebraischer Zahlkörper

2.1 Algebraische Zahlkörper

Zwei für die Behandlung der Klassenzahl wesentliche Begriffe sind der des algebraischen Zahlkörpers und der des Ringes der ganzen Zahlen, einer speziellen Teilmenge des algebraischen Zahlkörpers. Doch um diese beiden definieren zu können benötigt man zunächst einige Voraussetzungen.

Definition 2.1.1 *Seien K und L zwei Körper und gelte $K \subseteq L$, dann ist L ein so genannter **Erweiterungskörper** von K. Faßt man nun L als Vektorraum über K auf, heißt die Erweiterung L/K **endlich**, falls die Dimension des Vektorraumes L über K endlich ist. Diese Dimension nennt man **Erweiterungsgrad** $[L : K]$.*

Definition 2.1.2 *Sei L/K eine Körpererweiterung, $\alpha \in L$ heißt **algebraisch** über K, falls es ein Polynom $f(x) \in K[x]$ mit $f(\alpha) = 0$ gibt. Ist jedes $\alpha \in L$ algebraisch über K, so heißt die Körpererweiterung algebraisch.*

Definition 2.1.3 *Ein Körper E heißt **algebraisch abgeschlossen**, wenn jedes Polynom $f(x) \in E[x]$ eine Nullstelle $\alpha \in E$ besitzt.*

Definition 2.1.4 *Sei R Teilring eines Körpers K, ein Element $\alpha \in K$ heißt **ganz** oder auch **ganzalgebraisch** bezüglich R, wenn α Nullstelle eines normierten Polynoms mit Koeffizienten aus R ist.*

Definition 2.1.5 *Sei R Teilring eines Körpers K, dann wird die Gesamtheit O der bezüglich R ganzen Elemente von K als **ganzalgebraische Hülle** von R in K bezeichnet.*

Eine interessante Eigenschaft ganzer Elemente ist, dass bereits das Minimalpolynom, also das eindeutig bestimmte, irreduzible Polynom kleinsten Grades, dass das Element als Nullstelle hat, nur Koeffizienten aus dem Ring besitzt. Der Beweis hierfür ist nicht sonderlich kompliziert und kann zum Beispiel in [4] gefunden werden. Auch das folgende Lemma gibt eine Eigenheit

ganzer Elemente an.

Lemma 2.1.1 *Sei K ein Körper, R ein Teilring von K und $M \subseteq K$ ein endlich erzeugter R-Modul, sodass M auch ein Teilring von K ist, dann sind alle Elemente aus M ganz bezüglich R.*

Beweis: Sei $M = \{a_1 w_1 + \cdots + a_k w_k | a_1, \ldots a_k \in R\}$, da M ein Ring ist, gilt für alle $\alpha \in M$, dass $\alpha w_i \in M$ und sich somit mittels $\alpha w_i = \sum_{i=1}^{k} a_{ij} w_i$ mit $a_{ij} \in R$ darstellen lässt. Setzt man nun $A = (a_{ij})$ und $B = \alpha I_n - A = (b_{ij})$, dann erhält man:

$$\begin{aligned}\sum_{j=1}^{n} b_{ij} w_j &= \sum_{j=1}^{n} (\alpha \delta_{ij} - a_{ij}) w_j \\ &= \alpha u_i - \sum_{j=1}^{n} a_{ij} w_j \\ &= 0\end{aligned}$$

Hieraus folgt $B(w_1, \ldots, w_k)^T = (0, \ldots, 0)^T$. Da aber $(w_1, \ldots, w_k) \neq (0, \ldots, 0)$, muss $\det(B) = 0$ gelten und somit, weil die Determinante von B ein normiertes Polynom in $R[\alpha]$ ist, ist α ganzalgebraisch über R.

□

Mit Hilfe des Vorhergehenden kann man nun algebraische Zahlkörper und den Ring der ganzen Zahlen O_K definieren. Im folgenden werden vor allem die Ideale von O_K, das sind Teilringe I, für die $aI \subseteq I$ für alle a aus O_K gilt, eine wichtige Rolle spielen.

Definition 2.1.6 *Sei $K \subseteq \mathbb{C}$ ein endlicher Erweiterungskörper von $\mathbb{Q}$, dann heißt K* ***algebraischer Zahlkörper*** *und der ganzalgebraische Abschluß von $\mathbb{Z}$ in K* ***Ring der ganzen Zahlen*** *O_K.*

Ist K ein algebraischer Zahlkörper vom Grad n, so gibt es ein Element $\alpha \in K$ vom Grad n, sodass $K = \mathbb{Q}(\alpha)$ gilt. Einen Beweis dieser Tatsache findet man etwa in [4]. Zu jedem algebraischen Zahlkörper gibt es äquivalente Körper, die sogenannten Konjugierten Körper. Ihre Anzahl ist gleich dem

Grad der Körpererweiterung. Vor allem die zahlenmäßige Aufteilung in reelle und komplexe Körper, die sogenannte Signatur, wird im folgenden immer wieder eine wichtige Rolle spielen.

Definition 2.1.7 *Sei K ein algebraischer Zahlkörper mit Erweiterungsgrad n, das heißt $\exists \alpha \in K : K = \mathbb{Q}(\alpha)$ und sei*

$$m_\alpha(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_s)(x-\overline{\alpha}_{s+1})\cdots(x-\alpha_{s+t})(x-\overline{\alpha}_{s+t})$$

$$\alpha_1, \ldots, \alpha_s \in \mathbb{R}\ ,\ \alpha_{s+1}, \ldots, \alpha_{s+t}, \overline{\alpha}_{s+1}, \ldots, \overline{\alpha}_{s+t} \in \mathbb{C} \setminus \mathbb{R}\ ,\ n = s + 2t$$

das Minimalpolynom von α, dann kann man einen Isomorphismus

$$\sigma_j : \begin{array}{ccc} \mathbb{Q}(\alpha) & \to & \mathbb{Q}(\alpha_j) \\ \alpha & \to & \alpha_j \end{array}$$

definieren. Die Körper

$$\mathbb{Q}(\alpha_j) \cong \mathbb{Q}(\alpha) = K$$

*werden als die zu K **konjugierten Körper** bezeichnet. Die Wurzeln des Minimalpolynoms von α werden die **Konjugierten** von α genannt.*

Definition 2.1.8 *Sei K ein algebraischer Zahlkörper und*

$$\sigma_1(K), \ldots, \sigma_s(K), \sigma_{s+1}(K), \ldots, \sigma_{s+t}(K), \overline{\sigma}_{s+1}(K), \ldots, \overline{\sigma}_{s+t}(K)$$

*($s + 2t = n$) die konjugierten Körper von K, wobei $\sigma_1(K), \ldots, \sigma_s(K) \subseteq \mathbb{R}$ und $\sigma_{s+1}(K), \ldots, \sigma_{s+t}(K) \nsubseteq \mathbb{R}$ gilt. Dann heißt das Paar $[s,t]$ die **Signatur** von K.*

Für jedes Element eines Erweiterungskörpers kann man zwei Kenngrößen definieren, die Norm und die Spur.

Definition 2.1.9 *Sei L/K eine endliche Erweiterung. Für jedes $\alpha \in L$ ist die Abbildung*

$$a \to \alpha a$$

eine lineare Abbildung auf L.
Sei $\omega_1, \ldots, \omega_n$ eine Basis von L über K und sei

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j\ ,\ a_{ij} \in K$$

dann bezeichnet

$$f_\alpha(x) = \det(xI - (a_{ij}))$$

das ***charakteristische Polynom*** *von* α.
Die Determinante von (a_{ij}) *heißt* ***Norm***

$$N_{L/K}(\alpha) = det(a_{ij})$$

und die Spur von (a_{ij}) ***Spur*** *von* α

$$Sp_{L/K}(\alpha) = \sum_{i=1}^{n} a_{ii}$$

.

Eine nützliche Eigenschaft der Norm beziehungsweise der Spur, die hier jedoch nicht gezeigt werden soll, ist ihre Multiplikativität beziehungsweise Addidivität, das heißt für $\alpha, \beta \in L$ gilt

$$\begin{aligned} N_{L/K}(\alpha\beta) &= N_{L/K}(\alpha)N_{L/K}(\beta) \\ Sp_{L/K}(\alpha+\beta) &= Sp_{L/K}(\alpha) + Sp_{L/K}(\beta). \end{aligned}$$

Für einen Beweis dieser Tatsache siehe [6].Wie das folgende Lemma zeigt, liegen für ein Element aus dem Ring der ganzen Zahlen eines algebraischen Zahlkörpers die Norm und die Spur immer in $\mathbb{Z}$.

Lemma 2.1.2 *Sei* K *ein algebraischer Zahlkörper vom Grad* n *über* $\mathbb{Q}$ *und* $\alpha \in O_K$*, dann liegen* $Sp_{K/\mathbb{Q}}(\alpha)$ *und* $N_{K/\mathbb{Q}}(\alpha)$ *in* $\mathbb{Z}$.

Beweis: Seien $w_1, \ldots, w_n$ eine Basis von L/K und $\alpha w_i = \sum_{j=1}^{n} a_{ij} w_j$, dann gilt

$$\alpha^{(k)} w_i^{(k)} = \sum_{j=1}^{n} a_{ij} w_j^{(k)},$$

wobei $\alpha^{(k)}$ die k-te Konjugierte von α bezeichnet. Unter Verwendung des Kronecker Deltas kann man diese Gleichung auch folgendermaßen schreiben:

$$\sum_{j=1}^{n} \delta_{jk} \alpha^{(j)} w_i^{(j)} = \sum_{j=1}^{n} a_{ij} w_j^{(k)}$$

mit

$$\delta_{ij} = \begin{cases} 0 & \text{für} \quad i \neq j \\ 1 & \text{für} \quad i = j \end{cases}$$

Definiert man nun folgende Matrizen mittels

$$A_0 = (\alpha^{(i)}\delta_{ij}), \quad W = (w_i^{(j)}), \quad A = (a_{ij})$$

so ergibt sich

$$WA_0 = AW \qquad \text{oder auch} \qquad A_0 = W^{-1}AW$$

woraus sich $SpA = SpA_0$ und $\det A = \det A_0$ schließen lässt. SpA_0 ist aber die Summe der Konjugierten von α und somit bis auf das Vorzeichen der Koeffizient von x^{n-1} im Minimalpolynom von α und gleichermaßen ist $\det A_0$ das Produkt der Konjugierten von α und daher wiederum bis auf ein Vorzeichen der konstante Term im Minimalpolynom. Hieraus folgt, da die Koeffizienten des Minimalpolynoms ganze Zahlen sind, dass $Sp_{L/K}(\alpha)$ und $N_{L/K}(\alpha)$ in $\mathbb{Z}$ liegen.

□

Wie dieser Beweis zeigt, gilt für ganze Zahlen algebraischer Zahlkörper folgende Tatsache: die Norm ist das Produkt und die Spur die Summe der Konjugierten des Elementes.

Im folgenden sollen nun die Begriffe der Ganzheitsbasis und der Diskriminante eines algebraischen Zahlkörpers eingeführt werden. Vor allem die Diskriminante ist eine wichtige Kenngröße und wird auch im weiteren immer wieder eine zentrale Rolle einnehmen.

Satz 2.1.1 *Sei M ein von $\alpha_1, \ldots, \alpha_n$ endlich erzeugtes $\mathbb{Z}$-Modul und N ein Teilmodul, dann gilt*

(i) $\exists \beta_1, \ldots, \beta_m$ *in* N *mit* $m \leq n$, *sodass*

$$N = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \cdots + \mathbb{Z}\beta_m$$

und $\beta_i = \sum_{j \geq i} p_{ij}\alpha_j$ *mit* $1 \leq i \leq m$ *und* $p_{ij} \in \mathbb{Z}$,

(ii) ist $m = n$, *so folgt* $[M : N] = p_{11}p_{22}\cdots p_{nn}$.

Beweis:

(i) Der Beweis soll mittels Induktion nach der Anzahl der erzeugenden Elemente von M geführt werden. Ist $n = 0$ so ist die Aussage trivial. Angenommen der Satz wurde für $n-1$ oder weniger erzeugende Elemente gezeigt, so definiert man M' als das Teilmodul, das von $\alpha_2, \ldots, \alpha_n$ erzeugt wird und betrachtet $N' = N \cap M'$. Ist $n = 1$, dann ist $M' = 0$ und es ist nichts weiter zu beweisen, gilt $N' = N$ so ist die Aussage wahr nach der Induktionsannahme.

Nun bleibt noch der Fall $N' \neq N$ zu betrachten. Sei A die Menge aller ganzen Zahlen k für die es $k_2, \ldots, k_n \in \mathbb{Z}$ gibt, sodass $k\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \in N$ gilt. Da N ein Teilmodul ist, ist A eine Untergruppe der ganzen Zahlen. Jede additive Untergruppe der ganzen Zahlen ist von der Form $m\mathbb{Z}$ für eine ganze Zahl m, daher kann man A mittels $k_{11}\mathbb{Z}$ darstellen. Sei $\alpha \in N$, dann gilt

$$\alpha = \sum_{i=1}^{n} h_i\alpha_i$$

mit $h_i \in \mathbb{Z}$, somit $h_1 \in A$ und daher $h_1 = ak_{11}$. Setzt man nun $\beta_1 = k_{11}\alpha_1 + k_{12}\alpha_2 + \cdots + k_{1n}\alpha_n$, so folgt $\alpha - a\beta_1 \in N'$. Nach Induktionsvoraussetzung existieren

$$\beta_i = \sum_{j \geq i} k_{ij}\alpha_j \quad i = 2, 3, \ldots, m$$

die N' erzeugen, fügt man dieser Menge β_1 hinzu, so erhält man ein Erzeugendensystem von N, das das geforderte Kriterium erfüllt.

(ii) Sei α ein beliebiges Element aus M mit der Darstellung $\alpha = \sum_{i=1}^{n} c_i\alpha_i$ und sei p_{11} gegeben durch

$$\beta_i = \sum_{j \geq i} p_{ij}\alpha_j,$$

dann lässt sich c_1 als $c_1 = p_{11}q_1 + r_1$ mit ganzen Zahlen q_1 und r_1 schreiben und es gilt $0 \leq r_1 < p_{11}$. Bildet man nun $\alpha - q_1\beta_1 = \sum c_i'\alpha_i$, so gilt $0 \leq c_1' < p_{11}$ und $\alpha \equiv \alpha - q_1\beta_1 \mod N$. Wiederholt man nun diesen Vorgang mit c_2' so erhält man $c_2' = p_{22}q_2 + r_2$ mit $0 \leq r_2 < p_{22}$ und außerdem

$$\alpha \equiv \alpha - q_1\beta_1 - q_2\beta_2 \mod N.$$

Wie sich leicht mittels Induktion zeigen lässt ergibt sich durch Fortführen dieser Vorgehensweise ein $\alpha' = \sum k_i\alpha_i$ mit $0 \leq k_i < p_{ii}$ und $\alpha \equiv \alpha' \mod N$.

Nun muss noch gezeigt werden, dass wenn $\alpha = \sum c_i\alpha_i$ und $\beta = \sum d_i\alpha_i$ mit $c_i \neq d_i$ für mindestens ein i und $0 \leq c_i, d_i < p_{ii}$, α und β nicht äquivalent mod$N$ sind. Angenommen

$$\sum c_i\alpha_i \equiv \sum d_i\alpha_i \mod N$$

und sei r der kleinste Index, sodass $c_r \neq d_r$, dann folgt $\sum_{i\geq r}(c_i - d_i)\alpha_i \in N$ und somit

$$\sum_{i\geq r}(c_i - d_i)\alpha_i = \sum_{i\geq r} l_i\beta_i = \sum_{i\geq r} l_i \left(\sum_{j\geq i} p_{ij}\alpha_j\right).$$

Da c_r und d_r beide kleiner als p_{rr} sind, muss $c_r = d_r$ gelten, im Widerspruch zur Annahme. Daher hat jede Nebenklasse von M/N einen eindeutig bestimmten Repräsentanten

$$\alpha = \sum c_i\alpha_i \quad \text{mit} \quad 0 \leq c_i < p_{ii}$$

und da es $p_{11}p_{22}\cdots p_{nn}$ von ihnen gibt, gilt $[M : N] = p_{11}p_{22}\cdots p_{nn}$.

□

Lemma 2.1.3 *Sei O_K der Ring der ganzen Zahlen des Körpers K, dann existieren $w_1^*, w_2^*, \ldots, w_n^* \in K$, sodass*

$$O_K \subseteq \mathbb{Z}w_1^* + \mathbb{Z}w_2^* + \cdots + \mathbb{Z}w_n^*$$

gilt.

Beweis: Sei $w_1, w_2, \ldots, w_n$ eine Basis von $K/\mathbb{Q}$. Für jedes $\alpha \in K$ gibt es eine ganze Zahl m, sodass $m\alpha \in O_K$. Der Beweis dieser Tatsache ist nicht besonders schwierig, man kann ihn zum Beispiel in [4] nachlesen. Daher kann man annehmen, dass $w_1, \ldots, w_n \in O_K$. Definiert man nun eine Bilineare Abbildung

$$B(x,y) : \begin{array}{ccc} K \times K & \to & \mathbb{Q} \\ (x,y) & \to & Sp_{K/\mathbb{Q}}(xy) \end{array}$$

so ist B regulär und man kann somit eine duale Basis $w_1^*, \ldots, w_n^*$ finden, für die $B(w_i, w_i^*) = \delta_{ij}$ gilt (siehe zum Beispiel [4]). Schreibt man nun $w_j^* =$

$\sum c_{kj} w_k$ ergibt sich

$$\begin{aligned}\delta_{ij} &= Sp_{K/\mathbb{Q}}(w_i w_j^*) \\ &= Sp_{K/\mathbb{Q}}(w_i \sum c_{kj} w_k) \\ &= \sum c_{kj} Sp_{K/\mathbb{Q}}(w_i w_k)\end{aligned}$$

Führt man nun die Matrizen $C = (c_{ij})$ und $W = (w_i^{(j)})$ ein, so erhält man aus obiger Gleichung

$$I_n = WW^T C \quad \text{bzw.} \quad C^{-1} = WW^T$$

wobei I_n die Einheitsmatrix bezeichnet. Hieraus folgt, dass C regulär ist und somit, dass $w_1^*, \ldots, w_n^*$ eine Basis bilden.

Sei nun α ein beliebiges Element aus O_K, dann lässt sich α mittels

$$\alpha = \sum_{j=1}^{n} a_j w_j^* \quad \text{mit} \quad a_j \in \mathbb{Q}$$

darstellen. Bildet man nun αw_i so erhält man

$$\alpha w_i = \sum_{j=1}^{n} a_j w_i w_j^* \quad \forall i$$

und somit

$$Sp_{K/\mathbb{Q}}(\alpha w_i) = \sum_{j=1}^{n} a_j Sp_{K/\mathbb{Q}}(w_i w_j^*) = a_i \quad \forall i$$

Da aber $\alpha w_i \in O_K$, folgt daraus, dass $a_i \in \mathbb{Z}$ für alle i und daher gilt $O_K \subseteq \mathbb{Z}w_1^* + \cdots + \mathbb{Z}w_n^*$.

□

Nach diesen Vorbereitungen ist es nicht mehr schwierig zu zeigen, dass der Ring der ganzen Zahlen eine Ganzheitsbasis besitzt.

Satz 2.1.2 *K besitzt eine **Ganzheitsbasis**, das heißt es existieren $w_1, w_2, \ldots, w_n \in O_K$, sodass $O_K = w_1\mathbb{Z} + \cdots + w_n\mathbb{Z}$.*

Beweis: Aus dem vorhergehenden Lemma folgt, dass es immer $w_1^*, w_2^*, \ldots, w_n^* \in K$ gibt, sodass $O_K \subseteq \mathbb{Z}w_1^* + \mathbb{Z}w_2^* + \cdots + \mathbb{Z}w_n^*$. Setzt man nun in Satz 2.1.1 $M = \mathbb{Z}w_1^* + \cdots + \mathbb{Z}w_n^*$ und $N = O_K$, dann existieren $w_1, \ldots, w_n \in O_K$, sodass $O_K = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$ gilt.

□

Lemma 2.1.4 *Jedes Ideal I von O_K besitzt eine Ganzheitsbasis.*

Den Beweis dieses Lemmas findet man zum Beispiel in [4]. Ausgehend vom Begiff der Ganzheitsbasis ist es nun möglich die Diskriminante eines algebraischen Zahlkörpers zu definieren.

Definition 2.1.10 *Sei K ein algebraischer Zahlkörper vom Grad n mit Ganzheitsbasis $w_1, \ldots, w_n$, dann definiert man die* ***Diskriminante*** *d_K von K folgendermaßen*

$$d_K := \det\left(w_i^{(j)}\right)^2,$$

wobei $w_i^{(j)}$ die Konjugierten von w_i darstellen.

Satz 2.1.3 *Die Diskriminante eines algebraischen Zahlkörpers ist wohldefiniert, das heißt, dass je zwei Ganzheitsbasen eines algebraischen Zahlkörpers die gleiche Diskriminante liefern.*

Beweis: Seien $w_1, \ldots, w_n$ und $\theta_1, \ldots, \theta_n$ zwei verschiedene Ganzheitsbasen des algebraischen Zahlkörpers K, dann gilt

$$w_i = \sum_{j=1}^{n} c_{ij}\theta_j$$

und

$$\theta_i = \sum_{j=1}^{n} d_{ij}w_j$$

für alle i mit ganzzahligen c_{ij} und d_{ij}. Daher sind $(c_{ij}), (c_{ij})^{-1} \in \mathbb{Z}^{n\times n}$ und somit $\det(c_{ij}), \det(c_{ij})^{-1} \in \mathbb{Z}$, das heißt $\det(c_{ij}) = \pm 1$. Außerdem gilt für alle i und j

$$\begin{aligned} Sp(w_iw_j) &= Sp\left(\left(\sum_l c_{il}\theta_l\right)\left(\sum_m c_{jm}\theta_m\right)\right) \\ &= \sum_{l,m} c_{il}c_{jm}Sp(\theta_l\theta_m). \end{aligned}$$

Setzt man nun $W = (w_i^{(j)})$, $C = (c_{ij})$ und $\Theta = (\theta_i^{(j)})$, kann man obige Gleichungen zu

$$W^T W = C(\Theta^T \Theta) C^T$$

zusammenfassen. Hieraus folgt

$$d_K = (\det W)^2 = (\det \Theta)^2 (\det C)^2 = (\det \Theta)^2,$$

und somit, dass die Diskriminante von der Wahl der Basis unabhängig ist.

□

Die Definition der Diskriminante ist aber nicht nur auf Basen eingeschränkt, sondern kann auch für eine beliebige Menge von Elementen aus K erfolgen.

Definition 2.1.11 *Man kann den Begriff der Diskriminante erweitern, indem man sie für beliebige Elemente $a_1, \ldots, a_n \in K$ folgendermaßen definiert*

$$d_{K/\mathbb{Q}} = \left[\det\left(\sigma_i(a_j)\right)\right]^2,$$

wobei n der Erweiterungsgrad von K ist.

Die folgenden zwei Lemmata beschreiben noch einige Eigenschaften der Diskriminante.

Lemma 2.1.5 *Seien $u_1, \ldots, u_n$ und $v_1, \ldots, v_n$ aus K mit $u_i = \sum_{j=1}^n a_{ij} v_j$, $a_{ij} \in \mathbb{Q}$, dann gilt*

$$d_{K/\mathbb{Q}}(u_1, \ldots, u_n) = \left(\det\left(a_{ij}\right)\right)^2 d_{K/\mathbb{Q}}(v_1, \ldots, v_n).$$

Beweis: Nach Definition gilt $d_{K/\mathbb{Q}}(u_1, \ldots, u_n) = [\det(\sigma_i(u_j))]^2$ und außerdem

$$\sigma_i(u_j) = \sigma_i\left(\sum_{k=1}^n a_{jk} v_k\right) = \sum_{k=1}^n a_{jk} \sigma_i(v_k).$$

Definiert man die drei Matrizen U, A und V folgendermaßen

$$U = (\sigma_i(u_j)) \quad A = (a_{ij}) \quad V = \sigma_i(v_j))$$

erhält man $U = VA^T$ und somit $(\det U)^2 = (\det VA^T)^2$. Hieraus folgt unmittelbar

$$d_{K/\mathbb{Q}}(u_1, \ldots, u_n) = (\det(a_{ij}))^2 d_{K/\mathbb{Q}}(v_1, \ldots, v_n).$$

□

Lemma 2.1.6 *Seien $a_1, \ldots, a_n \in O_K$ linear unabhängig über $\mathbb{Q}$ und m der Index des von $a_1, \ldots, a_n$ erzeugten $\mathbb{Z}$-Moduls, dann gilt*

$$d_{K/\mathbb{Q}}(a_1, \ldots, a_n) = m^2 d_K. \tag{2.1}$$

Beweis: Sei $\alpha_1, \ldots, \alpha_n$ eine Ganzheitsbasis von O_K und N das von $a_1, \ldots, a_n$ erzeugte $\mathbb{Z}$-Modul, dann besitzt N nach Satz 2.1.1 eine Basis $b_1, \ldots, b_n$, sodass $b_i = \sum_{j \geq i} p_{ij} \alpha_j$. Nach Lemma 2.1.5 gilt dann

$$\begin{aligned} d_{K/\mathbb{Q}}(b_1, \ldots, b_n) &= (\det(p_{ij}))^2 \, d_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \\ &= m^2 d_k \end{aligned}$$

Da sowohl $a_1, \ldots, a_n$ als auch $b_1, \ldots, b_n$ N erzeugen, gilt

$$a_i = \sum_{j=1}^{n} c_{ij} b_j$$

und

$$b_i = \sum_{j=1}^{n} d_{ij} a_j$$

für alle i mit ganzzahligen c_{ij} und d_{ij}. Daher sind $(c_{ij}), (c_{ij})^{-1} \in \mathbb{Z}^{n \times n}$ und somit $\det(c_{ij}), \det(c_{ij})^{-1} \in \mathbb{Z}$, das heißt $\det(c_{ij}) = \pm 1$. Außerdem gilt für alle i und j

$$\begin{aligned} Sp(a_i a_j) &= Sp\left(\left(\sum_l c_{il} b_l\right)\left(\sum_m c_{jm} b_m\right)\right) \\ &= \sum_{l,m} c_{il} c_{jm} Sp(b_l b_m). \end{aligned}$$

Setzt man nun $A = (a_i^{(j)})$, $C = (c_{ij})$ und $B = (b_i^{(j)})$, kann man obige Gleichungen zu

$$A^T A = C(B^T B) C^T$$

zusammenfassen. Hieraus folgt

$$d_{K/\mathbb{Q}}(a_1, \ldots, a_n) = (\det A)^2 = (\det B)^2 (\det C)^2 = (\det B)^2,$$

und somit

$$d_{K/\mathbb{Q}}(b_1, \ldots, b_n) = d_{K/\mathbb{Q}}(a_1, \ldots, a_n),$$

womit die Aussage bewiesen wäre.

□

2.2 Noethersche und Dedekindsche Ringe

Das Ziel dieses Kapitels ist es zu zeigen, dass die Menge der Bruchideale eines Dedekindschen Ringes eine multiplikative Gruppe bilden und dass darüberhinaus jedes Ideal eine eindeutige Zerlegung in Primideale besitzt. Außerdem wird sich herausstellen, dass der Ring der ganzen Zahlen eines algebraischen Zahlkörpers ein Dedekindscher Ring ist, der die endliche Normbedingung erfüllt.

Um zu einer Gruppenstruktur beziehungsweise zu einer eindeutigen Primfaktorenzerlegung zu kommen benötigt man die Begriffe des Produkts, der Summe und der Teilerfremdheit zweier Ideale.

Definition 2.2.1 *Seien I und J Ideale eines kommutativen Ringes mit Einselement R, dann definiert man die* ***Summe*** *zweier Ideale als die Menge*

$$I + J = \{a + b \mid a \in I \ , \ b \in J\}$$

und das ***Produkt*** *als*

$$IJ = \{a_1 b_1 + \cdots + a_k b_k \mid a_i \in I \ , \ b_i \in J \ , \ k \geq 1\}.$$

$I + J$ und IJ sind dann wieder Ideale von R.

Für das Produkt beziehungsweise die Summe zweier Ideale, gilt folgende Beziehung:

$$I_1 I_2 \subseteq I_1 \cap I_2 \subseteq I_1, I_2 \subseteq I_1 + I_2$$

Definition 2.2.2 *Zwei Ideale I und J eines kommutativen Ringes mit Einselement R heißen* ***teilerfremd****, wenn $I + J = R$ gilt.*

Da in einem Dedekindschen Ring jedes Primideal ein maximales Ideal ist, sind je zwei Primideale in einem Dedekindschen Ring teilerfremd. Das folgende Lemma beschreibt eine interessante Eigenschaft teilerfremder Ideale, nämlich, dass ihr Produkt gleich ihrem Durchschnitt ist.

Lemma 2.2.1 *Sind $I_1, \ldots, I_n$ paarweise teilerfremde Ideale eines kommutativen Ringes mit 1, so gilt*

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$$

Beweis: Der Beweis wird mit Hilfe von vollständiger Induktion geführt, zuerst wird das Lemma für $n = 2$ gezeigt: Die erste Inklusion $I_1 I_2 \subseteq I_1 \cap I_2$ folgt direkt aus der Definition des Produktes zweier Ideale. Es bleibt also noch die zweite zu zeigen, dazu betrachtet man ein $x \in I_1 \cap I_2$. Da I_1 und I_2 teilerfremd sind, muss es Elemente $a \in I_1$ und $b \in I_2$ geben, sodass $a + b = 1$ gilt. Daher kann man x darstellen als $x = xa + xb$ und Da xa und xb beide Elemente aus $I_1 I_2$ muss auch ihre Summe in diesem Ideal liegen.

Sei nun $k > 2$ und das Lemma bereits für $n = k - 1$ gezeigt, dann kann man $I_1 \cap \cdots \cap I_n = (I_1 \cap \cdots \cap I_{k-1}) \cap I_k$ als $(I_1 \cap \cdots \cap I_{k-1}) \cap I_k = (I_1 \cdots I_{k-1}) \cap I_k$ schreiben. Sind I_k und $I_1 \cdots I_{k-1}$ teilerfremd, so folgt $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$. Es bleibt also nun noch die Teilerfremdheit von I_k und $I_1 \cdots I_{k-1}$ zu zeigen.

Angenommen man betrachtet drei Ideale I, J_1, J_2 und es gilt, dass I sowohl zu J_1 als auch zu J_2 teilerfremd ist, dann muss es Elemente $a_1, a_2 \in I$, $b_1 \in J_1$ und $b_2 \in J_2$ geben, sodass $a_1 + b_1 = 1$ und $a_2 + b_2 = 1$, daher gilt $1 = (a_1 + b_1)(a_2 + b_2) = a_1 a_2 + a_1 b_2 + a_2 b_1 + b_1 b_2$ mit $a_1 a_2 + a_1 b_2 + a_2 b_1 \in I$ und $b_1 b_2 \in J_1 J_2$, das heißt es sind auch I und $J_1 J_2$ teilerfremd. Diese Tatsache lässt sich leicht mittels Induktion auf beliebig viele Elemente ausweiten.

□

Der folgende Satz ist das Analogon zum Chinesischen Restsatz für Ideale, hierbei heißen zwei Elemente a, b kongruent modulo eines Ideals I, wenn $a - b \in I$ gilt.

Satz 2.2.1 (Chinesischer Restsatz) *Seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale eines kommutativen Ringes R mit 1 und $a_1, \ldots, a_n \in R$ gegeben, dann gibt es ein $x \in R$ sodass*

$$\begin{aligned} x &\equiv a_1 \quad (I_1) \\ &\vdots \\ x &\equiv a_n \quad (I_n) \end{aligned}$$

und x ist eindeutig bestimmt modulo $I_1 \cdots I_n$.

Beweis: Zuerst wird die Existenz mit Hilfe eines Induktionsbeweises gezeigt: Sei $n = 2, a_1, a_2 \in R$ und I_1, I_2 zwei teilerfremde Ideale von R, dann existieren $a \in I_1$ und $b \in I_2$, sodass $a + b = 1$ gilt. Das ist gleichbedeutend mit $a \equiv 1$ (I_2) und $b \equiv 1$ (I_1). Sei $x := a_1 b + a_2 a$ dann folgt

$$\begin{array}{ll} x \equiv a_1 & (I_1) \\ x \equiv a_2 & (I_2) \end{array}$$

Ist $n > 2$, dann gibt es ein $v \in R$, sodass

$$v \equiv a_j \quad (I_j) \quad , \quad 1 \leq j \leq n-1$$

. und ein $x \in R$, sodass

$$\begin{array}{lll} x & \equiv & v \quad (I_1 \cdots I_{n-1}) \\ x & \equiv & a_n \quad (I_n) \end{array}$$

gilt. Daraus folgt

$$x \equiv a_j \quad (I_j) \quad , \quad 1 \leq j \leq n \quad .$$

Nun bleibt noch die Eindeutigkeit zu zeigen: Angenommen es existieren $x, y \in R$ mit

$$\begin{array}{lll} x \equiv a_j & (I_j) & 1 \leq j \leq n \\ y \equiv a_j & (I_j) & 1 \leq j \leq n \end{array}$$

gilt, dann liegt $x - y$ in $I_1 \cap \ldots \cap I_n$, da aber $I_1, \ldots, I_n$ teilerfremd sind, gilt wegen Lemma 2.2.1 $I_1 \cap \ldots \cap I_n = I_1 \cdots I_n$ und somit $x = y(I_1 \cdots I_n)$.

□

Um nun Dedekindsche Ringe zu definieren, benötigt man zunächst den Begriff des Noetherschen Ringes, der nach der wohl bekanntesten Mathematikerin des 20. Jahrhunderts Emmy Noether benannt ist.

Definition 2.2.3 *Ein kommutativer Ring mit* 1 *heißt* ***Noethersch****, wenn jede aufsteigende Kette von Idealen* $I_1 \subseteq I_2 \subseteq \ldots$ *endlich ist, das heißt es gibt ein* N*, sodass für* $m \geq N$ *immer* $I_{m+1} = I_m$ *gilt.*

Ein zu dieser Definition äquivalentes Kriterium für Noethersche Ringe liefert das folgende Lemma.

Lemma 2.2.2 *Ein kommutativer Ring* R *mit* 1 *ist genau dann Noethersch, wenn jedes Ideal von* R *endlich erzeugt ist.*

Beweis: Nimmt man zunächst an, dass es ein Ideal I in R gibt, das nicht endlich erzeugt ist, so folgt die Existenz von Elementen $x_1, x_2, \ldots \in I$ mit $x_{m+1} \notin x_1R + \cdots + x_mR$. Definiert man nun ein Ideal I_m als $I_m = x_1R + \cdots x_mR$ und betrachtet die so entstehende Idealkette, so ist diese nicht endlich, da $I_1 \subsetneq I_2 \subsetneq \cdots$ gilt, im Widerspruch zu Noethersch.

Geht man umgekehrt davon aus, dass jedes Ideal endlich erzeugt wird und betrachtet die Idealkette $I_1 \subseteq I_2 \cdots$, so kann man ein Ideal I mittels $I = \bigcup_{m\geq 1} I_m$ definieren. Dieses Ideal ist natürlich endlich erzeugt, also $I = x_1R + \cdots + x_kR\ ,\ x_1, \ldots, x_k \in I$. Daraus folgt die Existenz eines Index N, sodass $x_1, \ldots, x_k \in I_N$. Das heißt aber, dass I eine Teilmenge von I_N sein muss, also gilt $I \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I$ und damit $I_N = I_{N+1} = I_{N+2} = \cdots$.

□

Definition 2.2.4 *Ein Noetherscher Ring heißt* ***Dedekindscher Ring****, wenn er ganzalgebraisch abgeschlossen und jedes seiner Primideale maximal ist.*

Ziel ist es zu zeigen, dass in einem Dedekindschen Ring jedes Ideal einerseits invertierbar ist, andererseits eine eindeutige Primfaktorenzerlegung besitzt, dazu benötigt man zunächst folgende zwei Lemmata.

Lemma 2.2.3 *Sei R ein Noetherscher Ring und I ein Ideal von R, dann gibt es Primideale $P_1, \ldots, P_s$, sodass*

$$P_1 \cdots P_s \subseteq I \subseteq P_1 \cap \ldots \cap P_s \tag{2.2}$$

gilt.

Beweis: Sei J die Menge aller Ideale von R, für die die Bedingung (2.2) nicht erfüllbar ist und I ein maximales Element von J. Die Existenz eines solchen Elementes folgt aus der Definition von Noethersch und dem Lemma von Zorn. I kann natürlich nicht prim sein, da sonst (2.2) mit $s = 1$ und $P_1 = I$ erfüllt wäre. Also gibt es Elemente $a, b \in R$, sodass $a \notin I$, $b \notin I$ aber $ab \in I$ gilt. Nun definiert man Ideale A und B folgendermaßen:

$$A := I + aR = I + (a)$$
$$B := I + bR = I + (b)$$

Dann ist $I \subsetneqq A$ und $I \subsetneqq B$. Daraus folgt, wegen der Maximalität von I, die Existenz von Primidealen $Q_1, \ldots, Q_r$ und $\overline{Q}_1, \ldots, \overline{Q}_t$, sodass A und B (2.2) erfüllen. Da aber

$$AB \subseteq I \subseteq A \cap B$$

gilt, müßte I (2.2) erfüllen, im Widerspruch zur Annahme. Daher ist $J = \emptyset$.

Bemerkung: Das Lemma von Zorn besagt, dass eine geordnete Menge, in der jede vollständig geordnete Teilmenge eine obere Grenze hat, mindestens ein maximales Element besitzt.

□

Lemma 2.2.4 *Seien $P_1, \ldots, P_k, P$ mit $P \neq R$ Primideale eines Dedekindschen Ringes R und gelte $P_1 \cdots P_k \subseteq P$, dann gibt es einen Index i, $1 \leq i \leq k$, sodass $P_i = P$.*

Beweis: Zunächst wird das Lemma für $k = 2$ bewiesen und anschließend mit Hilfe von vollständiger Induktion verallgemeinert.

Sei $k = 2$, dann gilt $P_1 P_2 \subseteq P$. Nimmt man nun an es gibt ein $a_1 \in P_1 \setminus P$ und ein $a_2 \in P_2 \setminus P$, dann liegt das Produkt $a_1 a_2$ in $P_1 P_2 \subseteq P$. Da aber P ein Primideal ist muss entweder a_1 oder a_2 in P liegen, im Widerspruch zu der Annahme, dass keines der beiden dies tut. Daraus folgt $P_1 \subseteq P$ oder $P_2 \subseteq P$ und somit, da in einem Dedekindschen Ring jedes Primideal $P \neq 0$ ein maximales Ideal ist, $P_1 = P$ oder $P_2 = P$.

Man nimmt nun an, dass man das Lemma bereits für k bewiesen hat und folgert daraus die Korrektheit für $k + 1$. Sei $P_1 \cdots P_{k+1} \subseteq P$, angenommen es existieren $a_1 \in P_1 \cdots P_k \setminus P$ und $a_2 \in P_{k+1} \setminus P$, dann liegt $a_1 a_2$ in $P_1 \cdots P_{k+1} \subseteq P$, daraus folgt, wie im ersten Schritt, dass entweder $a_1 \in P$ oder $a_2 \in P$ gelten muss, wodurch wiederum ein Widerspruch entsteht. Ist nun $P_1 \cdots P_k$ eine Teilmenge von P, so kann man nach Induktionsvoraussetzung $P = P_i$ für ein i, $1 \leq i \leq k$ schließen, gilt allerdings $P_{k+1} \subseteq P$, so ist $P_{k+1} = P$

□

Definition 2.2.5 *Sei R ein Integritätsbereich und K sein Quotientenkörper. Ein R-Modul $I \neq 0$, $I \subseteq K$ heißt **Bruchideal** von K, wenn es ein $a \in R$, $a \neq 0$ gibt, sodass $aI \subseteq R$ gilt.*

Definition 2.2.6 *Ein* ***Hauptbruchideal*** *ist ein Bruchideal der Form*

$$I = aR \ , \ a \in K$$

Wie der folgende Satz zeigt, gibt es zu jedem Primideal ein Bruchideal, welches das zugehörige inverse Element darstellt. Gemeinsam mit Satz 2.2.3 ergibt sich hieraus, dass für jedes Ideal eines Dedekindschen Ringes ein inverses Bruchideal existiert. Da die Menge der Ideale eine Teilmenge der Bruchideale darstellt, erhält man somit, dass die Bruchideale eines Körpers eine Gruppe bilden, für einen genauen Beweis dieser Tatsache siehe zum Beispiel [6].

Satz 2.2.2 *Sei R ein Dedekindscher Ring, K sein Quotientenkörper und $P \neq 0$ ein Primideal von R, definiert man*

$$P' = \{x \in K | xP \subseteq R\}$$

so ist P' ein Bruchideal und es gilt $PP' = R$ sprich $P' = P^{-1}$.

Beweis: Zuerst soll gezeigt werden, dass P' ein Bruchideal ist. Klarerweise ist P' ein R-Modul, da P ein Ring ist kann man Lemma 2.1.1 anwenden, woraus folgt, dass jedes Element aus P ganz bezüglich R ist. Daher gibt es ein $\alpha \neq 0 \in P$ das Nullstelle eines normierten Polynoms $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ mit Koeffizienten aus R ist. Somit folgt, dass sich $a_0 \neq 0$ auf folgende Weise darstellen lässt $a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha)$ und daher im Durchschnitt von R und P liegt. Nach der Definition von P' gilt nun $a_0 P' \subseteq PP' \subseteq R$, daher ist P' ein Bruchideal.

Da $P \neq 0$ gilt, gibt es ein Element $a \neq 0 \in P$. Betrachtet man das von a erzeugte Hauptideal aR, so gibt es nach Lemma 2.2.3 Primideale $P_1, \ldots, P_k$, sodass $P_1 \cdots P_k \subseteq aR \subseteq P$ gilt. Man wählt nun a so, dass k minimal ist.

Da $P_1 \cdots P_k \subseteq P$ gilt, kann man nach Lemma 2.2.4 ohne Beschränkung der Allgemeinheit annehmen, dass $P_1 = P$ ist. Da k zuvor minimal gewählt wurde, kann $P_2 \cdots P_k$ keine Teilmenge mehr von aR sein, somit existiert ein $b \in P_2 \cdots P_k \setminus aR$, für das dann $bP \subseteq PP_2 \cdots P_k \subseteq aR$ gilt. Daraus folgt $ba^{-1}P \subseteq R$ und damit $ba^{-1} \in P'$. Da $b \notin aR$, ist ba^{-1} kein Element aus R und deshalb gilt $R \subsetneq P'$. PP' ist wieder ein Ideal und weil $P = RP \subseteq PP' \subseteq R$ gilt, muss, da in einem Dedekindschen Ring jedes Primideal maximal ist, $PP' = P$ oder $PP' = R$ gelten.

Betrachtet man nun ersteren Fall, sprich $PP' = P$, so muss auch $P(P')^n = P,\ n = 0, 1, 2, \ldots$ gelten. Konkret heißt das, dass für $x \in P \setminus \{0\}$ und $y \in P' \setminus R$ xy^n in $P \subseteq R$ liegen muss und somit $xR[y]$ ein Ideal von R ist, das darüber hinaus gehend, da R noethersch ist, wegen Lemma 2.2.2 endlich erzeugt wird. Deswegen wird auch $R[y]$ als R-Modul endlich erzeugt, außerdem ist $R[y]$ ein Ring. Daraus folgt mit Lemma 2.1.1 , dass alle $z \in R[y]$ ganzalgebraisch sind. Im speziellen ist $y \in R[y]$, daher muss y ganzalgebraisch sein und deswegen, da R ganzalgebraisch abgeschlossen ist, in R liegen. Das ist jedoch ein Widerspruch zu der Annahme, dass $y \in P' \setminus R$, daher kann nur der zweite Fall eintreten, nämlich, dass $PP' = R$.

□

Satz 2.2.3 *In einem Dedekindschen Ring R kann jedes Ideal I, $0 \neq I \neq R$, als Produkt von Primidealen dargestellt werden, das heißt*

$$I = \prod_{P \in \mathbb{P}_I} P^{e(P)},$$

wobei $\mathbb{P}_I = \{P | P \text{ prim},\ P | I\}$ die Menge aller Primideale die I teilen bezeichnet. Diese Darstellung ist bis auf die Reihenfolge eindeutig.

Beweis: Angenommen es existiert ein Ideal I von R, das nicht als Produkt von Primidealen dargestellt werden kann, dann gibt es aber wegen Lemma (2.2.3) Primideale $P_1, \ldots, P_k$, sodass $P_1 \cdots P_k \subseteq I$ gilt. Man wählt nun I so, dass k kleinstmöglich ist, allerdings muss $k \geq 2$ sein, da in einem Dedekindschen Ring jedes Primideal maximal ist. Ferner gibt es ein weiteres Primideal P mit $I \subseteq P$. Somit gilt $P_1 \cdots P_k \subseteq P$ und man kann wegen Lemma 2.2.4 ohne Beschränkung der Allgemeinheit annehmen, dass $P = P_1$ ist. Es gilt also $P_1 \cdots P_k \subseteq I \subseteq P_1$ und da wegen Satz 2.2.2 jedes Primideal invertierbar ist folgt daraus $P_2 \cdots P_k \subseteq IP_1^{-1} \subseteq R$. Da aber zu Beginn I so gewählt wurde, dass k kleinst möglich ist, muss $J = IP_1^{-1} \leq R$ als Produkt von Primidealen darstellbar sein, also $J = Q_1 \cdots Q_s$. Dann ließe sich aber auch I als Produkt von Primidealen darstellen, nämlich $I = P_1 Q_1 \cdots Q_s$, im Widerspruch zur Annahme.

Nun muss nur noch die Eindeutigkeit gezeigt werden. Nimmt man an es gibt für I zwei verschiedene Darstellungen durch Primideale $P_1, \ldots, P_k$ und $Q_1, \ldots, Q_s$, $I = P_1 \cdots P_k = Q_1 \cdots Q_s$, so muss $P_1 \cdots P_k \subseteq Q_1$ gelten. Daraus folgt , dass für ein i, $\quad 1 \leq i \leq k$ $P_i = Q_1$ gilt und man kann ohne Beschränkung der Allgemeinheit annehmen, dass $i = 1$ ist. Da aber jedes

Primideal in R invertierbar ist, muss auch $P_2 \cdots P_k = Q_2 \cdots Q_s$ gelten und man kann somit sukzessive $P_i = Q_i$ verifizieren.

□

Lemma 2.2.5 *Jedes Bruchideal I eines Dedekindschen Ringes besitzt eine eindeutige Darstellung der Form*

$$I = \frac{P_1 P_2 \cdots P_m}{P_1' P_2' \cdots P_n'} := (P_1')^{-1}(P_2')^{-1} \cdots (P_n')^{-1} P_1 P_2 \cdots P_m$$

wobei $P_1, \ldots, P_m, P_1', \ldots, P_n'$ Primideale sind.

Der Beweis dieses Lemmas soll hier entfallen, er ist nicht sonderlich schwierig und kann zum Beispiel in [4] nachgelesen werden.

Fasst man die bisherigen Ergebnisse über die Eigenschaften von Idealen in Dedekindschen Ringen zusammen, so kann man eine große Ähnlichkeit zu den gewöhnlichen ganzen Zahlen erkennen. Es gibt Primelemente, eine eindeutige Primfaktorenzerlegung und eine zu den rationalen Zahlen analoge Erweiterung um auch bezüglich der Multiplikation eine Gruppenstruktur zu erhalten. Sogar der chinesische Restsatz gilt für Ideale. Es ist daher nur natürlich auch eine Teilbarkeitsbedingung und den größten gemeinsamen Teiler zweier Ideale zu definieren.

Definition 2.2.7 *Seien I und J zwei Ideale eines Dedekindschen Ringes, dann sagt man I teilt J, wenn es ein Ideal K gibt, sodass $J = KI$ gilt.*

Definition 2.2.8 *Seien A und B zwei Ideale eines Dedekindschen Ringes, dann definiert man den größten gemeinsamen Teiler $D = ggT(A, B)$ folgendermaßen: D teilt A und B und jeder gemeinsame Teiler von A und B teilt auch D.*

Die folgenden beiden Lemmata liefern wichtige Eigenschaften des größten gemeinsamen Teilers beziehungsweise der Teilbarkeit zweier Ideale, die Beweise findet man zum Beispiel in [4].

Lemma 2.2.6 *Seien I und J zwei Ideale eines Dedekindschen Ringes dann gilt I teilt J genau dann, wenn $J \subseteq I$.*

Lemma 2.2.7 *Seien A und B zwei Ideale eines Dedekindschen Ringes, dann gilt $ggT(A, B) = A + B$.*

Für die Ideale gewisser Dedekindscher Ringe lässt sich eine Norm definieren, die immer ganzzahlig und größer oder gleich 1 ist. Außerdem ist sie multiplikativ, wie die folgenden Sätze zeigen werden.

Definition 2.2.9 *Ein Dedekindscher Ring R erfüllt die **endliche Normbedingung**, falls für alle Ideale $I \neq 0$ der Faktorring R/I endlich ist. In diesem Fall heißt die Mächtigkeit $N(I) = |R/I|$ die **Norm** des Ideals I.*

Satz 2.2.4 *Sei R ein Dedekindscher Ring und I ein Ideal von R mit $I = \prod_{i=1}^{r} P_i^{e_i}$, dann gilt*

(i)
$$N(I) = \prod_{i=1}^{r} N(P_i^{e_i})$$

(ii) $R/P \simeq P^{e-1}/P^e$ *und*
$$N(P^e) = N(P)^e$$
für jede ganze Zahl $e \geq 0$.

Beweis:

(i) Betrachtet man die Abbildung
$$\Phi : \begin{array}{ccc} R & \to & \oplus_{i=1}^{r}(R/P_i^{e_i}) \\ x & \to & (x_1, \ldots, x_r) \end{array}$$
mit $x_i \equiv x \ (P_i^{e_i})$, so folgt aus dem Chinesischen Restsatz, dass Φ surjektiv ist. Außerdem ist Φ ein Homomorphismus, da jede ihrer Komponenten $x \to x_i \ (P_i^{e_i})$ ein Homomorphismus ist. Wegen Lemma 2.2.1 gilt $\bigcap_{i=1}^{r} P_i^{e_i} = \prod_{i=1}^{r} P_i^{e_i}$ und da $\ker(\Phi) = \bigcap_{i=1}^{r} P_i^{e_i}$, folgt
$$R/I \simeq \oplus(R/P_i^{e_i})$$

oder anders ausgedrückt $N(I) = \prod_{i=1}^{r} N(P_i^{e_i})$.

(ii) Wegen der eindeutigen Primfaktorenzerlegung gilt $P^{e+1} \subsetneq P^e$ und somit gibt es ein $a \in P^e \setminus P^{e+1}$. Definiert man nun ein Abbildung g mittels

$$g : \begin{array}{ccc} \langle R, + \rangle & \to & \langle P^e, + \rangle \\ x & \mapsto & ax, \end{array}$$

so ist g ein Homomorphismus und es gilt $g(P) \subseteq P^{e+1}$. Weiters kann man eine Abbildung $\overline{g}$

$$\overline{g} : \begin{array}{ccc} \langle R/P, + \rangle & \to & \langle P^e/P^{e+1}, + \rangle \\ x + P & \mapsto & ax + P^{e+1} \end{array}$$

einführen, die ebenfalls ein Homomorphismus ist und darüberhinaus bijektiv, wie nun gezeigt werden soll.

Sei $\overline{x} = x + P \in \ker \overline{g}$, dann ist $ax \in P^{e+1}$ und außerdem gilt $(a) \subseteq P^e$ und somit $(a) = P^e Q$ mit $P \nmid Q$. Da $P^e Q(x) = (ax) \subseteq P^{e+1}$ und daher $P^{e+1} | P^e Q(x)$, erhält man $P | Q(x)$ und somit $P|(x)$ woraus $x \in P$ beziehungsweise $\overline{x} = \overline{0}$ und somit die Injektivität von $\overline{g}$ folgt.

Nun bleibt noch die Surjektivität zu zeigen. Sei $\overline{y} = y + P^{e+1}$ mit $y \in P^e$. Da $ggT((a), P^{e+1}) = P^e$ gilt, folgt $aR + P^{e+1} = P^e$ nach Lemma 2.2.7 und somit die Existenz von $x \in R$ und $z \in P^{e+1}$, sodass $ax + z = y$ gilt. Mit diesem x ergibt sich $\overline{g}(x + P) = \overline{y}$ und damit das Gewünschte.

Da die Abbildung

$$\begin{array}{ccc} \langle R/P^e, + \rangle & \to & \langle R/P^{e+1}, + \rangle \\ x + P^e & \mapsto & x + P^{e-1} \end{array}$$

ein surjektiver Homomorphismus mit Kern P^{e-1}/P^e, gilt

$$(R/P^e)/(P^{e-1}/P^e) \simeq R/P^{e-1}.$$

Wegen $N(P^1) = N(P)^1$ kann man Vollständige Induktion anwenden und erhält somit für $e \geq 2$

$$\begin{aligned} N(P^e) = |R/P^e| &= |R/P^{e-1}||P^{e-1}/P^e| \\ &= N(P^{e-1}N(P) \\ &= N(P)^{e-1}N(P) \\ &= N(P)^e. \end{aligned}$$

□

Lemma 2.2.8 *Erfüllt ein Dedekindscher Ring R die endliche Normbedingung, dann gilt*

(i) $N(IJ) = N(I)N(J)$

(ii) Für alle $T \geq 0$ *ist die Menge* $\{0 \neq I \trianglelefteq R | N(I) \leq T\}$ *endlich.*

Beweis:

(i) Die Behauptung folgt direkt aus Satz 2.2.4.

(ii) Seien $a_0, \ldots, a_m$ $m+1$ verschiedene Elemente aus R und I ein Ideal von R mit $N(I) \leq m$, dann gilt $|R/I| \leq m$ und somit muss es $a_i \neq a_j$ geben mit $a_i - a_j \in I$. Hieraus folgt $(a_i - a_j) \subseteq I$ und daher $I|(a_i - a_j)$, es gibt also nur endlich viele Möglichkeiten für I.

□

Das folgende Lemma liefert einen interessanten Zusammenhang zwischen der Norm eines Hauptideals und der Norm seines erzeugenden Elementes.

Lemma 2.2.9 *Ist $a \neq 0$ ein Element des Ringes der ganzen Zahlen O_K und $I = aO_K$, das von a erzeugte Hauptideal, dann gilt*

$$N(I) = |N_{K/Q}(a)| \tag{2.3}$$

Beweis: Sei $O_K = \mathbb{Z}w_i + \cdots + \mathbb{Z}w_n$, dann existieren nach Satz 2.1.1 und Lemma 2.1.4 $\alpha_i = \sum_{j=1}^{n} p_{ij} w_j$, $1 \leq i \leq n$ mit $p_{ii} > 0$, $p_{ij} \in \mathbb{Z}$, sodass $(a) = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$ und $N((a)) = p_{11} \cdots p_{nn}$. Andererseits gilt $(a) = \mathbb{Z}aw_1 + \cdots + \mathbb{Z}aw_n$. Setzt man nun $C = (c_{ij})$ wobei $aw_i = \sum_{j=1}^{n} c_{ij} w_j$ und $R = (r_{ij})$ mit $aw_i = \sum_{j=1}^{n} r_{ij}\alpha_j$, $r_{ij} \in \mathbb{Z}$ und weiters $P = (p_{ij})$, so erhält man

$$\begin{aligned}(aw_1, \ldots, aw_n)^T &= C(w_1, \ldots, w_n)^T \\ &= R(\alpha_1, \ldots, \alpha_n)^T \\ &= RP(w_1, \ldots, w_n)^T,\end{aligned}$$

und daher $N_{K/\mathbb{Q}}(a) = \det C = \det(RP) = \det R \det P$. Da $\{aw_i\}$ und $\{\alpha_i\}$ beide $\mathbb{Z}$-Basen von (a) sind, müssen sowohl R als auch R^{-1} ganzzahlige Einträge haben und somit muss $\det R = \pm 1$ gelten. Hieraus folgt $\det C = \pm \det P$ und wegen $\det P \geq 0$ erhält man insgesamt

$$|N_{K/\mathbb{Q}}(a)| = |\det C| = \det P = N((a)).$$

□

Bisher war vor allem von allgemeinen Dedekindschen Ringe die Rede. Ziel ist es nun zu zeigen, dass der Ring der ganzen Zahlen O_K ein solcher Dedekindscher Ring ist, der darüber hinaus die endliche Normbedingung erfüllt.

Lemma 2.2.10 *Sei I ein Ideal von O_K, dann gilt $I \cap \mathbb{Z} \neq 0$.*

Beweis: Sei $\alpha \in I$ dann gibt es $a_i \in \mathbb{Z}$, sodass $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$ mit $a_m \neq 0$ und somit gilt $a_m \in I \cap \mathbb{Z}$.

□

Satz 2.2.5 *Der Ring der ganzen Zahlen O_K erfüllt die endliche Normbedingung.*

Beweis: Sei I ein Ideal von O_K, dann gibt es nach Lemma 2.2.10 ein $a \in I \cap \mathbb{Z}$, $a \neq 0$. Bezeichnet man mit A das von a erzeugte Hauptideal, so genügt es, da man jeder Restklasse von O_K/A eine Restklasse von O_K/I zuordnen kann, zu zeigen, dass der Index von A in O_K endlich ist, nämlich a^n beträgt.

Sei $w_1, \ldots, w_n$ die Ganzheitsbasis von O_K und $S = \{\sum c_i w_i | 0 \leq c_i < a\}$, dann ist S ein vollständiges Repräsentantensystem der Nebenklassen von O_K/A. Angenommen $w = \sum m_i w_i \in O_K$, dann lässt sich m_i als $m_i = q_i a + c_i$ mit $0 \leq c_i < a$ schreiben und es gilt

$$w \equiv \sum c_i w_i \quad (a).$$

Somit enthält jede Nebenklasse ein Element von S. Angenommen es lägen zwei Elemente von S $\sum c_i w_i$ und $\sum c_i' w_i$ in der selben Nebenklasse, dann würde aus der linearen Unabhängigkeit der w_i folgen, dass $c_i - c_i'$ durch a teilbar wäre. Da aber $0 \leq c_i, c_i' < a$ gilt, folgt daraus $c_i = c_i'$ und daher dass S ein vollständiges Repräsentantensystem der Nebenklassen von O_K/A darstellt mit $|S| = a^n$.

□

Satz 2.2.6 *Sei K ein algebraischer Zahlkörper und O_K der Ring der ganzen Zahlen von K, dann ist O_K ein Noetherscher Ring.*

Beweis: Sei $I_1 \subseteq I_2 \subseteq \ldots$ eine Idealkette von O_K, da $N(I_i)$ immer enlcih ist und darüberhinaus aus $I_1 \subseteq I_i$ folgt, dass $N(I_1) \geq N(I_i)$, kann es nur endlich viele Ideale geben, die I_1 enghalten.

□

Die folgenden zwei Lemmata sollen nicht bewiesen werden, hierfür siehe zum Beispiel [4]

Lemma 2.2.11 *Sei R ein kommutativer Ring mit Einselement, dann gilt:*

(i) Das Ideal I ist genau dann maximal, wenn R/I ein Körper ist.

(ii) Das Ideal I ist genau dann prim, wenn R/I ein Integritätsbereich ist.

Lemma 2.2.12 *Jeder endliche Integritätsbereich ist ein Körper.*

Lemma 2.2.13 *Jedes Primideal von O_K ist maximal.*

Beweis: Da O_K die endliche Normbedingung erfüllt, ist O_K/P endlich für jedes Primideal P, außerdem ist O_K/P nach Lemma 2.2.11 (ii) ein Integritätsbereich, da aber wegen Lemma 2.2.12 jeder endliche Integriätsbereich bereits ein Körper ist, kann man Satz 2.2.11 (i) anwenden und erhält somit, dass P maximal ist.

□

Lemma 2.2.14 *Sei K ein Körper und $R \subseteq K$ ein Ring, dann ist der ganzalgebraische Abschluss $\overline{R}$ ganzalgebraisch abgeschlossen, das heißt es gilt*

$$\overline{\overline{R}} = \overline{R}$$

Beweis: Sei $\vartheta \in \overline{\overline{R}}$, dann gibt es ein normiertes Polynom $f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 \in \overline{R}[x]$ mit $f(\vartheta) = 0$, da die Koeffizienten von $f(x)$ in $\overline{R}$ liegen gibt es normierte Polynome $g_j(x) \in R[x]$ mit $grad(g_j) = k_j$,

sodass $g_j(\alpha_j) = 0$ gilt. Betrachtet man nun das R-Modul

$$\begin{aligned} M &= \left\langle \vartheta^m \alpha_0^{l_0} \cdots \alpha_{n-1}^{l_{n-1}} \right\rangle_{\substack{0 \leq m < n \\ 0 \leq l_i < k_i}} \\ &= R[\vartheta, \alpha_0, \ldots, \alpha_{n-1}] \end{aligned}$$

so ist M sogar ein Ring und aus Lemma 2.1.1 folgt, dass $M \subseteq \overline{R}$ und da $\vartheta \in M$, gilt somit $\vartheta \in \overline{R}$.

□

Satz 2.2.7 *Sei K ein algebraischer Zahlkörper und O_K der Ring der ganzen Zahlen von K, dann ist O_K ein Dedekindscher Ring.*

Beweis: Wie bereits gezeigt, ist O_K ein Noetherscher Ring und jedes seiner Primideale maximal. Außerdem ist O_K der ganzalgebraische Abschluss von $\mathbb{Z}$ in K und somit ganzalgebraisch abgeschlossen.

□

Zum Abschluss dieses Kapitels sollen noch zwei Kenngrößen eines Primideals betrachtet werden, der Verzweigungs- und der Trägheitsindex.

Lemma 2.2.15 *Jedes Primideal $P \neq 0$ von O_K enthält genau eine Primzahl.*

Beweis: Nach Lemma 2.2.10 enthält jedes Ideal von O_K eine ganze Zahl. Diese Zahl ist nun entweder bereits eine Primzahl, oder einer ihrer Primfaktoren muss in P liegen, da nach der Definition eines Primideals mit ab entweder a oder b in P liegen muss. Angenommen P würde zwei Primzahlen p und q enthalten, so müsste P auch ihren größten gemeinsamen Teiler 1 enthalten, da sich dieser nach dem Euklidischen Algorithmus mittels $rp + sq$ mit ganzzahligen r und s darstellen lässt. Hieraus würde aber $P = O_K$ folgen, im Widerspruch zur Annahme.

□

Satz 2.2.8 *Sei K ein algebraischer Zahlkörper mit Erweiterungsgrad n und P ein Primideal von O_K, dann ist $P \cap \mathbb{Z}$ ein Primideal von $\mathbb{Z}$, das heißt $P \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p. Sei $I = pO_K$, dann gilt weiters $I = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$ mit $P_1 = P$ und $N(P_i) = p^{f_i}$, $f_i \in \mathbb{N}, f_i \geq 1$ und überdies erhält man*

$$\sum_{i=1}^{g} e_i f_i = n$$

Beweis: Klarerweise ist $P \cap \mathbb{Z}$ ein Ideal von $\mathbb{Z}$, außerdem gilt, sind $a, b \in \mathbb{Z}$ und $ab \in P \cap \mathbb{Z}$, so folgt, wegen $ab \in P$, $a \in P$ oder $b \in P$ und somit $a \in P \cap \mathbb{Z}$ oder $b \in P \cap \mathbb{Z}$. Da es nach Lemma 2.2.15 genau eine Primzahl in $P \cap \mathbb{Z}$ gibt, ist p eindeutig bestimmt und weil $I \subseteq P$ kann man ohne Beschränkung der Allgemeinheit $P_1 = P$ setzten. Da wegen Lemma 2.2.8 $N((p)) = N(P_1)^{e_1} \cdots N(P_g)^{e_g}$ gilt, folgt

$$N((p)) = N_{K/\mathbb{Q}}(p) = p^n = N(P_1)^{e_1} \cdots N(P_g)^{e_g}$$

und somit muss es für jedes P_i ein f_i geben, sodass $N(P_i) = p^{f_i}$. Hieraus erhält man unmittelbar

$$\sum_{i=1}^{g} e_i f_i = n$$

□

Definition 2.2.10 *Sei K ein algebraischer Zahlkörper, $P \neq 0$ ein Primideal von O_K und $p \in \mathbb{Z}$ so gewählt, dass $P \cap \mathbb{Z} = p\mathbb{Z}$ gilt und $pO_K = P^e P_2^{e_2} \cdots P_g^{e_g}$, dann heißt die natürliche Zahl $e \geq 1$ der* ***Verzweigungsindex*** *von P. Den* ***Trägheitsindex*** *$f(P)$ von P definiert man mittels $|O_K/P| = p^{f(P)}$.*

2.3 Die Klassenzahl

Den Abschluss dieses einführenden Kapitels bildet die Definition der Klassenzahl und der Beweis der Tatsache, dass diese immer endlich ist. Hierfür benötigt man zunächst den Begriff des Quotientenkörpers.

Definition 2.3.1 *Sei R ein Integritätsbereich. Auf den formalen Quotienten $\frac{a}{b}$ a , $b \in R$, $b \neq 0$ wird durch*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

und

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

eine Addition und eine Multiplikation definiert.
Zwei Quotienten $\frac{a}{b}$ *und* $\frac{c}{d}$ *heißen* ***gleich*** *oder* ***äquivalent****, falls*

$$ad = bc$$

gilt. Diese (Äquivalenz-) Relation ist mit den Operationen $+$, $\cdot$ *verträglich. Faktorisiert man nach dieser (Kongruenz-) Relation, so erhält man den* ***Quotientenkörper*** *von* R*.*
R *lässt sich in seinen Quotientenkörper einbetten, indem man* $a \in R$ *mit der Äquivalenzklasse identifiziert, die den Quotienten* $\frac{a}{1}$ *enthält.*

Definition 2.3.2 *Sei* K *ein algebraischer Zahlkörper,* $G(K)$ *die Gruppe der Bruchideale in* K *und* $P(K)$ *die Untergruppe der Hauptbruchideale. Dann bezeichnet man*

$$H(K) = G(K)/P(K)$$

als die ***Idealklassengruppe*** *und*

$$h(K) = |H(K)|$$

als die ***Klassenzahl*** *von* K*.*

Alternativ kann man die Klassenzahl auch folgendermaßen definieren

Definition 2.3.3 *Seien* I *und* J *zwei Bruchideale von* O_K*, dann sind* I *und* J *äquivalent, wenn es Elemente* $a, b \in O_K \setminus \{0\}$ *gibt, sodass*

$$aI = bJ$$

gilt. Die Anzahl der Äquivalenzklassen dieser Äquivalenzrelation entspricht dann der Klassenzahl $h(K)$*.*

Bemerkung: Die beiden Definitionen sind äquivalent, da aus $aI = bJ$ $(a)I = (b)J$ und somit $I = (\frac{b}{a})J$ folgt.

Das folgende Lemma zeigt, dass jede Bruchidealklasse ein Ideal enthält, das heißt, dass es in vielen Situationen ausreicht Ideale zu betrachten anstelle von Bruchidealen, den Beweis findet man zum Beispiel in [4].

Lemma 2.3.1 *Jede Klasse von Bruchidealen kann durch ein Ideal repräsentiert werden.*

Im folgenden soll nun gezeigt werden, dass die Klassenzahl immer endlich ist. Der hier geführte Beweis beruht auf einem Satz H. Minkowskis.

Lemma 2.3.2 *Sei X_t ein Gebiet bestehend aus allen Punkten*

$$(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) \in \mathbb{R}^{r+2s}$$

mit

$$|x_1| + \cdots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \cdots + 2\sqrt{y_s^2 + z_s^2} < t,$$

dann ist X_t beschränkt, symmetrisch und konvex.

Beweis: Klarerweise ist X_t beschränkt und symmetrisch. Um die Konvexität zu beweisen, wählt man zwei beliebige Punkte

$$P = (a_1, \ldots, a_r, b_1, c_1, \ldots, b_s, c_s)$$

und

$$Q = (d_1, \ldots, d_r, e_1, f_1, \ldots, e_s, f_s)$$

aus X_t und zeigt, dass auch $\lambda P + \mu Q$ mit $\lambda, \mu \geq 0$ und $\lambda + \mu = 1$ in X_t liegt. Da, wie leicht nachzurechnen ist, die Ungleichungen

$$|\lambda a_i + \mu d_i| \leq \lambda |a_i| + \mu |d_i|$$

und

$$\sqrt{(\lambda b_i + \mu e_i)^2 + (\lambda c_i + \mu f_i)^2} \leq \lambda \sqrt{b_i^2 + c_i^2} + \mu \sqrt{e_i^2 + f_i^2}$$

gelten, folgt

$$\begin{aligned}
&|\lambda a_1 + \mu d_1| + \cdots + |\lambda a_r + \mu d_r| + 2\sqrt{(\lambda b_1 + \mu e_1)^2 + (\lambda c_1 + \mu f_1)^2} + \cdots \\
&\qquad + 2\sqrt{(\lambda b_s + \mu e_s)^2 + (\lambda c_s + \mu f_s)^2} \\
&\leq \lambda|a_1| + \mu|d_1| + \cdots + \lambda|a_r| + \mu|d_r| + 2\lambda\sqrt{b_1^2 + c_1^2} + 2\mu\sqrt{e_1^2 + f_1^2} + \cdots \\
&\qquad + 2\lambda\sqrt{b_s^2 + c_s^2} + 2\mu\sqrt{e_s^2 + f_s^2} \\
&< \lambda t + \mu t = t.
\end{aligned}$$

□

Lemma 2.3.3 *Sei X_t wie im vorhergehenden Lemma definiert, dann gilt für das Volumen des Gebietes*

$$vol(X_t) = \frac{2^{r-s}\pi^s t^n}{n!}$$

mit $n = r + 2s$.

Beweis: Um das Volumen von X_t zu berechnen, führt man zunächst eine Koordinatentransformation in Polarkoordinaten durch und erhält so mittels $2y_j = \rho_j \cos\theta_j$, $2z_j = \rho_j \sin\theta_j$ und somit $4dy_j dz_j = \rho_j d\rho_j d\theta_j$ für $x_i \geq 0$, $1 \leq i \leq r$

$$\begin{aligned}
vol(X_t) &= 2^r 2^{-2s} \int \rho_1 \cdots \rho_s dx_1 \cdots dx_r d\rho_1 \cdots d\rho_s d\theta_1 \cdots d\theta_s \\
&= 2^r 2^{-2s} (2\pi)^s \int_{Y_t} \rho_1 \cdots \rho_s dx_1 \cdots dx_r d\rho_1 \cdots d\rho_s
\end{aligned}$$

mit

$$Y_t = \{(x_1, \ldots, x_r, \rho_1, \ldots, \rho_s) : x_i, \rho_j \geq 0, x_1 + \cdots + x_r + \rho_1 + \cdots + \rho_s \leq t\}.$$

Setzt man nun

$$f_{r,s}(t) = \int_{Y_t} \rho_1 \cdots \rho_s dx_1 \cdots dx_r d\rho_1 \cdots d\rho_s$$

so erhält man

$$\begin{aligned}
f_{r,s}(1) &= \int_0^1 f_{r-1,s}(1 - x_1) dx_1 \\
&= f_{r-1,s}(1) \int_0^1 (1 - x_1)^{r-1+2s} dx_1 \\
&= \frac{1}{r + 2s} f_{r-1,s}(1)
\end{aligned}$$

Führt man nun diese Vorgehensweise fort, so ergibt sich

$$f_{r,s}(1) = \frac{(2s)!}{(r+2s)!} f_{0,s}(1).$$

Jetzt bleibt nur noch $f_{0,s}(1)$ zu bestimmen:

$$\begin{aligned} f_{0,s}(1) &= \int_0^1 \rho_s f_{0,s-1}(1-\rho_s) d\rho_s \\ &= f_{0,s-1}(1) \int_0^1 \rho_s (1-\rho_s)^{2s-2} d\rho_s \\ &= \frac{f_{0,s-1}(1)}{2s(2s-1)}. \end{aligned}$$

Geht man nun wieder induktiv vor ergibt sich

$$f_{0,s}(1) = \frac{1}{(2s)!}$$

und man erhält insgesamt

$$f_{r,s}(1) = \frac{1}{(r+2s)!} = \frac{1}{n!}.$$

□

Lemma 2.3.4 *Sei C ein beschränktes, symmetrisches, konvexes Gebiet in $\mathbb{R}^n$ und $A \in \mathbb{R}^{n\times n}$ eine Matrix, deren Reihen $a_1, \ldots, a_n$ linear unabhängig über $\mathbb{R}$ sind und für die überdies*

$$vol(C) > 2^n |\det A|$$

gilt, dann gibt es ganze Zahlen $x_1, \ldots, x_n$, nicht alle Null, sodass

$$x_1 a_1 + \cdots + x_n a_n \in C$$

gilt.

Beweis: Betrachtet man die Menge D bestehend aus allen $(x_1, \ldots, x_n) \in \mathbb{R}^n$, sodass

$$x_1 a_1 + \cdots + x_n a_n \in C,$$

so ist D beschränkt, symmetrisch und konvex, da C all diese Eigenschaften besitzt. Außerdem gilt $D = A^{-1}C$ und daher

$$vol(D) = vol(C)(|\det A|)^{-1}.$$

Ist nun $vol(D) > 2^n$, so enthält D einen ganzzahligen Punkt $(x_1, \ldots, x_n) \neq 0$, sodass $x_1a_1 + \cdots + x_na_n \in C$. Da aber $vol(D) > 2^n$ äquivalent zu $vol(C) > 2^n|\det A|$ ist, erhält man das Gewünschte.

□

Lemma 2.3.5 *Sei I ein Ideal von O_K das von $w_1, \ldots, w_n$ erzeugt wird und A die Matrix, deren Zeilen die Vektoren*

$$a_i = (\sigma_1(w_i), \ldots, \sigma_{r_1}(w_i), \Re(\sigma_{r_1+1}(w_i)), \Im(\sigma_{r_1+1}(w_i)), \ldots, \Re(\sigma_{r_1+r_2}(w_i)), \Im(\sigma_{r_1+r_2}(w_i)))$$

bilden, dann gilt

$$|\det A| = 2^{-r_2}|N(I)||d_k|^{1/2}$$

Beweis: Betrachte man die Diskriminante der Elemente $w_1, \ldots, w_n$, so erhält man

$$\begin{aligned} d_{K/\mathbb{Q}}(w_1, \ldots, w_n) &= [\det(\sigma_i(w_j))]^2 \\ &= [\det(\sigma_1(w_i), \ldots, \sigma_{r_1}(w_i), 2\Re\sigma_{r_1+1}(w_i), -i\Im\sigma_{r_1+1}(w_i), \ldots, \\ &\qquad 2\Re\sigma_{r_1+r_2}(w_i), -i\Im\sigma_{r_1+r_2}(w_i))_{i=1,\ldots,n}]^2 \\ &= (-2i)^{2r_2}[\det(\sigma_1(w_i), \ldots, \sigma_{r_1}(w_i), \Re\sigma_{r_1+1}(w_i), \Im\sigma_{r_1+1}(w_i), \\ &\qquad \ldots, \Re\sigma_{r_1+r_2}(w_i), \Im\sigma_{r_1+r_2}(w_i))_{i=1,\ldots,n}]^2 \\ &= (-2i)^{2r_2}(\det A)^2. \end{aligned}$$

Wegen Lemma 2.1.6 gilt außerdem $d_{K/\mathbb{Q}}(w_1, \ldots, w_n) = N(I)^2 d_K$, woraus unmittelbar das Gewünschte folgt.

□

Lemma 2.3.6 *Sei K ein algebraischer Zahlkörper mit Signatur $[r_1, r_2]$ und I ein Ideal von O_K, dann gibt es ein $a \neq 0$ in I, sodass*

$$|N_{K/Q}(a)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|N(I)||d_K|^{\frac{1}{2}}$$

gilt.

Beweis: Sei I ein beliebiges Ideal von O_K und $w_1, \ldots, w_n$ eine Basis von I, dann sind die Vektoren

$$a_i = (\sigma_1(w_i), \ldots, \sigma_{r_1}(w_i), \Re(\sigma_{r_1+1}(w_i)), \Im(\sigma_{r_1+1}(w_i)), \ldots, \\ \Re(\sigma_{r_1+r_2}(w_i)), \Im(\sigma_{r_1+r_2}(w_i))) \in \mathbb{R}^n$$

linear unabhängig. Betrachtet man das beschränkte, symmetrische, konvexe Gebiet X_t, das in Lemma 2.3.2 definiert wurde mit $r = r_1$ und $s = r_2$, dann beträgt nach Lemma 2.3.3 das Volumen von X_t

$$vol(X_t) = \frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!}.$$

Wählt man t so, dass $vol(X_t)$ größer als $2^n|\det A|$ ist, so gibt es nach Lemma 2.3.4 $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, für den

$$0 \neq x_1a_1 + \cdots + x_na_n \in X_t$$

gilt, wobei die Matrix A wie in Lemma 2.3.4 definiert wird. Setzt man $\alpha = x_1w_1 + \cdots + x_nw_n \in I$, so folgt aus der arithmetisch - geometrischen Mittel Ungleichung

$$|N(\alpha)|^{1/n} < \frac{t}{n}$$

und somit

$$|N(\alpha)| < \left(\frac{t}{n}\right)^n.$$

Außerdem gilt mit $\det A = 2^{-r_2}|N(I)||d_K|^{1/2}$

$$\frac{t^n}{n!} = \frac{2^n|\det A|}{2^{r_1-r_2}\pi^{r_2}} = \left(\frac{4}{\pi}\right)^{r_2}|N(I)||d_K|^{1/2}$$

und daher erhält man insgesamt

$$|N(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|N(I)||d_K|^{1/2}$$

.

□

Satz 2.3.1 *Die Klassenzahl $h(K)$ ist für jeden algebraischen Zahlkörper endlich.*

Beweis: Der hier geführte Beweis geht auf H. Minkowski zurück und verwendet folgendes Lemma, das auch eine Abschätzung für $h(K)$ liefert.

Lemma 2.3.7 *Ist K eine algebraische Körpererweiterung mit Erweiterungsgrad n und Signatur $[s,t]$, dann gibt es in jeder Idealklasse ein Ideal dessen Norm nicht größer ist als*

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t\sqrt{|d_K|}.$$

Beweis: Sei I ein beliebiges Ideal von O_K, dann gilt für ein Element $a \in I$, dass das von a erzeugte Hauptideal in I enthalten ist und somit, dass $I|(a)$. Daraus folgt die Existenz eines Ideals J, sodass $IJ = (a)$. Nun kann man Lemma 2.3.6 anwenden und erhält

$$|N_{K/Q}(c)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t\sqrt{|d_K|}N(J) \tag{2.4}$$

für ein $c \neq 0$ aus J. Das von c erzeugte Hauptideal ist, da $(c) \subseteq J$ gilt, durch J teilbar, das heißt es existiert ein Ideal B mit $(c) = BJ$. Daraus folgt, dass $(a)B = (c)I$ und daher liegen B und I in der selben Idealklasse. Da man wegen Lemma 2.2.8(i) und Lemma 2.2.9 $N(B)$ als $N(B) = \frac{|N_{K/Q}(c)|}{N(J)}$ schreiben kann, gilt

$$N(B) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t\sqrt{|d_K|}.$$

□

Satz 2.3.1 folgt nun unmittelbar aus Lemma 2.2.8(ii).

Definition 2.3.4 *Die Zahl*

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t\sqrt{|d_K|} \tag{2.5}$$

wird die Minkowski Konstante des Körpers K genannt.

Abschließend kann man sagen, dass die Anzahl der Ideale des Ringes der ganzen Zahlen eines algebraischen Zahlkörpers, deren Norm kleiner oder gleich der Minkowski Konstante ist, eine obere Schranke für die Klassenzahl dieses Zahlkörpers darstellt.

Den Abschluß dieses Kapitels soll ein Satz bilden, der noch einen Hinweis darauf liefert, warum die Fragestellung, wann ein algebraischer Zahlkörper die Klassenzahl eins besitzt, so interessant ist, den Beweis findet man zum Beispiel in [6].

Satz 2.3.2 *Ist O_K ein Dedekindscher Ring, dann sind die folgenden drei Aussagen äquivalent:*

(i) $H(K) = 1$

(ii) O_K *ist ein Hauptidealring*

(iii) O_K *ist ein faktorieller Ring*

3 Quadratische Zahlkörper

Bisher wurden vor allem allgemeine algebraische Zahlkörper behandelt, in diesem Kapitel soll nun auf einen Spezialfall, die quadratischen Zahlkörper eingegangen werden. Der Vorteil dieser Zahlkörper besteht darin, dass die Lösung des Klassenzahlenproblems sich hier einfacher gestaltet. Insbesondere für den Fall negativer Diskriminante gilt das Problem als gelöst.

3.1 Einführung

Ziel dieses ersten Abschnitts ist es, einige wesentliche Eigenschaften quadratischer Zahlkörper anzuführen. Wichtig ist vor allem eine Ganzheitsbasis für den Ring der ganzen Zahlen zu bestimmen.

Definition 3.1.1 *Ein algebraischer Zahlkörper mit* $[K : \mathbb{Q}] = 2$ *heißt* ***quadratisch****.*

Lemma 3.1.1 *Sei* K *ein quadratischer Zahlkörper, dann gibt es eine eindeutig bestimmte quadratfreie ganze Zahl* $d \neq 1$ *mit* $K = \mathbb{Q}(\sqrt{d})$*.*

Beweis: Da K quadratisch ist, gibt es ein γ, sodass $K = \mathbb{Q}(\gamma)$ mit

$$a\gamma^2 + b\gamma + c = 0 \text{ und } a, b, c \in \mathbb{Z}\ ,\ a, c \neq 0\ ,\ b^2 - 4ac \neq 0.$$

Daraus folgt

$$\gamma = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

setzt man $D = b^2 - 4ac = q^2 d$, d quadratfrei, gilt somit $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$.

Sei nun $K = \mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$, d_1, d_2 quadratfrei, dann kann man $\sqrt{d_2}$ durch

$$\sqrt{d_2} = a + b\sqrt{d_1}$$

ausdrücken. In dieser Darstellung muss $a \neq 0$ sein, da sonst d_2 nicht quadratfrei, und $b \neq 0$, da sonst $\sqrt{d_2} \in \mathbb{Q}$ wäre. Quadriert man nun obige Gleichung, erhält man

$$d_2 = a^2 + 2ab\sqrt{d_1} + b^2 d_1,$$

woraus $\sqrt{d_1} \in \mathbb{Q}$ folgen würde im Widerspruch zu d_1 quadratfrei. Somit ist auch die Eindeutigkeit bewiesen.

□

Satz 3.1.1 *Sei $d \neq 1$ quadratfrei und $K = \mathbb{Q}(\sqrt{d})$, dann gilt für den Ring der ganzen Zahlen O_K*

$$O_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}\ , \qquad d_K = 4d \text{ für } d \equiv 2,3 \quad (4) \tag{3.1}$$

$$O_K = \mathbb{Z} + \mathbb{Z}\left(\frac{-1+\sqrt{d}}{2}\right),\ d_K = d \quad \text{für } d \equiv 1 \quad (4) \tag{3.2}$$

Beweis: Sei γ ein beliebiges Element aus K mit der Darstellung $\gamma = r + s\sqrt{d}$, dann gilt $\gamma^2 - (sp(\gamma))\gamma + N(\gamma) = 0$ mit $sp(\gamma) = 2r$ und $N(\gamma) = r^2 - ds^2$. Daher ist γ genau dann aus O_K, wenn $2r \in \mathbb{Z}$ und $r^2 - ds^2 \in \mathbb{Z}$. Sind diese Bedingungen erfüllt, so muss $(2r)^2 - 4ds^2 \in \mathbb{Z}$ und somit, da $2r \in \mathbb{Z}$, auch $4ds^2$ in $\mathbb{Z}$ liegen. Da d quadratfrei ist, gilt $2s \in \mathbb{Z}$. Setzt man $m = 2r$ und $n = 2s$ dann ist $m^2 - dn^2 \equiv 0\ (4)$.

Ist nun $d \equiv 2,3\ (4)$ dann gilt entweder $m^2 + n^2 \equiv 0\ (4)$ oder $m^2 + 2n^2 \equiv 0\ (4)$. Da $m^2, n^2 \equiv 0, 1\ (4)$, folgt hieraus $m \equiv n \equiv 0\ (2)$ und damit $r, s \in \mathbb{Z}$ beziehungsweise $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Für die Determinante d_K gilt dann

$$d_K = \begin{vmatrix} sp(1) & sp(\sqrt{d}) \\ sp(\sqrt{d}) & sp(d) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d$$

Betrachte man den Fall $d \equiv 1\ (4)$, so ist $m^2 - n^2 \equiv 0\ (4)$ und somit $m \equiv n\ (2)$. Für den Ring der ganzen Zahlen gilt deshalb

$$\begin{aligned} O_K &= \left\{ \frac{m+n\sqrt{d}}{2} |\ m, n \in \mathbb{Z} \quad , \quad m \equiv n \quad (2) \right\} \\ &= \left\{ \frac{m+n}{2} + n\left(\frac{-1+\sqrt{d}}{2}\right) |\ m, n \in \mathbb{Z} \quad , \quad m \equiv n \quad (2) \right\} \\ &= \mathbb{Z} + \mathbb{Z}\frac{-1+\sqrt{d}}{2}. \end{aligned}$$

Die Diskriminante ist dann wie man analog zu oben leicht nachrechnen kann $d_K = d$.

□

Bemerkung: Aus obigem Satz folgt unmittelbar, dass für $m = d_K$ das Paar $(1, (m + \sqrt{m})/2)$ immer eine Ganzheitsbasis von O_K bildet.

Eine endliche Körpererweiterung E/K heißt Galoisch, falls E Zerfällungskörper eines separablen Polynoms ist, das heißt, es gibt ein Polynom, das keine mehrfachen Nullstellen besitzt und über E in Linearfaktoren zerfällt. Der folgende Satz besagt, dass jede quadratische Körpererweiterung diese Eigenschaft erfüllt. Der Beweis dieser Tatsache basiert darauf, das setzt man $E = \mathbb{Q}(\sqrt{d})$, das Minimalpolynom von $\sqrt{d}$ $p(x) = x^2 - d$ einerseits über $\mathbb{Q}(\sqrt{d})$ in Linearfaktoren zerfällt und andererseits für $d \neq 0$ nur einfache Nullstellen besitzt.

Satz 3.1.2 *Jede quadratische Körpererweiterung von $\mathbb{Q}$ ist Galoisch.*

Weiters heißt eine Galoische Körpererweiterung $K/\mathbb{Q}$ Abelsch, falls ihre Galoisgruppe, das heißt die Gruppe der Automorphismen auf K, die $\mathbb{Q}$ elementweise fest lassen, Abelsch ist. Da die Galoisgruppe eines quadratischen Zahlkörpers gleich $\{id, \sqrt{d} \mapsto -\sqrt{d}\}$ ist, trifft diese Tatsache zu.

Satz 3.1.3 *Jeder quadratische Zahlkörper ist abelsch.*

Im folgenden sollen, wenn nicht anders angegeben, K immer einen quadratischen Zahlkörper, d die eindeutig bestimmte, quadratfreie ganze Zahl, für die $K = \mathbb{Q}(\sqrt{d})$ gilt, d_K die zugehörige Diskriminante und O_K den Ring der ganzen Zahlen bezeichnen.

3.2 Die Dirichletsche Klassenzahlformel

Dieser Abschnitt ist dem Beweis der Dirichletschen Klassenzahlformel gewidmet. Viele der verwendeten Sätze gehen bereits auf Dirichlet zurück. Zunächst benötigt man den Begriff des Legendresymbols. Das Legendresymbol gibt an, ob eine Zahl n quadratischer Rest modulo einer Primzahl ist oder nicht.

Definition 3.2.1 *Sei p eine Primzahl, dann definiert man das **Legendresymbol** $(\frac{n}{p})$ durch*

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \textit{falls} \quad x^2 \equiv n \pmod{p} \textit{ lösbar} \quad \textit{und } p \nmid n \\ -1 & \textit{falls} \quad x^2 \equiv n \pmod{p} \textit{ unlösbar} \quad \textit{und } p \nmid n \\ 0 & \textit{falls} \quad p|n \end{cases} \tag{3.3}$$

Das Legendresymbol besitzt einige interessante Eigenschaften, die seine Berechnung wesentlich vereinfachen, es gilt zum Beispiel $(a/p) = (b/p)$ falls $a \equiv b \bmod p$, wie unmittelbar aus der Definition folgt. Die Beweise zu den Sätzen 3.2.1 und 3.2.3, sowie Lemma 3.2.1 findet man zum Beispiel in [4].

Lemma 3.2.1 *Das Legendresymbol ist mulitiplikativ, das heißt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Satz 3.2.1 *Sei p eine ungerade Primzahl, dann gilt*

(i)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

(ii)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

(iii)

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

Satz 3.2.2 *Die Anzahl der quadratischen Reste ist gleich der Anzahl der quadratischen Nichtreste* $\bmod p$.

Beweis: Für eine Primzahl p ist die zugehörige Faktorgruppe zyklisch mit einem erzeugenden Element g der Ordnung $p-1$. Daher gilt für jede gerade Potenz g^{2k} von g

$$\left(g^{2k}\right)^{(p-1)/2} = \left(g^{p-1}\right)^k \equiv 1 \quad (p),$$

für ungerade jedoch

$$\left(g^{2k+1}\right)^{(p-1)/2} = \left(g^{(p-1)/2}\right) \not\equiv 1 \quad (p).$$

Es gilt also für die Hälfte der Elemente der Faktorgruppe, nämlich für die geraden Potenzen von g

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv 1 \quad (p).$$

Da die Mächtigkeit der Faktorgruppe einer Primzahl p jedoch immer $p-1$ beträgt, sind $(p-1)/2$ Elemente quadratische Reste und die übrigen $(p-1)/2$ quadratische Nichtreste $\mod p$.

□

Folgerung: Für eine feste Primzahl p gilt

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Satz 3.2.3 (Quadratisches Reziprozitätsgesetz) *Für zwei unterschiedliche, ungerade Primzahlen p und q gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{3.4}$$

Eine natürliche Verallgemeinerung des Legendresymbols stellt das Jacobisymbol dar.

Definition 3.2.2 *Für ganze Zahlen a und ungerade, positive Zahlen b wird das **Jacobisymbol** $(\frac{a}{b})$ durch*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_l}\right)$$

definiert, wobei $b = p_1 \cdots p_l$ die Primfaktorenzerlegung von b ist und $(\frac{a}{p_j})$ das Legendresymbol bezeichnet.

Für das Jacobisymbol gelten ganz ähnliche Rechenregeln wie für das Legendresymbol, man beachte jedoch, dass hier die Bedingung $(a/b) = 1$ nur noch notwendig, jedoch nicht hinreichend für die Lösbarkeit von $x^2 \equiv a \mod b$ ist. Den Beweis für den folgenden Satz findet man zum Beispiel in [4].

Satz 3.2.4 (Rechenregeln für das Jacobisymbol) *Seien a_1, a_2, a ganze Zahlen und b_1, b_2, b ungerade ganze Zahlen, dann gilt*

(i)

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$$

(ii)

$$\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$$

(iii)

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$$

(iv)

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

(v)

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

In Anlehnung an die bisher definierten Symbole kann man ein weiteres Symbol, das Kroneckersymbol einführen.

Definition 3.2.3 *Mit Hilfe des Legendresymbols kann man für gewisse Zahlen d das* ***Kroneckersymbol*** $(\frac{d}{n})$ *folgendermaßen definieren:*

(i) $d = \varepsilon p_1 \cdots p_r \equiv 1 \ (4)$ *mit* $\varepsilon = \pm 1,\ r \geq 1$ *und* $p_i \equiv 1 \ (2),\ 1 \leq i \leq r$

$$\left(\frac{d}{n}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)$$

(ii) $d = 4\varepsilon p_1 \cdots p_r$ *mit* $\varepsilon p_1 \cdots p_r \equiv 3 \ (4),\ r \geq 0$ *und* $p_i \equiv 1 \ (2),\ 1 \leq i \leq r$

$$\left(\frac{d}{n}\right) = \begin{cases} \eta \prod_{i=1}^{r} \left(\frac{n}{p_i}\right) & \text{für } n \equiv 1 \quad (2) \\ 0 & \text{für } n \equiv 0 \quad (2) \end{cases}$$

wobei

$$\eta = \begin{cases} 1 & \text{für } n \equiv 1 \quad (4) \\ -1 & \text{für } n \equiv -1 \quad (4) \end{cases}$$

(iii) $d = 8\varepsilon p_1 \cdots p_r$ *mit* $r \geq 0$ *und* $p_i \equiv 1 \ (2),\ 1 \leq i \leq r$

$$\left(\frac{d}{n}\right) = \begin{cases} (-1)^{(n^2-1)/8} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right) & \text{falls } n \equiv 1 \quad (2) \\ & \text{und } sgn(d) = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) \\ \eta(-1)^{(n^2-1)/8} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right) & \text{falls } n \equiv 1 \quad (2) \\ & \text{und } sgn(d) \neq \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) \\ 0 & \text{falls } n \equiv 0 \quad (2) \end{cases}$$

Alternativ kann man das Kroneckersymbol auch folgendermaßen mit Hilfe des Jacobisymbols definieren. Der Beweis für die Äquivalenz der beiden Definitionen soll hier nicht ausgeführt werden. Es sei nur bemerkt, dass er unmittelbar aus den Sätzen über das Legendre- und das Jacobisymbol, sowie aus Lemma 3.2.2 folgt.

Satz 3.2.5 *Sei* $d \equiv 0, 1 \ (4)$ *und* $n = 2^c n_1,\ 2 \nmid n_1$, *dann definiert man eine Erweiterung des Jacobisymbols folgendermaßen*

$$\left(\frac{d}{n}\right) = \left(\frac{d}{2}\right)^c \left(\frac{d}{n_1}\right),$$

wobei (d/n_1) *das Jacobisymbol bezeichnet und* $(d/2)$ *wie folgt definiert wird*

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & \text{falls} \quad d \equiv 0 \bmod 4 \\ 1 & \text{falls} \quad d \equiv 1 \bmod 8 \\ -1 & \text{falls} \quad d \equiv 5 \bmod 8 \end{cases}.$$

Dieses erweiterte Jacobisymbol ist äquivalent zum Kroneckersymbol.

Wie dieser Satz zeigt, lassen sich einige Eigenschaften des Jacobisymbols, wie zum Beispiel die Multiplikativität der unteren Komponente auf das Kroneckersymbol übertragen. Außerdem folgt aus der Definition des Kroneckersymbols über das Legendresymbol zum Beispiel $(d/n) = (d/n_0)$ falls $n \equiv n_0 \ (d)$.

Lemma 3.2.2 *Sei* d *Diskriminante eines quadratischen Zahlkörpers und* $(d/2)$

das Kroneckersymbol, dann gilt

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & \textit{falls} \quad 2|d \\ 1 & \textit{falls} \quad d \equiv 1 \bmod 8 \\ -1 & \textit{falls} \quad d \equiv 5 \bmod 8. \end{cases} \tag{3.5}$$

Beweis: Der Fall $2|d$ folgt direkt aus der Definition des Kronecker Symbols. Wegen Satz 3.2.1 (ii) ist 2 immer quadratischer Rest der Primzahlen der Form $8n+1$ oder $8n+7$ und quadratischer Nichtrest der Primzahlen der Form $8n+5$ oder $8n+3$. Daher gilt

$$\left(\frac{p}{2}\right) = \begin{cases} 1 & \text{falls} \quad p = 8n+1 \quad \text{oder} \quad p = 8n+7,\ p \quad \text{prim} \\ -1 & \text{falls} \quad p = 8n+5 \quad \text{oder} \quad p = 8n+3,\ p \quad \text{prim}. \end{cases}$$

Da d als Diskriminante eines quadratischen Zahlkörpers äquivalent $0, 1 \ (4)$ sein muss, kann sie im Falle $2 \nmid d \mod 8$ nur äquivalent 1 oder 5 sein. Hat nun d die Primfaktorenzerlegung $d = p_1 \cdots p_s$ und bezeichne r_i den Rest von p_i modulo 8 , so muss, weil ja das Produkt der Reste $\mod 8$, der Rest des Produktes ist, $r_1 \cdots r_s \equiv 1, 5 \ (8)$ gelten. Da die ungeraden Reste $\mod 8$ eine involutorische Gruppe bilden, kann d nur dann äquvialent $1 \mod 8$ sein, wenn die Reste $3, 5$ und 7 entweder alle in gerader oder alle in ungerader Anzahl vorkommen. Daraus folgt aber, dass $(d/2) = 1$ gilt. Ist nun d äquivalent $5 \mod 8$, so muss entweder 5 in einer ungeraden Anzahl auftreten oder 3 und 7, in beiden Fällen ist dann $(d/2) = -1$.

□

Der folgende Satz liefert einen Zusammenhang zwischen dem Legendresymbol (d/p), wobei hier p eine ungerade Primzahl darstellt, und der Struktur des von p erzeugten Hauptideals. Für $p = 2$ gilt eine ähnliche Aussage, man betrachtet hier jedoch die Reste modulo 8 beziehungsweise die Teilbarkeit durch 2.

Satz 3.2.6 *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper, d_K seine Diskriminante, p eine ungerade Primzahl und bezeichne (d/p) das Legendre Symbol, dann gilt:*

(i) $(d/p) = 1$ *dann und nur dann, wenn* $pO_K = PP'$,

(ii) $(d/p) = 0$ *dann und nur dann, wenn* $pO_K = P^2$,

(iii) $(d/p) = -1$ *dann und nur dann, wenn* $pO_K = P$,

wobei $P \neq P'$ *Primideale von* O_K *sind. Ist jedoch* $p = 2$, *dann folgt*

(i) $2O_K = PP'$ *dann und nur dann, wenn* $d \equiv 1 \bmod 8$ *und* $2 \nmid d_K$,

(ii) $2O_K = P^2$ *dann und nur dann, wenn* $2|d_K$,

(iii) $2O_K = P$ *dann und nur dann, wenn* $d \equiv 5 \bmod 8$ *und* $2 \nmid d_K$.

Beweis: Zunächst soll der Satz für $p \neq 2$ bewiesen werden:

(i) $\Rightarrow$ Da $(d/p) = 1$ gilt, gibt es ein a, sodass

$$a^2 \equiv d \quad (p).$$

Setzt man nun

$$P = (p, a + \sqrt{d}) \quad \text{und} \quad P' = (p, a - \sqrt{d})$$

so erhält man $pO_K = PP'$, denn

$$\begin{aligned} PP' &= (p, a + \sqrt{d})(p, a - \sqrt{d}) \\ &= (p^2, p(a + \sqrt{d}), p(a - \sqrt{d}), a^2 - d) \\ &= (p)(p, a + \sqrt{d}, a - \sqrt{d}, (a^2 - d)/p) \\ &= (p) \end{aligned}$$

Die letzte Gleichheit gilt, da $2a$ und p beide im zweiten Ideal enthalten sind, nun ist aber $(2a, p) = 1$ und daher $1 \in (p, a + \sqrt{d}, a - \sqrt{d}, (a^2 - d)/p)$. Klarerweise ist $P \neq P'$ da sonst $2a$ und p in P liegen würden, woraus $P = O_K$ folgen würde, was nicht der Fall sein kann. Da die Norm von pO_K gleich p^2 ist, muss $N(P)|p^2$ gelten. Weil $P \neq (1)$ gilt $N(P) \neq 1$ und aus Symmetriegründen kann die Norm von P auch nicht p^2 sein, somit besitzen sowohl P als auch P' als Norm p und sind daher beide prim.

$\Leftarrow$ Da $pO_K = PP'$ muss es ein $a \in P$ geben, dass allerdings nicht in pO_K liegt. Nach der Bemerkung zu Satz 3.1.1 bildet $\{1, (m + \sqrt{m})/2\}$ mit $m = d_K$ eine Ganzheitsbasis von O_K, also lässt sich a mittels

$$a = x + y\frac{m + \sqrt{m}}{2}$$

darstellen, wobei p kein gemeinsamer Teiler von x und y ist. Betrachtet man nun das von a erzeugte Ideal, so gilt $(a) \subseteq P$ also $P|(a)$, daher muss die Norm von P auch die Norm von (a)

$$N(a) = \left| \left(x + \frac{ym}{2}\right)^2 - \frac{y^2 m}{4} \right|$$

teilen. Daraus folgt

$$(2x + ym)^2 \equiv y^2 m \quad (p).$$

Gilt nun $p|y$ so folgt $p|(2x+ym)^2$, dann müsste aber p $2x$ und somit, da p ungerade ist, x teilen, im Widerspruch zu der Voraussetzung, dass p kein gemeinsamer Teiler von x und y ist. Also folgt y^2 ist nicht äquivalent 0 mod p und da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist gilt

$$\frac{(2x + ym)^2}{y^2} \equiv m \quad (p).$$

Daher wurde ein z gefunden, sodass $z^2 \equiv m$ (p) und da $m = d$ oder $m = 4d$ gilt erhält man $(d/p) = 1$.

(ii) $\Rightarrow$ Zunächst soll gezeigt werden, dass $pO_K = (p, \sqrt{d})^2$ gilt: Da $(d/p) = 0$ folgt $p|d$ und da d quadratfrei ist, sind d/p und p relativ prim, das heißt $(p, \sqrt{d}, d/p) = 1$, somit erhält man

$$\begin{aligned}(p, \sqrt{d})^2 &= (p^2, p\sqrt{d}, d) \\ &= (p)(p, \sqrt{d}, d/p) \\ &= (p).\end{aligned}$$

Aus den gleichen Gründen wie oben folgt, dass $(p, \sqrt{d})$ ein Primideal ist.

$\Leftarrow$ Analog zu obigem Beweis muss es wiederum ein a geben, dass in P, nicht aber in pO_K liegt. Sei m die Diskriminante von K dann lässt sich a folgendermaßen darstellen:

$$a = x + y\frac{m + \sqrt{m}}{2},$$

wobei p abermals kein gemeinsamer Teiler von x und y ist. Da $a^2 \in O_K$, erhält man

$$\frac{(2x + ym)^2 + my^2}{4} + 2y\frac{2x + ym}{4}\sqrt{m} \in pO_K.$$

Hieraus folgt $p|(2x+ym)^2+my^2$ und $p|y(2x+ym)$. Teilt p nun y, so folgt p teilt $2x$ und da p ungerade ist $p|x$, im Widerspruch zur Annahme, dass a kein Element von pO_K ist. Also gilt $p|2x+ym$ und $p|my^2$, woraus $p|m$ folgt. Da p eine ungerade Primzahl ist ergibt sich hieraus $(d/p) = 0$.

(iii) Diese Äquvivalenz folgt unmittelbar aus den beiden vorherigen. Ist $(d/p) = -1$ so kann nur der Fall $pO_K = P$ eintreten, da die anderen beiden möglichen Fälle ausgeschlossen werden können. (Der Fall, dass pO_K ein Produkt von mehr als 2 Primidealen ist, ist nicht möglich, da $N(pO_K) = p^2$ und die Norm multiplikativ ist.) Umgekehrt bleibt für $pO_K = P$ nur der Wert $(d/p) = -1$.

Jetzt bleibt noch der Fall $p = 2$ zu betrachten.

(i) $\Leftarrow$ Analog zum vorhergehenden Beweis soll gezeigt werden, dass

$$2O_K = PP' \quad \text{mit} \quad P = \left(2, \frac{1+\sqrt{d}}{2}\right) \quad \text{und} \quad P' = \left(2, \frac{1-\sqrt{d}}{2}\right).$$

Betrachtet man nun PP' so erhält man

$$\left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right) = (2)\left(2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{4}\right),$$
$$= (2)$$

da $1 = (1+\sqrt{d})/2 + (1-\sqrt{d})/2$ im zweiten Ideal enthalten ist. Die prim-Eigenschaft folgt wie oben.

$\Rightarrow$ Sei $(2) = PP'$ mit $P \neq P'$, dann folgt wegen (ii) $d \equiv 1\ (4)$. Außerdem existiert ein Element $a \in P$, das allerdings nicht in PP' liegt, daher gilt, schreibt man a als

$$a = m + n\frac{1+\sqrt{d}}{2},$$

dass 2 kein gemeinsamer Teiler von m und n ist. Da $(a) \subseteq P$ gilt, folgt $2 = N(P)|N((a))$. Da

$$N((a)) = |N(a)| = \left|\frac{(2m+n)^2}{4} - \frac{n^2 d}{4}\right|,$$

erhält man

$$(2m+n)^2 \equiv n^2 d \bmod 8.$$

Angenommen $n = 2n_1$, $n_1 \equiv 1\ (2)$, dann folgt $2|(m+n_1)^2 + n_1^2 d$. 2 ist allerdings kein Teiler von $n_1^2 d$, daher kann 2 auch nicht $(m+n_1)^2$ teilen. Hieraus ergibt sich, dass m gerade sein muss im Widerspruch zu der Tatsache, dass 2 ein gemeinsamer Teiler von m und n ist. Angenommen $4|n$, dann muss 4 auch ein Teiler von $2m+n$ sein, und somit wäre m gerade, abermals im Widerspruch zur Voraussetzung. Es muss also n ungerade sein und ist daher äquivalent zu einer primen Restklasse mod 8. Aus der Gruppeneigenschaft der Menge der primen Restklassen folgt nun die Existenz eines n_2, sodass $nn_2 \equiv 1\ (8)$ gilt. Man erhält also

$$d \equiv n_2^2(2m+n)^2 \bmod 8$$

und da $2 \nmid d$, muss $n_2(2m+n)$ ungerade sein, woraus

$$d \equiv 1 \bmod 8$$

folgt.

(ii) $\Leftarrow$ Teilt 2 d_K, dann folgt nach Satz 3.1.1, dass $d \equiv 2,\ 3\ (4)$. Ist $d \equiv 2\ (4)$ dann folgt $(2) = (2, \sqrt{d})^2$, denn

$$\begin{aligned}(2, \sqrt{d})^2 &= (4, 2\sqrt{d}, d) \\ &= (2)(2, \sqrt{d}, d/2)\cdot \\ &= (2)\end{aligned}$$

Die letzte Gleichheit erhält man aus der Tatsache, dass 2 und $d/2$ teilerfremd sind, da d quadratfrei ist und somit $(2, \sqrt{d}, d/2) = O_K$ gilt. $P = (2, \sqrt{d})$ ist weiters ein Primideal, da $N(P) = 2$ gelten muss. Tritt nun der Fall $d \equiv 3\ (4)$ ein, so ist $(2) = (2, 1+\sqrt{d})^2$, weil

$$\begin{aligned}(2, 1+\sqrt{d})^2 &= (4, 2+2\sqrt{d}, 1+d+2\sqrt{d}) \\ &= (2)\left(1, 1+\sqrt{d}, \frac{1+d}{2} + \sqrt{d}\right) \\ &= (2).\end{aligned}$$

Die letzte Gleichheit gilt wiederum da $1+\sqrt{d}$ und $\frac{1+d}{2} + \sqrt{d}$ teilerfremd sind. Der Rest folgt analog zu oben.

$\Rightarrow$ Nach Satz 3.1.1 ist $d_K \equiv 0, 1\ (4)$. Angenommen $d_K \equiv 1\ (4)$, dann wäre

$$O_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$$

und für ein $a \in P \setminus P^2$ würde $a = m + n(1+\sqrt{d})/2$ mit m und n sind entweder 0 oder 1 gelten, da für jedes $\alpha \in O_K$ $a + 2\alpha$ in $P \setminus P^2$ liegt. Würde $n = 0$ gelten, dann müsste $m \neq 0$ sein, da sonst $a = 0 \in (2) = P^2$, ist andererseits $m = 1$ so wäre $a = 1$ und daher $a \notin P$ da $P \neq O_K$. Also folgt $n = 1$ und $m = 0$ oder 1. Da a^2 in (2) liegt, erhält man im Widerspruch dazu

$$\begin{aligned} a^2 &= \left(m + \frac{1+\sqrt{d}}{2} \right)^2 \\ &= m^2 + \frac{d-1}{4} + (2m+1)\frac{1+\sqrt{d}}{2} \notin (2), \end{aligned}$$

da $(2m+1)$ ungerade ist. Somit muss $d_K \equiv 0 \ (4)$ gelten.

(iii) Die dritte Aussage folgt direkt aus den beiden ersten, da aus $2 \nmid d_K$ und d nicht äquivalent 1 mod 8 folgt, dass $d \equiv 5 \ (8)$. Andererseits muss $(2) = P$ gelten, da die anderen beiden Fälle, $(2) = PP'$ und $(2) = P^2$ ausgeschlossen sind.

□

Bemerkung: Nach Satz 3.2.5 gilt, wenn man mit $(d/2)$ das Kroneckersymbol bezeichnet, ein zum ersten Teil des Satzes analoges Ergebnis.

Mit Hilfe dieser Ergebnisse lassen sich nun die folgenden zwei Lemmata beweisen, die eine Formel für die Anzahl der Ideale mit einer bestimmten Norm liefern. Diese Formel hängt nur von der Diskriminante und der Primfaktorenzerlegung der Norm ab.

Lemma 3.2.3 *Sei a_n die Anzahl der Ideale in O_K mit Norm n, dann gilt für alle Primzahlen p*

$$a_{p^\alpha} = \sum_{j=0}^{\alpha} \left(\frac{d_K}{p^j} \right) = \sum_{l | p^\alpha} \left(\frac{d_K}{l} \right). \tag{3.6}$$

Beweis: Wegen Satz 2.2.8 und Satz 3.2.6 ist die Norm eines Primideals entweder p oder p^2, wobei der zweite Fall nur auftreten kann, wenn $(d_K/p) = -1$ ist. Die Fälle $\alpha = 1$ und $\alpha = 2$ folgen nun unmittelbar aus den vorhergehenden Sätzen. Sei nun $\alpha > 2$, ist $(d_K/p) = -1$, dann gilt $a_{p^\alpha} = 0$ für α

ungerade und $a_{p^\alpha} = 1$ für α gerade, da nur Ideale, deren Norm eine gerade Potenz von p ist, dargestellt werden können. Im Falle $(d_K/p) = 1$, sind die Ideale mit Norm p^α von der Form $P^j(P')^{\alpha-j}$, $0 \leq j \leq \alpha$, es gibt also genau $\alpha + 1$ von ihnen. Das stimmt mit obiger Summe überein. Es bleibt jetzt nur noch die letzte Möglichkeit zu betrachten, nämlich $(d_K/p) = 0$. Hier gibt es nur ein Ideal mit passender Norm.

□

Lemma 3.2.4 *Sei a_n die Anzahl der Ideale mit Norm n, dann gilt*

$$a_n = \sum_{l|n} \left(\frac{d_K}{l} \right). \tag{3.7}$$

Beweis: Da aus der Multiplikativität der Norm und der eindeutigen Primfaktorenzerlegung der Ideale die Multiplikativität von a_n folgt, erhält man aus dem vorhergehenden Lemma

$$a_n = \prod_{p^\alpha | n} \left(\sum_{j=0}^{\alpha} \left(\frac{d_K}{p^j} \right) \right).$$

Die Formel (3.7) folgt nun unmittelbar durch Umformungen.

□

Zwei weitere Eigenschaften des Kroneckersymbols (d_K/n) liefern die folgenden beiden Lemmata. Einerseits gilt, dass es immer ein n gibt, sodass $(d_K/n) = -1$, andererseits ist für jedes x die Summe $\left|\sum_{n \leq x} \left(\frac{d_K}{n}\right)\right|$ immer kleiner oder gleich dem Betrag der Determinante.

Lemma 3.2.5 *Sei d_K die Diskriminante eines quadratischen Zahlkörpers, dann gibt es ein $n > 0$, sodass $(d_K/n) = -1$ gilt.*

Beweis: Aus Satz 3.1.1 folgt, dass d_K nur folgende Formen annehmen kann:

(i)

$$d_K = \varepsilon p_1 \cdots p_r \equiv 1 \quad (4) \quad \text{mit} \quad \varepsilon = \pm 1,\ r \geq 1$$
$$\text{und} \quad p_i \equiv 1 \quad (2),\ 1 \leq i \leq r$$

(ii)

$$d_K = 4\varepsilon p_1 \cdots p_r \quad \text{mit} \quad \varepsilon p_1 \cdots p_r \equiv 3 \quad (4),\ r \geq 0$$
$$\text{und} \quad p_i \equiv 1 \quad (2),\ 1 \leq i \leq r$$

(iii)

$$d_K = 8\varepsilon p_1 \cdots p_r \quad \text{mit} \quad r \geq 0$$
$$\text{und} \quad p_i \equiv 1 \quad (2),\ 1 \leq i \leq r$$

Nun betrachtet man die einzelnen Fälle gesondert:

(i) Aus der Definition des Kroneckersymbols erhält man

$$\left(\frac{d}{n}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)$$

Wegen des chinesischen Restsatzes kann man n so wählen, dass

$$\begin{aligned} n &\equiv a_i^2 \quad (p_i)\ ,\ i = 1, \ldots, r-1 \\ n &\equiv a_r \quad (p_r) \end{aligned}$$

gilt, wobei a_r quadratischer Nichtrest $\mod p_r$ ist. Somit gilt $(n/p_i) = 1$ für $i \neq r$ und $(n/p_r) = -1$, also insgesamt $(d/n) = -1$.

(ii) Es gilt

$$\left(\frac{d}{n}\right) = \begin{cases} \eta \prod_{i=1}^{r} \left(\frac{n}{p_i}\right) & \text{für } n \equiv 1 \quad (2) \\ 0 & \text{für } n \equiv 0 \quad (2) \end{cases}$$

wobei

$$\eta = \begin{cases} 1 & \text{für } n \equiv 1 \quad (4) \\ -1 & \text{für } n \equiv -1 \quad (4) \end{cases}$$

Wegen des chinesischen Restsatzes kann man n so wählen, dass

$$\begin{aligned} n &\equiv a_i^2 \quad (p_i)\ ,\ i = 1, \ldots, r \\ n &\equiv -1 \quad (4) \end{aligned}$$

woraus $(d/n) = -1$ folgt.

(iii) Im letzten Fall gilt

$$\left(\frac{d}{n}\right) = \begin{cases} (-1)^{(n^2-1)/8} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right) & \text{falls } n \equiv 1 \quad (2) \\ & \text{und } \operatorname{sgn}(d) = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) \\ \eta(-1)^{(n^2-1)/8} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right) & \text{falls } n \equiv 1 \quad (2) \\ & \text{und } \operatorname{sgn}(d) \neq \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) \\ 0 & \text{falls } n \equiv 0 \quad (2) \end{cases}$$

Hier muss man die beiden Möglichkeiten $\operatorname{sgn}(d) = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right)$ und $\operatorname{sgn}(d) \neq \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right)$ unterscheiden. Im ersten Fall wählt man n so, dass

$$\begin{aligned} n &\equiv a_i^2 \quad (p_i) \ , \ i = 1, \ldots, r \\ n &\equiv 3 \quad (16) \end{aligned}$$

gilt, da aus $n \equiv 3$ (16) folgt, dass $(n^2-1)/8 \equiv 1$ (2) ist und somit $(d/n) = -1$. Im zweiten Fall sucht man ein n, sodass

$$\begin{aligned} n &\equiv a_i^2 \quad (p_i) \ , \ i = 1, \ldots, r \\ n &\equiv -3 \quad (16). \end{aligned}$$

Hieraus folgt $(-1)^{(n^2-1)/8} = -1$ und $\eta = 1$, also wiederum das gewünschte $(d/n) = -1$

□

Lemma 3.2.6 *Sei (d_K/n) das Kroneckersymbol, dann gilt*

$$\left| \sum_{n \leq x} \left(\frac{d_K}{n}\right) \right| \leq |d_K|.$$

Beweis: Sei

$$S = \sum_{\substack{n \mod |d_K| \\ (n, d_K)=1}} \left(\frac{d_K}{n}\right),$$

wegen Lemma 3.2.5 kann man immer ein n_0 finden, sodass $(n_0, |d_K|) = 1$ und $(d_K/n_0) = -1$ gilt. Betrachtet man nun

$$\left(\frac{d_K}{n_0}\right) S = \sum_{\substack{n \bmod |d_K| \\ (n,d_K)=1}} \left(\frac{d_K}{nn_0}\right),$$

stellt man fest, dass

$$-S = \left(\frac{d_K}{n_0}\right) S = S$$

gilt, da mit n auch nn_0 alle Restklassen $\bmod |d_K|$ durchläuft. Also muss $S = 0$ sein. Definiert man nun v mittels $v|d_K| \leq x < (v+1)|d_K|$, so folgt

$$\sum_{n \leq x} \left(\frac{d_K}{n}\right) = \sum_{|d_K| v \leq n \leq x} \left(\frac{d_K}{n}\right)$$

da

$$\sum_{n < |d_K| v} \left(\frac{d_K}{n}\right) = \sum_{j=1}^{v} \left(\sum_{(j-1)|d_K| < n < j|d_K|} \left(\frac{d_K}{n}\right) \right) = 0$$

weil die innere Summer immer gleich S ist. Somit erhält man

$$\left| \sum_{n \leq x} \left(\frac{d_K}{n}\right) \right| \leq |d_K|.$$

□

Ein für den Beweis der Dirichletschen Klassenzahlformel wichtiger Begriff ist der des Dirichletschen Charakters. Ein Charakter allgemein ist eine multiplikative Abbildung von einer bliebigen abelschen Gruppe in die punktierte komplexe Zahlenebene. Ist diese Gruppe eine prime Restklassengruppe, dann spricht man von einem Dirichletschen Charakter. Ein Beispiel für einen solchen Charakter ist das Kroneckersymbol.

Definition 3.2.4 *Ein **Charakter** f ist ein Homomorphismus einer beliebigen abelschen Gruppe G in die punktierte komplexe Zahlenebene, das heißt:*

$$f : G \longrightarrow \mathbb{C} \setminus 0$$

$$f(ab) = f(a)f(b)$$

Ist $G = G(m)$ die prime Restklassengruppe $\bmod m$*, dann definiert man zu jedem Charakter f von $G(m)$ eine arithmetische Funktion $\chi = \chi_f$ folgendermaßen*

$$\chi(a) = \begin{cases} f(a \bmod m) & \textit{wenn} \quad (a,m) = 1, \\ 0 & \textit{sonst} \end{cases}.$$

Diese Funktion heißt ***Dirichletscher Charakter*** $\bmod m$*.*

Charaktere haben viele interessante Eigenschaften, so gilt zum Beispiel für endliche Gruppen $f(e) = 1$, wenn man mit e das neutrale Element dieser Gruppe bezeichnet. Hieraus folgt auch unmittelbar, dass jeder Wert $f(a)$ eine Einheitswurzel ist. Definiert man die Muliplikation zweier Charaktere fogendermaßen

$$(f_i f_j)(a) = f_i(a) f_j(a),$$

so bildet die Menge der Charaktere einer endlichen abelschen Gruppe ebenfalls eine abelsche Gruppe. Das inverse Element eines Charakters f_i ist sein Reziprokwert $1/f_i$. Mit f ist auch die komplex konjugierte Funktion $\overline{f}$, definiert durch $\overline{f}(a) = \overline{f(a)}$, ein Charakter und es gilt insgesamt

$$\overline{f}(a) = \frac{1}{f(a)} = f(a^{-1}).$$

Jede abelsche Gruppe besitzt zu mindest einen Charakter, nämlich jene Funktion, die auf der gesamten Gruppe identisch 1 ist. Einen Beweis all dieser Eigenschaften findet man zum Beispiel in [1]. Dieser Charakter wird auch Hauptcharakter genannt.

Summen die Charaktere beinhalten, spielen in der Zahlentheorie eine wichtige Rolle, so auch die erstmals von C. F. Gauß behandelten und nach ihm benannten Gaußschen Summen.

Definition 3.2.5 *Sei $m \in \mathbb{N}$ fest gewählt, χ ein Dirichletscher Charakter* $\bmod m$ *und $\zeta_m = e^{2\pi i/m}$ die m-te Einheitswurzel, dann definiert man für ein fixes $a \in \mathbb{Z}$ die* ***Gaußsche Summe*** *$\tau_a(\chi)$ mittels*

$$\tau_a(\chi) = \sum_{r=1}^{m} \chi(r) \zeta_m^{ar} \tag{3.8}$$

Im Falle $a = 1$ soll im weitern $\tau(\chi)$ statt $\tau_1(\chi)$ geschrieben werden.

Der folgende Satz liefert eine notwendige Bedingung dafür, dass $\tau_n(\chi) \neq 0$ gilt, falls $(n, m) > 1$.

Satz 3.2.7 *Sei χ ein Dirichletscher Charakter* $\bmod m$ *und $\tau_n(\chi) \neq 0$ für ein n mit $(n, m) > 1$, dann gibt es einen Teiler d von m, $d < m$, sodass*

$$\chi(a) = 1 \text{ für alle } a \text{ mit } (a, m) = 1 \text{ und } a \equiv 1 \bmod d \tag{3.9}$$

gilt.

Beweis: Für ein festes n sei $q = (n, m)$ und $d = m/q$, dann $d|m$ und da $q > 1$ gilt $d < m$. Wählt man nun ein a mit $(a, m) = 1$ und $a \equiv 1 \mod d$, dann kann man in $\tau_n(\chi)$ den Summationsindex r durch ar ersetzen und erhält

$$\tau_n(\chi) = \sum_{r \bmod m} \chi(r) e^{2\pi i n r/m} = \sum_{r \bmod m} \chi(ar) e^{2\pi i n a r/m} = \chi(a) \sum_{r \bmod m} \chi(r) e^{2\pi i n a r/m}.$$

Da $a \equiv 1 \mod d$ und $d = m/q$ kann man $a = 1 + bm/q$ für ein $b \in \mathbb{N}$ schreiben und es gilt, da $q|n$

$$\frac{anr}{m} = \frac{nr}{m} + \frac{bmnr}{qm} = \frac{nr}{m} + \frac{bnr}{q} \equiv \frac{nr}{m} \mod 1.$$

Hieraus folgt $e^{2\pi i n a r/m} = e^{2\pi i n r/m}$ und somit

$$\tau_n(\chi) = \chi(a) \sum_{r \bmod m} \chi(r) e^{2\pi i n r/m} = \chi(a) \tau_n(\chi).$$

Da $\tau_n(\chi) \neq 0$ bedeutet das $\chi(a) = 1$.

□

In Anlehnung an den letzten Satz lassen sich zwei Begriffe definieren, der des induzierten Modulus und der des primitiven Charakters.

Definition 3.2.6 *Sei χ ein Dirichletscher Charakter* $\bmod m$ *und $d > 0$ ein Teiler von m, dann heißt d ein* ***induzierter Modulus*** *für χ, wenn (3.9) gilt.*

Definition 3.2.7 *Ein Dirichletscher Charakter χ* $\bmod m$ *heißt* ***primitiv****, wenn er keinen induzierten Modulus $d < m$ besitzt.*

Ein Beispiel für einen primitiven Charakter wäre das Legendresymbol, ein anderes, wie das folgende Lemma zeigt, das Kroneckersymbol, für $m > 1$ ist der Hauptcharakter nicht primitiv. Einen Beweis dieser Tatsachen findet man zum Beispiel in [7], [1].

Lemma 3.2.7 *Das Kroneckersymbol ist ein primitiver, reeller Dichrichletsche Charakter.*

Die folgenden beiden Sätze liefern weitere wichtige Eigenschaften Gauß'scher Summen. Interessant ist, dass es verhältnismäßig einfach ist zu zeigen, dass $|\tau(\chi)| = m$ gilt, wohingegen der Beweis von Satz 3.2.9 doch einigen Aufwand benötigt.

Satz 3.2.8 *Sei $(a, m) = 1$ und b eine beliebige ganze Zahl, dann gilt*

$$\tau_{ab}(\chi) = \overline{\chi(a)}\tau_b(\chi).$$

Ist χ ein primitiver Charakter, dann gilt diese Gleichheit für alle $a \in \mathbb{Z}$.

Beweis: Wegen $|\chi(a)|^2 = \chi(a)\overline{\chi}(a) = 1$ gilt

$$\chi(r) = \overline{\chi}(a)\chi(a)\chi(r) = \overline{\chi}(a)\chi(ar),$$

daraus folgt

$$\begin{aligned}\tau_{ab}(\chi) &= \sum_{r \bmod m} \chi(r)\zeta_m^{abr} = \overline{\chi}(a) \sum_{r \bmod m} \chi(ar)\zeta_m^{bar} \\ &= \overline{\chi}(a) \sum_{k \bmod m} \chi(k)\zeta_m^{bk} = \overline{\chi}(a)\tau_b(\chi)\end{aligned}$$

und somit wäre der erste Teil bewiesen. Ist nun χ ein primitiver Dirichletscher Charakter, so ist nach Satz 3.2.7 $\tau_a(\chi) = 0$ für alle a mit $(a, m) > 1$. Da aber in diesem Fall auch $\overline{\chi}(a) = 0$ gilt, stimmt die Aussage.

□

Satz 3.2.9 *Sei χ ein reeller primitiver Charakter* mod m*, dann gilt*

$$\tau(\chi) = \begin{cases} m^{1/2} & \textit{falls} \quad \chi(-1) = 1 \\ im^{1/2} & \textit{falls} \quad \chi(-1) = -1 \end{cases} \tag{3.10}$$

Weitere Charakere beinhaltende Summen sind die sogenannten Dirichletschen L-Reihen $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. Da $|\chi(n)n^{-s}| \leq n^{-s}$ gilt, konvergiert $L(s,\chi)$ im gleichen Bereich wie die Riemannsche ζ-Funktion $\zeta(s)$, das heißt für $s > 1$, und ist dort auch stetig.

Definition 3.2.8 *Unter einer* ***Dirichletschen L-Reihe*** *versteht man eine Reihe der Form*

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

Setzt man für χ das Kronecker Symbol ein, so erhält man

$$L_d(s) = \sum_{n=1}^{\infty} \frac{\left(\frac{d}{n}\right)}{n^s}.$$

Nach diesen Vorbereitungen kann mit dem eigentlichen Beweis der Dirchletschen Klassenzahlformel begonnen werden. Zentrale Bedeutung kommt den Sätzen 3.2.12 und 3.2.13 beziehungsweise 3.2.14 zu, die einen Zusammenhang zwischen dem Volumen einer beschränkten, offenen Menge des $\mathbb{R}^2$ und der Anzahl der Ideale, deren Norm $\leq x$ ist, einer Idealklasse herstellen.

Satz 3.2.10 *Sei (a_m) eine Folge komplexer Zahlen und gelte*

$$A(x) = \sum_{m \leq x} a_m = O(x^{\delta}) \quad \textit{für} \quad \delta \geq 0,$$

dann konvergiert die Summe

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} \quad \textit{für} \quad \Re(s) > \delta$$

und hat in dieser Halbebene die Darstellung

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} = s \int_1^{\infty} \frac{A(x)}{x^{s+1}} dx.$$

Beweis: Zuerst formt man $\sum a_m/m^s$ folgendermaßen um:

$$\begin{aligned}\sum_{m=1}^{M} \frac{a_m}{m^s} &= \sum_{m=1}^{M} \left(A(m) - A(m-1)\right) m^{-s} \\ &= A(M)M^{-s} + \sum_{m=1}^{M-1} A(m)\{m^{-s} - (m+1)^{-s}\}.\end{aligned}$$

Wegen

$$m^{-s} - (m+1)^{-s} = s \int_m^{m+1} \frac{dx}{x^{s+1}}$$

erhält man

$$\sum_{m=1}^{M} \frac{a_m}{m^s} = \frac{A(M)}{M^s} + s \int_1^M \frac{A(x)dx}{x^{s+1}}.$$

Für $\Re(s) > \delta$ gilt

$$\lim_{M\to\infty} \frac{A(M)}{M^s} = 0$$

da $A(x) = O\left(x^{\delta}\right)$. Daraus ergibt sich

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} = s \int_1^{\infty} \frac{A(x)dx}{x^{s+1}}$$

in der Halbebene $\Re(s) > \delta$.

□

Definition 3.2.9 *Eine Abbildung*

$$f : \mathbb{N} = 1, 2, 3, \ldots \longrightarrow \mathbb{C}$$

heißt ***zahlentheoretische Funktion****.*

Satz 3.2.11 *Seien $g(n)$ und $h(n)$ zwei zahlentheoretische Funktionen und*

$$f(n) = \sum_{l|n} g(l)h\left(\frac{n}{l}\right)$$

ihr Dirichletprodukt, weiters seien $G(x)$ und $H(x)$ folgendermaßen definiert:

$$G(x) = \sum_{n\leq x} g(n)$$

$$H(x) = \sum_{n \leq x} h(n)$$

Dann gilt für ein beliebiges $y > 0$

$$\sum_{n \leq x} f(n) = \sum_{l \leq y} g(l) H\left(\frac{x}{l}\right) + \sum_{l \leq \frac{x}{y}} h(l) G\left(\frac{x}{l}\right) - G(y) H\left(\frac{x}{y}\right). \tag{3.11}$$

Beweis:

$$\begin{aligned}
\sum_{n \leq x} f(n) &= \sum_{le \leq x} g(l)h(e) \\
&= \sum_{\substack{le \leq x \\ l \leq y}} g(l)h(e) + \sum_{\substack{le \leq x \\ l > y}} g(l)h(e) \\
&= \sum_{l \leq y} g(l) H\left(\frac{x}{l}\right) + \sum_{e \leq \frac{x}{y}} h(e) \left\{ G\left(\frac{x}{e}\right) - G(y) \right\} \\
&= \sum_{l \leq y} g(l) H\left(\frac{x}{l}\right) + \sum_{e \leq \frac{x}{y}} h(e) G\left(\frac{x}{e}\right) - G(y) H\left(\frac{x}{y}\right)
\end{aligned}$$

□

Lemma 3.2.8 *Sei K ein quadratischer Zahlkörper mit Diskriminante d und a_n die Anzahl der Ideale mit Norm n in O_K, dann gilt:*

$$\sum_{n \leq x} a_n = cx + O(\sqrt{x})$$

mit

$$c = \sum_{l=1}^{\infty} \left(\frac{d}{l}\right) \frac{1}{l}$$

Beweis: Nach Lemma 3.2.4 gilt

$$a_n = \sum_{l | n} \left(\frac{d}{l}\right)$$

und es kann Satz 3.2.11 mit $g(l) = (\frac{d}{l})$, $h(l) = 1$ und $y = \sqrt{x}$ angewendet werden und somit erhält man

$$\sum_{n \leq x} a_n = \sum_{l \leq \sqrt{x}} \left(\frac{d}{l}\right) \left\lfloor \frac{x}{l} \right\rfloor + \sum_{l \leq \sqrt{x}} G\left(\frac{x}{l}\right) - G(\sqrt{x}) \lfloor \sqrt{x} \rfloor.$$

Aus Lemma 3.2.6 folgt $|G(x)| \leq |d|$, setzt man außerdem $\lfloor x/l \rfloor = x/l + O(1)$, so erhält man

$$\sum_{n \leq x} a_n = \sum_{l \leq \sqrt{x}} \left(\frac{d}{l}\right) \frac{x}{l} + O(\sqrt{x}).$$

Schließlich kann man

$$\sum_{l \leq \sqrt{x}} \left(\frac{d}{l}\right) \frac{1}{l} = \sum_{l=1}^{\infty} \left(\frac{d}{l}\right) \frac{1}{l} - \sum_{l > \sqrt{x}} \left(\frac{d}{l}\right) \frac{1}{l}$$

schreiben. Wegen Satz 3.2.10 konvergiert die Reihe

$$\sum_{l=1}^{\infty} \left(\frac{d}{l}\right) \frac{1}{l} = c$$

und außerdem gilt

$$\sum_{l > \sqrt{x}} \left(\frac{d}{l}\right) \frac{1}{l} = O\left(\frac{1}{\sqrt{x}}\right).$$

Insgesamt erhält man also

$$\sum_{n \leq x} a_n = cx + O(\sqrt{x}).$$

□

Satz 3.2.12 *Sei D eine beschränkte, offene Menge im $\mathbb{R}^2$ und $N(x)$ die Anzahl von ganzzahligen Punkten $(u, v) \in \mathbb{Z}^2$ in xD, dann gilt*

$$\lim_{x \to \infty} \frac{N(x)}{x^2} = vol(D) \tag{3.12}$$

Beweis: Ohne Beschränkung der Allgemeinheit kann man D durch einen ganzzahligen Punkt in den ersten Quadranten verschieben. Ein beliebiger ganzzahliger Punkt (u, v) liegt genau dann in xD, wenn $(u/x, v/x)$ in D liegt. Teilt man nun die Ebene parallel zu den Koordinatenachsen in Quadrate mit Seitenlänge $1/x$ und bezeichnet die Anzahl der inneren Quadrate mit I_x und die der Randquadrate mit B_x, so erhält man nach der Definition des Riemannschen Integrals

$$\frac{I_x}{x^2} \leq vol(D) \leq \frac{I_x + B_x}{x^2}$$

und somit

$$\lim_{x\to\infty} \frac{I_x}{x^2} = \lim_{x\to\infty} \frac{I_x + B_x}{x^2} = vol(D).$$

Andererseits gilt für $N(x)$

$$I_x \leq N(x) \leq I_x + B_x$$

und es ergibt sich

$$\lim_{x\to\infty} \frac{N(x)}{x^2} = vol(D).$$

□

Lemma 3.2.9 *Sei K ein algebraischer Zahlkörper, C eine Idealklasse von K und $N(x, C)$ die Anzahl der Ideale $I \neq 0$ in O_K, für die gilt $I \in C$, $N(I) \leq x$, dann folgt für ein Ideal $J \in C^{-1}$, dass $N(x, C)$ die Anzahl der Hauptideale $(\alpha) \neq 0$ mit $\alpha \in J$ und $|N_K(\alpha)| \leq xN(J)$ ist.*

Beweis: Für jedes $I \in C$ gilt $IJ = (\alpha)$, also ist $(\alpha) \subseteq J$ und $N_K(\alpha) = N(I)N(J)$. Ist nun andererseits $\alpha \in J$, so folgt, dass $I = J^{-1}(\alpha)$ ein Ideal mit Norm $\leq x$ ist.

□

Satz 3.2.13 *Sei K ein imaginär quadratischer Zahlkörper, C eine Idealklasse von O_K und d_K die Diskriminante von K, dann gilt*

$$\lim_{x\to\infty} \frac{N(x, C)}{x} = \frac{2\pi}{w\sqrt{|d_K|}} \tag{3.13}$$

wobei w die Anzahl der Einheitswurzeln in K ist.

Beweis: Nach Lemma 3.2.9 ist $wN(x, C)$ die Anzahl von ganzen Zahlen $\alpha \in I$, $I \in C^{-1}$, sodass $0 < |N_K(\alpha)| < x|N(I)|$ gilt. Sei $\{\alpha_1, \alpha_2\}$ eine Basis von I, dann definiert man

$$D = \{(u, v) \in \mathbb{R}^2 : 0 < |u\alpha_1 + v\alpha_2|^2 < 1\}.$$

Es ist unmittelbar klar, dass D beschränkt ist. Betrachtet man nun $\sqrt{x|N(I)|}D$, so stellt sich heraus, dass $wN(x,C)$ genau die Anzahl der ganzzahligen Punkte in dieser Menge ist. Wegen Satz 3.2.12 gilt nun

$$\lim_{x\to\infty} \frac{wN(x,C)}{x|N(I)|} = vol(D),$$

und es bleibt nur noch $vol(D)$ zu berechnen. Sei $u_1 = \Re(u\alpha_1 + v\alpha_2)$ und $u_2 = \Im(u\alpha_1 + v\alpha_2)$ dann folgt

$$\begin{aligned} vol(D) &= \iint\limits_{|u\alpha_1+v\alpha_2|^2<1} dudv \\ &= \frac{2}{N(I)\sqrt{|d_K|}} \iint\limits_{u_1^2+u_2^2<1} du_1du_2 \\ &= \frac{2\pi}{N(I)\sqrt{|d_K|}}. \end{aligned}$$

□

Satz 3.2.14 *Sei K ein reell quadratischer Zahlkörper mit Diskriminante d_K und fundamentaler Einheit ϵ und C eine Idealklasse von O_K, dann gilt*

$$\lim_{x\to\infty} \frac{N(x,C)}{x} = \frac{2\log\epsilon}{\sqrt{|d_K|}} \tag{3.14}$$

Beweis: Sei $I \in C^{-1}$, dann gibt es nach Lemma 3.2.9 $N(x,C)$ Hauptideale (α), $\alpha \in I$ mit $N_K(\alpha) \leq xN(I)$. Da es aber wegen $(\alpha) = (\epsilon^m\alpha)$, $m \in \mathbb{Z}$ unendlich viele Wahlmöglichkeiten für α gibt, muss ihre Anzahl eingeschränkt werden. Da

$$-\frac{\log\left|\frac{\alpha}{\overline{\alpha}}\right|}{2\log\epsilon} \in \mathbb{R}$$

existiert ein ganzzahliges m, sodass

$$m \leq -\frac{\log\left|\frac{\alpha}{\overline{\alpha}}\right|}{2\log\epsilon} < m+1$$

oder äquivalent dazu

$$-2m\log\epsilon \leq \log\left|\frac{\alpha}{\overline{alpha}}\right| < (2m+2)\log\epsilon$$

gilt. Setzt man $w = \epsilon^m \alpha$ erhält man durch Umformen obiger Ungleichung

$$0 \leq \log \left| \frac{w}{|N_K(w)^{1/2}|} \right| < \log \epsilon.$$

Seien w_1 und w_2 zwei assoziierte Elemente aus I, das heißt es gilt $w_1 = \eta w_2$ für eine Einheit η von O_K, die beide obige Ungleichung erfüllen, so erhält man für ihre Differenz

$$0 \leq \log \left| \frac{w_2}{|N_K(w_2)^{1/2}|} \right| - \log \left| \frac{w_1}{|N_K(w_1)^{1/2}|} \right| < \log \epsilon,$$

hieraus ergibt sich

$$0 \leq \log |\eta| < \log \epsilon$$

und somit

$$1 \leq |\eta| < \epsilon.$$

Da ϵ die fundamentale Einheit ist muss deswegen $\eta = \pm 1$ gelten, hieraus folgt, dass die Anzahl der w, für die

$$0 < |N_K(w)| < xN(I)$$

und

$$0 \leq \log \left| \frac{w}{|N_K(w)|^{1/2}} \right| < \log \epsilon$$

gilt, gleich $2N(x, C)$ ist. Daher ist $2N(x, C)$ die Anzahl von Gitterpunkten in $\sqrt{xN(I)}D$ mit

$$D = \left\{ (u, v) \in \mathbb{R}^2 : \begin{array}{c} 0 < |u\beta_1 + v\beta_2||u\overline{\beta}_1 + v\overline{\beta}_2| < 1 \\ 0 < \log \left| \frac{u\beta_1 + v\beta_2}{|u\beta_1 + v\beta_2|^{1/2}|u\overline{\beta}_1 + v\overline{\beta}_2|^{1/2}} \right| < \log \epsilon, \end{array} \right\}$$

wobei $\{\beta_1, \beta_2\}$ eine Ganzheitsbasis von I ist. Es folgt daher mit Satz 3.2.12

$$\lim_{x \leftarrow \infty} \frac{2N(x, C)}{x} = \frac{4 \log \epsilon}{\sqrt{|d_K|}}.$$

□

Lemma 3.2.10 *Sei K ein imaginär quadratischer Zahlkörper und bezeichne h die Klassenzahl von K, dann gilt*

$$\lim_{x \to \infty} \frac{N(x, K)}{x} = \frac{2\pi h}{w\sqrt{|d_K|}} \tag{3.15}$$

Beweis: Sei $H(K)$ die Idealklassengruppe von K, dann gilt

$$N(x,K) = \sum_{C \in H(K)} N(x,C).$$

Diese Summe ist endlich, da die Klassenzahl endlich ist und somit kann man Grenzübergang und Summation vertauschen und erhält

$$\lim_{x\to\infty} \frac{N(x,K)}{x} = \sum_{C\in H(K)} \lim_{x\to\infty} \frac{N(x,C)}{x}.$$

In Satz 3.2.13 wurde

$$\lim_{x\to\infty} \frac{N(x,C)}{x} = \frac{2\pi}{w\sqrt{|d_K|}}$$

gezeigt, woraus unmittelbar (3.15) folgt.

□

Lemma 3.2.11 *Sei K ein reell quadratischer Zahlkörper und bezeichne h die Klassenzahl von K dann gilt*

$$\lim_{x\to\infty} \frac{N(x,K)}{x} = \frac{2h\log\varepsilon}{\sqrt{|d_K|}} \tag{3.16}$$

Beweis: Der Beweis erfolgt analog zum letzten Lemma mit Satz 3.2.14.

□

Satz 3.2.15 (Dirichletsche Klassenzahlformel) *Sei K ein quadratischer Zahlkörper mit Diskriminante $d_K = d$, $\varepsilon(d)$ die Anzal der Einheitswurzeln im Falle $d<0$ beziehungsweise $\varepsilon > 1$ die Fundamentale Einheit in K im Falle $d>0$ und $h(d)$ die Klassenzahl, dann gilt*

$$h(d) = \begin{cases} \frac{\varepsilon(d)|d|^{1/2}}{2\pi} L_d(1) & \text{für } d<0 \\ \frac{d^{1/2}}{2\log\varepsilon} L_d(1) & \text{für } d>0 \end{cases} \tag{3.17}$$

bzw.

$$h(d) = \begin{cases} \frac{\varepsilon(d)}{2d} \sum_{n=1}^{|d|} \left(\frac{d}{n}\right) n & \text{für } d<0 \\ \frac{-1}{log\varepsilon} \sum_{0<n<\frac{d}{2}} \left(\frac{d}{n}\right) log\left(sin\frac{\pi n}{d}\right) & \text{für } d>0 \end{cases} \tag{3.18}$$

Beweis: Zuerst soll (3.17) bewiesen werden. Nach Lemma 3.2.8 ist die Anzahl der Ideale von O_K mit Norm $\leq x$ gleich $cx + O(\sqrt{x})$ mit

$$c = \sum_{n=1}^{\infty} \frac{\left(\frac{d}{n}\right)}{n}.$$

Somit gilt

$$\lim_{x\to\infty} \frac{N(x,K)}{x} = \sum_{n=1}^{\infty} \frac{\left(\frac{d}{n}\right)}{n} = L_d(1)$$

und es muss nur noch dieses Ergebnis in die Formeln (3.15) und (3.16) eingesetzt werden.

□

Der Beweis von (3.18) soll in folgenden Lemmata erfolgen.

Lemma 3.2.12 *Sei χ ein primitiver Charakter* mod$m$*, dann gilt*

$$L(1,\chi) = -\frac{\tau(\chi)}{|m|} \sum_{j=1}^{m} \overline{\chi}(j) \left\{ \log\left(2\sin\frac{\pi j}{m}\right) + \pi i \left(\frac{1}{2} - \frac{j}{|m|}\right)\right\} \tag{3.19}$$

Beweis: Sei für $x \in (-1,1)$ die Funktion

$$f(x) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} x^n$$

definiert, dann gilt

$$\lim_{x\to 1} f(x) = L(1,\chi).$$

Wie man leicht sieht, ist

$$f(x) = \sum_{r=1}^{m} \chi(r) \sum_{n\equiv r \bmod m} \frac{x^n}{n} = \sum_{r=1}^{m} \chi(r) \sum_{n=0}^{\infty} \frac{x^{r+nm}}{r+nm},$$

leitet man nun $f(x)$ ab und summiert die geometrische Reihe, so erhält man

$$f(x) = -\int_0^x \sum_{r=1}^{m} \chi(r) \frac{t^{r-1}}{t^m - 1} dt = -\int_0^x \sum_{j=0}^{m} \frac{a_j}{t - \zeta_m^j} dt$$

wobei $\zeta_m = e^{2\pi i/m}$ und die Koeffizienten $a_0, a_1, \ldots$ fogendermaßen bestimmt werden: Da

$$\sum_{r=1}^{m} \chi(r) t^{r-1} = \sum_{j=0}^{m} a_j \frac{t^m - 1}{t - \zeta_m^j},$$

erhält man, lässt man auf beiden Seiten t gegen ζ_m^k streben,

$$\sum_{r=1}^{m} \chi(r) \zeta_m^{kr-k} = m a_k \zeta_m^{-k}$$

und somit $a_k = m^{-1}\tau_k(\chi)$. Aus der Tatsach, dass

$$\int_0^1 \frac{dt}{t - \zeta_m^j} = \log\left(2 \sin \frac{\pi j}{m}\right) + \pi i \left(\frac{1}{2} - \frac{j}{m}\right)$$

gilt und mit Satz 3.2.8 folgt schließlich

$$L(1, \chi) = -\frac{\tau(\chi)}{|m|} \sum_{j=1}^{m} \overline{\chi}(j) \left\{ \log\left(2 \sin \frac{\pi j}{m}\right) + \pi i \left(\frac{1}{2} - \frac{j}{|m|}\right) \right\}.$$

□

Lemma 3.2.13 *Sei $d = d_K$ Diskriminante eines quadratischen Zahlkörpers und (d/n) das Kroneckersymbol, dann gilt für $d < 0$*

$$L_d(1) = \frac{\pi}{d|d|^{1/2}} \sum_{n=1}^{|d|} n \left(\frac{d}{n}\right)$$

und für $d > 0$

$$L_d(1) = -d^{-1/2} \sum_{n=1}^{d} \left(\frac{d}{n}\right) \log(\sin(\pi n/d)).$$

Beweis: Wegen Lemma 3.2.7 ist (d/n) ein primitiver Charakter $\bmod |d|$. Aus Satz 3.2.9 folgt

$$\tau\left(\frac{d}{n}\right) = \begin{cases} d^{1/2} & \text{für } d > 0 \\ i|d|^{1/2} & \text{für } d < 0 \end{cases},$$

da $L_d(1)$ reell ist und

$$\sum_{j=1}^{d} \left(\frac{d}{j}\right) = 0$$

gilt (siehe dazu Beweis Lemma 3.2.6), folgt nun das gewünschte Ergebnis direkt aus (3.19).

□

Setzt man nun diese Formeln für die L-Reihen in 3.17 ein, so erhält man die zweite Version der Dirichletschen Klassenzahlformel.

3.3 Abelsche Zahlkörper

Quadratische Zahlkörper sind, wie zu Beginn dieses Kapitels bereits gezeigt wurde, ein Spezialfall sogenannter Abelscher Zahlkörper. Wie in der Einleitung bereits erwähnt, lässt sich die Klassenzahlformel auch für solche Zahlkörper formulieren. Der Beweis ist allerdings etwas aufwendiger und soll daher hier entfallen, man kann ihn, wie auch alle anderen Beweise dieses Abschnittes in [6] nachlesen. Obwohl Abelsche Zahlkörper schon einmal definiert wurden, soll das an dieser Stelle der besseren Lesbarkeit wegen wiederholt werden.

Definition 3.3.1 *Ein Erweiterungskörper L/K heißt **Zerfällungskörper** eines Polynoms $f(x) \in K[x]$, falls $f(x)$ über L in Linearfaktoren zerfällt, das heißt*

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n),$$

*und $L = K(\alpha_1, \ldots, \alpha_n)$ gilt. Die Körpererweiterung L/K heißt dann **normal**.*

Definition 3.3.2 *Sei L/K eine endliche Körpererweiterung, ein Element $\alpha \in L$ heißt **separabel**, falls sein Minimalpolynom $m_\alpha(x)$ keine mehrfachen Nullstellen besitzt. Die Erweiterung heißt separabel, wenn jedes $\alpha \in L$ separabel ist. Ein Polynom $f(x)$ heißt separabel, wenn es keine mehrfachen Nullstellen hat.*

Definition 3.3.3 *Eine endliche Erweiterung E/K heißt **Galoisch**, falls E Zerfällungskörper eines separablen Polynoms ist.*

Der folgende Satz liefert eine äquivalente Bedingung zu obiger Definition.

Satz 3.3.1 *Eine Körpererweiterung E/K ist genau dann Galoisch, wenn es eine endliche Gruppe G von Automorphismen auf E gibt, sodass K der Fixpunktkörper von G ist, das heißt $K = \{a \in E | \sigma(a) = a \text{ für alle } \sigma \in G\}$. Außerdem gilt $[E : K] = |G|$.*

Definition 3.3.4 *Die im vorangehenden Satz erwähnte Gruppe G heißt die* ***Galoisgruppe*** *$Gal_{E/K}$ der Galoiserweiterung E/K.*

Definition 3.3.5 *Eine Galoische Erweiterung $K/\mathbb{Q}$ heißt* ***Abelsch****, wenn ihre Galoisgruppe abelsch ist.*

Im Gegensatz zu der Klassenzahlformel für quadratische Zahlkörper, benötigt man für die allgemeinere Formel für Abelsche Zahlkörper weitere Begriffe und Definitionen, wie zum Beispiel Absolutbeträge oder den Regulator eines algebraischen Zahlkörpers.

Definition 3.3.6 *Sei K ein Körper, dann versteht man unter einem Absolutbetrag $\nu(x)$ eine Abbildung von K in die positiven reellen Zahlen, für die folgende Bedingungen erfüllt sein müssen:*

(i) $\nu(x) \geq 0$, $\forall x \in K$ *und* $\nu(x) = 0$ *dann und nur dann, wenn* $x = 0$

(ii) $\nu(xy) = \nu(x)\nu(y)$, $\forall x, y \in K$

(iii) $\nu(x + y) \leq \nu(x) + \nu(y)$, $\forall x, y \in K$.

Statt (iii) kann man auch folgende stärkere Bedingung formulieren:

(iv) $\nu(x + y) \leq \max(\nu(x), \nu(y))$, $\forall x, y \in K$.

Alle Absolutbeträge, die (iv) erfüllen, werden nicht-archimedische, alle übrigen archimedische Absolutbeträge genannt.

Definition 3.3.7 *Ein Absolutbetrag ν heißt diskret, wenn $\nu(K^\times)$ eine diskrete Untergruppe von $\mathbb{R}_+^\times$ ist.*

Definition 3.3.8 *Zwei Absolutbeträge heißen äquivalent, wenn sie die gleichen Topologien induzieren.*

Im folgenden soll die Menge aller archimedischer Absolutbeträge mit S_∞ bezeichnet werden. Der nächste Satz charakterisiert alle Absolutbeträge eines algebraischen Zahlkörpers.

Satz 3.3.2 *Sei K ein algebraischer Zahlkörper, dann ist jeder Absolutbetrag von K entweder diskret oder archimedisch. Ist ν archimedisch, so ist $\nu(x)$ äquivalent zu $|\sigma(x)|$, wobei $\sigma(x)$ eine Konjugierte von x darstellt, umgekehrt definiert jeder konjugierte Körper von K einen archimedischen Absolutbetrag. Zwei Absolutbeträge, die von unterschiedlichen Konjugationen induziert werden, sind genau dann äquivalent, wenn die zugehörigen Abbildungen konjugiert komplex sind.*

Definition 3.3.9 *Sei K ein algebraischer Zahlkörper mit Signatur (s,t) und $u_1,\dots,u_r$, $r=s+t-1$ ein System von Einheiten von K, das keine Einheitswurzeln enthält, dann definiert man den **Regulator** $R(u_1,\dots,u_r)$ mittels*

$$R(u_1,\dots,u_r) = |\det(\log(\nu_j(u_i)))|$$

wobei ν_j über alle Absolutbeträge aus S_∞ außer einem, der beliebig gewählt werden kann, läuft.

Diese Definition des Regulators ist sinnvoll, da jeder algebraische Zahlkörper nach Satz 3.3.2 genau $s+t$ nicht äquivalente archimedische Absolutbeträge besitzt und, wie der folgende Satz zeigt, die Determinante tatsächlich von der Wahl des gestrichenen Absolutbetrages unabhängig ist.

Satz 3.3.3 *(i) $R(u_1,\dots,u_r)$ hängt nicht von der Wahl des gestrichenen Absolutbetrages ab.*

(ii) $R(u_1,\dots,u_r)=0$ wenn die Einheiten $u_1,\dots,u_r$ multiplikativ abhängig sind, das heißt, wenn es $(n_1,\dots,n_r)\neq(0,\dots,0)$ gibt, sodass

$$\prod_{i=1}^{r} u_i^{n_i} = 1$$

gilt.

(iii) Sind $u_1,\dots,u_r$ und $u'_1,\dots,u'_r$ zwei fundamentale Systeme von Einheiten, dann gilt

$$R(u_1,\dots,u_r) = R(u'_1,\dots,u'_r),$$

das heißt man kann eine Konstante $R(K)$ mittels $R(K) = R(u_1, \ldots, u_r)$ definieren, wobei $u_1, \ldots, u_r$ ein fundamentales System von Einheiten bilden.

Bemerkung: Nach dem Dirichletschen Einheitensatz 4.1 gibt es in jedem algebraischen Zahlkörper $r = s + t - 1$ Einheiten $\epsilon_1, \ldots, \epsilon_r \in O_K$, sodass sich alle Einheiten ϵ von O_K mittels

$$\epsilon = \zeta \epsilon_1^{n_1} \cdots \epsilon_r^{n_r}$$

darstellen lassen, wobei ζ eine Einheitswurzel ist und $n_1, \ldots, n_r \in \mathbb{Z}$. Jede solche Menge von Einheiten nennt man fundamentales System von Einheiten.

Definition 3.3.10 *Sei $m \in \mathbb{N}$ und $\zeta_m = e^{2\pi i/m}$ dann heißt $L = \mathbb{Q}(\zeta_m)$* ***m-ter Kreisteilungskörper***

Kreisteilungskörper besitzen viele interessante Eigenschaften, einige davon werden in folgendem Satz genannt.

Satz 3.3.4 *(i) Sei $K_m = \mathbb{Q}(\zeta_m)$ mit $m \geq 1$ ein Kreisteilungskörper und bezeichne $\varphi(m)$ die Eulersche φ-Funktion, dann gilt $[K_m : \mathbb{Q}] = \varphi(m)$,*

$$d_{K_m} = \prod_{p^a | m} d_{K_{p^a}}^{\varphi(mp^{-a})}$$

und $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\varphi(m)-1}$ bilden eine Ganzheitsbasis, darüberhinaus ist K_m ein Abelscher Zahkörper, dessen Galoisgruppe isomorph zu der primen Restklassengruppe $\bmod m$ ist. Der Isomorphismus ist gegeben durch

$$r \mapsto g_r, \ g_r(\zeta_m) = \zeta_m^r.$$

(ii) Ist K ein beliebiger Abelscher Zahlkörper, dann gibt es einen Kreisteilungskörper K_m, sodass $K \subseteq K_m$. Der kleinste Index $f = f(K)$ für den das gilt, heißt der Anführer von K. Bezüglich des oben gegebenen Isomorphismuses entspricht K einer Untergruppe H der primen Restklassengruppe $G(m)$.

Sei $X(K)$ die Gruppe aller Charaktere auf $G(m)$ die auf H identisch eins sind, dann kann man jeden dieser Charaktere zuerst zu einem Dirichletschen Charakter mod m und anschließend zu einem primitiven Charakter erweitern. Liegt χ in $X(K)$ so bezeichnet man den zugehörigen primitiven Dirichletschen Charakter mit χ'. Sind $X(K)$ beziehungsweise $X'(K)$ die Gruppen von Charakteren, die zu den Einbettungen von K in $K_{f(K)}$ beziehungsweise in K_m, $m > f(K)$ gehören, dann gibt es einen Isomorphismus zwischen $X(K)$ und $X'(K)$ der die induzierten primitven Charaktere erhält. Daher kann man $X(K)$ mit $X'(K)$ identifizieren.

Nach diesen Vorbereitungen ist es nun möglich die Klassenzahlformel für Abelsche Zahlkörper zu definieren.

Satz 3.3.5 *Sei K ein Abelscher Zahlkörper mit Signatur (s,t) und $\varepsilon(K)$ die Anzahl der Einheitswurzel in K, dann gilt*

$$h(K) = \frac{\varepsilon(K)|d_K|^{1/2}}{2^{s+t}\pi^t R(K)} \prod_{\substack{\chi \in X(K) \\ \chi \neq 1}} L(1, \chi').$$

3.4 Quadratische Zahlkörper und quadratische Formen

Das erste Teilproblem des Klassenzahlenproblems, das gelöst wurde, war der Fall, dass der zugrundeliegende Körper ein quadratischer Zahlkörper mit negativer Diskriminante, das heißt ein imaginär quadratischer Zahlkörper, ist. Diese Tatsache ist vor allem darauf zurückzuführen, dass in dieser Situation ein Zusammenhang zwischen solchen Zahlkörpern und quadratischen Formen besteht. Ziel dieses Kapitels ist es diese Zusammenhänge näher zu betrachten.

Definition 3.4.1 *Ein Polynom der Form $f(x,y) = ax^2 + bxy + cy^2$ mit $a,b,c \in \mathbb{Z}$ heißt **quadratische Form** und $d(f) = b^2 - 4ac$ ihre **Diskriminante**. Falls $ggT(a,b,c) = 1$ ist, nennt $f(x,y)$ **primitiv**.*

Definition 3.4.2 *Eine quadratische Form heißt positiv definit, falls für alle Paare $(x,y) \neq (0,0)$ $f(x,y) > 0$ gilt.*

Bemerkung: Das ist genau dann der Fall, wenn $a > 0$ und $d(f) < 0$ ist.

Mit Hilfe der folgenden Definition lässt sich auf der Menge der quadratischen Formen eine Äquivalenzrelation erklären. Interessant ist, dass die Determinante für alle Formen einer solchen Äquivalenzklasse gleich ist, wie man leicht nachrechnen kann.

Definition 3.4.3 *Zwei quadratische Formen $f_1(x,y)$ und $f_2(x,y)$ heißen genau dann* äquivalent *wenn es eine Matrix*

$$\mathcal{A} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

mit $A, B, C, D \in \mathbb{Z}$ und $det(\mathcal{A}) = \pm 1$ gibt, sodass

$$f_1(Ax + By, Cx + Dy) = f_2(x, y)$$

gilt

Nun ist es möglich auch für quadratische Formen eine Klassenzahl zu definieren, die nur von der Diskriminante abhängt.

Definition 3.4.4 *Für $d \in \mathbb{Z}$, $d \neq 0$ heißt die Anzahl von Äquivalenzklassen von quadratischen Formen mit $d(f) = d$* Klassenzahl $h(d)$.

Die folgenden zwei Lemmata liefern einige wichtige Eigenschaften quadratischer Formen.

Lemma 3.4.1 *(i) Jede primitive positiv definite quadratische Form ist äquivalent zu einer Form $g(x,y) = ax^2 + bxy + cy^2$ mit*

$$|b| \leq a \leq c$$

(ii) Jede primitive indefinite quadratische Form mit nicht quadratischer Diskriminate ist äquivalent zu einer Form $g(x,y) = ax^2 + bxy + cy^2$ mit

$$|b| \leq |a| \ , \ |b| \leq |c|$$

(iii) Jede primitive indefinite quadratische Form mit einer quadratischen Diskriminante $d = D^2 \neq 0$ ist äquivalent zu einer Form

$$g(x,y) = ax^2 + Dxy \quad mit \quad 0 \leq a \leq D - 1$$

Beweis:

(i) Sei $a = f(x_1, y_1)$ der kleinste, positive von f angenommene Wert mit ganzzahligen Koordinaten und $c = f(x_2, y_2)$ der kleinste von f angenommene Wert mit ganzzahligen Koordinaten, der

$$\det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} = 1$$

erfüllt. Setzt man

$$\mathbf{A} = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix},$$

so gilt

$$\mathbf{A}f = ax^2 + bxy + cy^2 = g(x, y)$$

mit $b \in \mathbb{Z}$. Aus dieser Konstruktion folgt unmittelbar $a \leq c$ und da

$$\det \begin{pmatrix} x_1 & x_2 \pm x_1 \\ y_1 & y_2 \pm y_1 \end{pmatrix} = 1$$

erhält man $g(\pm 1, 1) = f(\pm x_1 + x_2, \pm y_1 + y_2) \geq c$ und somit $a \pm b + c \geq c$ woraus unmittelbar $|b| \leq a$ folgt.

(ii) Angenommen die Form $f(x, y) = dx^2 + exy + fy^2$ erfüllte die Bedingung $|e| \leq |d|$ und $|e| \leq |f|$ nicht selbst, und es gilt $|e| > |d|$, dann ist es möglich, da $(d, f) \neq (0, 0)$ ein ganzzahliges t zu finden, sodass $|2dt + e| \leq |d| < |b|$ gilt. Somit hat die zu f äquivalente Form $\mathcal{A}f$ mit

$$\mathcal{A} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

einen Mittelkoefizienten, dessen Betrag kleiner oder gleich dem ersten Koeffizienten ist. Ist nun ber Betrag des letzten Koeffizienten kleiner als der des mittleren, so kann man das gleiche Verfahren mit der Matrix

$$\mathcal{B} = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

anwenden. Diese Vorgehensweise muss ein Ende finden, da der Mittelkoeffizient der neuen Form immer echt kleiner als der der ursprünglichen ist. In dem Fall, dass $|e| > |f|$ gilt, kann man das gleiche Verfahren mit vertauschten Matrizen anwenden.

(iii) Ist $f(x,y) = Ax^2 + Bxy + Cy^2$ mit $AC \neq 0$, dann gilt

$$\frac{D-B}{2A} = \frac{-2C}{D+B} = \frac{\beta}{\delta},$$

wobei β und δ relativ prim sind. Löst man nun die Gleichung $\alpha\delta - \beta\gamma = 1$ für $\alpha, \gamma \in \mathbb{Z}$ und definiert

$$\mathbf{A} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

so ist $\mathbf{A}f(x,y) = A_1x^2 + Dxy$ mit $A_1 \in \mathbb{Z}$. Wendet man nun auf diese Form die Matrix

$$\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$$

an, erhält man eine Form $A_2x^2 + Dxy$, wobei $A_2 \equiv A_1 \mod D$ gilt. Wählt man nun k so, dass $0 \leq A_2 < D$ gilt, ergibt sich das Gewünschte.

Ist $C = 0$ so gilt $f(x,y) = Ax^2 \pm Dxy$. Im Falle $f(x,y) = Ax^2 - Dxy$ erhält man die äquivalente Form $A_1x^2 + Dxy$ indem man

$$\frac{A}{D} = \frac{\delta}{\beta}$$

mit $(\delta, \beta) = 1$ schreibt und die Gleichung $\alpha\delta - \beta\gamma = 1$ löst, die daraus resultierende Matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

liefert das erwünschte Ergebnis. Falls erforderlich kann man nun noch den letzten Schritt des vorherigen Falles anwenden.

Ist nun $A = 0$ so kann man das Problem auf letzteren Fall mittels Anwendung der Matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

zurückführen.

□

Definition 3.4.5 *Die quadratischen Formen g in 3.4.1 (i)-(iii) werden* ***reduzierte Formen*** *genannt.*

Lemma 3.4.2 *Sei $f(x,y) = ax^2 + bxy + cy^2$ eine positv definite, primitive, reduzierte quadratische Form, dann gilt*

(i) der kleinste positive von f angenommene Wert mit ganzzahligen Koordinaten ist $a = f(1,0)$

(ii) der kleinste von f angenommene Wert mit ganzzahligen Koordinaten (x,y) , $y \neq 0$ ist $c = f(0,1)$

(iii) der kleinste von f angenommene Wert mit ganzzahligen Koordinaten $(x,y) \neq (0,0)$ ist $a - |b| + c$.

Beweis: Da f reduziert ist gilt

$$f(1,0) = a \leq f(0,1) = c \leq a - |b| + c = \begin{cases} f(1,1) & \text{falls} \quad b = 0 \\ f(-\text{sgn}(b),1) & \text{falls} \quad b \neq 0 \end{cases},$$

daher genügt es zu zeigen, dass $f(x,y) \geq a - |b| + c$ für $xy \neq 0$. Sei $|x| \geq |y|$, dann folgt

$$\begin{aligned} f(x,y) &= |x| \left(a|x| + b\frac{x}{|x|}y \right) + cy^2 \\ &\geq |x|(a|x| - |by|) + cy^2 \\ &\geq |x|^2(a - |b|) + cy^2 \\ &\geq a - |b| + c. \end{aligned}$$

Ist $|y| \geq |x|$ so vertauscht man in obiger Umgleichung x mit y und a mit c und erhält ebenfalls das Gewünschte.

□

Wie für die Klassenzahl algebraischer Zahlkörper, gilt auch für die Klassenzahl quadratischer Formen, dass sie immer endlich ist. Der folgende Satz liefert darüberhinaus einige Abschätzungen für die Klassenzahl.

Satz 3.4.1 *Die Klassenzahl $h(d)$ ist endlich für alle $d \neq 0$ und es gilt:*

$$h(d) \leq \frac{2|d|}{3} , \quad d < 0 \tag{3.20}$$

$$h(d) \leq \left(\frac{2}{5} + o(1)\right) d \qquad d > 0 \ , \ d \text{ kein Quadrat} \tag{3.21}$$

$$h(d) = D \qquad d = D^2 \neq 0 \tag{3.22}$$

Beweis: Zuerst soll (3.20) bewiesen werden. Nach Lemma 3.4.1 ist jede positiv definite quadratische Form äquivalent zu einer Form $f(x,y) = ax^2+bxy+cy^2$ mit $|b| \le a \le c$, erfüllt nun ein Tripl $\langle a,b,c\rangle$ diese Bedingung und zusätzlich $b^2 - 4ac = d$, so folgt

$$3a^2 \le 4ac - a^2 \le 4ac - b^2 = |d|.$$

Es gilt also

$$|b| \le a \le \frac{|d|^{1/2}}{3^{1/2}},$$

Zählt man nun alle möglichen Tripel so erhält man maximal $2|d|/3$, da sich c aus a und b ergibt.

Ist d positiv und kein Quadrat und erfüllt das Tripel $\langle a,b,c\rangle$ die Bedingungen $|b| \le |a|$ und $|b| \le |c|$, dann muss ac negativ sein, somit gilt

$$5b^2 \le b^2 + 4|ac| = d$$

und man erhält $|b| \le (d/5)^{1/2}$, außerdem gilt $ac|(b^2-d)/4$ und somit folgt

$$\begin{aligned}
h(d) &\le 2 \sum_{|b|\le (d/5)^{1/2}} \sum_{\substack{a|(d-b^2)/4\\ a\ge 1}} 1 \\
&\le 4 \sum_{0\le b\le (d/5)^{1/2}} \sum_{a|(d-b^2)/4} 1 \\
&\le 4 \sum_{d/5\le a\le d/4} \sum_{\substack{1\le b\le (d/5)^{1/2}\\ b^2\equiv d \quad (a)}} 1 \\
&\le 4 \sum_{d/5\le a\le d/4} 2(a^{-1}(d/5)^{1/2}+1) \\
&\le \frac{2}{5}d + \frac{8}{\sqrt{5}} d^{1/2} \sum_{a\le d} 1/a \\
&\le (2/5 + o(1))\, d
\end{aligned}$$

Um die letzte Behauptung zu beweisen genügt es zu zeigen, dass zwei Formen $f(x,y) = ax^2 + Dxy$ und $g(x,y) = Ax^2 + Dxy$ mit $0 \le a < A \le D-1$ nicht äquivalent sind. Angenommen sie wären äquivalent, gebe es eine Matrix

$$\mathbf{A} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

mit $\det \mathbf{A} = 1$ sodass $g = \mathbf{A}f$ gilt. Vergleicht man in der daraus resultierenden Gleichung die Koeffizienten, so erhält man

$$\beta(a\beta + D\delta) = 0$$

$$2a\alpha\beta + D(\alpha\delta + \beta\gamma) = D.$$

Daraus folgt

$$\begin{aligned} -D\beta &= 2D\alpha\beta\delta - D\alpha\beta\delta - D\beta^2\gamma \\ &= D\beta(\alpha\delta - \beta\gamma) = D\beta. \end{aligned}$$

Es muss also $\beta = 0$ gelten, was zu $\alpha\delta = \pm 1$ beziehungsweise $\alpha = \delta = \pm 1$ führt. Vergleicht man nun die Koeffizienten von x^2 in g und f so erhält man

$$a\alpha^2 + D\alpha\gamma = A$$

Da $\alpha^2 = 1$ gilt, folgt daraus $a \equiv A \mod D$, im Widerspruch zu der Annahme $0 \leq a < A \leq D - 1$.

□

Bevor endgültig ein Zusammenhang zwischen quadratischen Zahlkörpern und quadratischen Formen hergestellt werden kann, benötigt man den Begriff der geometrischen Darstellung eines algebraischen Zahlkörpers. Es wird sich zeigen, dass die geometrische Darstellung eines algebraischen Zahlkörpers ein Gitter bildet

Definition 3.4.6 *Seien $a_1, \ldots, a_m \in \mathbb{R}^n$ linear unabhängige Vektoren über $\mathbb{R}$, dann heißt die davon erzeugte freie abelsche Gruppe $G = G(a_1, \ldots, a_m) = \{\sum_{i=1}^m k_i a_i | k_i \in \mathbb{Z}\}$* ***m-dimensionales Gitter des*** *$\mathbb{R}^n$. Ist $m = n$, so spricht man von einem vollständigen Gitter.*

Definition 3.4.7 *Die Menge $P = \{\sum_{i=1}^n x_i a_i | 0 \leq x_i < 1\}$ heißt* ***Fundamentalparallelepiped*** *der Gitterbasis $a_1, \ldots, a_n$ und das Volumen von P $VolP = |det(a_1, \ldots, a_n)| = d(G)$* ***Gitterkonstante*** *von G.*

Die Gitterkonstante ist wohldefiniert, da es zu je zwei Basen $\{a_1, \ldots, a_m\}$, $\{b_1, \ldots, b_m\}$ eines Gitters eine ganzzahlige Matrix (c_{ij}) mit $b_j = \sum_{j=1}^m c_{ij} a_i$ gibt, für die $\det(c_{ij}) = \pm 1$ gilt und somit die Gitterkonstante von der Wahl der Gitterbasis unabhängig ist.

Definition 3.4.8 *Sei K ein algebraischer Zahlkörper mit Signatur $[s, t]$ und bezeichnen $\sigma_1, \ldots, \sigma_s$ die reellen und $\sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ die komplexen*

Einbettungen von K in $\mathbb{C}$, so kann jedem $\alpha \in K$ ein

$$x(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)) \in \mathbb{R}^s \times \mathbb{C}^t \cong \mathbb{R}^{s+2t} = \mathbb{R}^n \tag{3.23}$$

zugeordnet werden. $x(K)$ bezeichnet man als die ***geometrische Darstellung*** *des Körpers K in $\mathbb{R}^n$.*

Lemma 3.4.3 *Die geometrische Darstellung von O_K bildet ein vollständiges Gitter mit Gitterkonstante $2^{-t}\sqrt{|d_K|}$, wobei d_K die Diskriminante von K bezeichnet.*

Beweis: Sei $a_1, \ldots, a_n$ eine Ganzheitsbasis von O_K, dann sind die Vektoren $x(a_i)$, $i = 1, \ldots, n$ linear unabhängig und die geometrische Darstellung von O_K bildet somit ein vollständiges Gitter. Für die Gitterkonstante gilt mit $A = ((\sigma_1(a_i), \ldots, \sigma_s(a_i), \sigma_{s+1}(a_i), \overline{\sigma_{s+1}(a_i)}, \ldots, \sigma_{s+t}(a_i), \overline{\sigma_{s+t}(a_i)})_{i=1,\ldots,n})$

$$\begin{aligned}\det A &= \det\left(\sigma_1(a_i), \ldots, \sigma_s(a_i), \sigma_{s+1}(a_i), \overline{\sigma_{s+1}(a_i)}, \ldots, \sigma_{s+t}(a_i), \overline{\sigma_{s+t}(a_i)}\right)_{i=1,\ldots,n} \\ &= (-2i)^t d\end{aligned}$$

wobei $|d| = d(G)$ gilt. Somit erhält man

$$d(G) = 2^{-t}\sqrt{|d_K|}$$

.

□

Das folgende Lemma liefert einen Zusammenhang zwischen der geometrischen Darstellung eines Ideals beziehungsweise des Ringes der ganzen Zahlen und der Norm des Ideals.

Lemma 3.4.4 *Sei K ein quadratischer Zahlkörper mit Diskriminante $d < 0$ und Signatur (s, t), I ein Ideal von O_K und G_I bzw. G_{O_K} die von I respektive O_K induzierten geometrischen Darstellungen, dann ist die Norm von I der Quotient der beiden zugehörigen Gitterkonstanten, das heißt*

$$N(I) = \frac{d(G_I)}{d(G_{O_K})}$$

Beweis: Nach Lemma 2.3.5 gilt $d(G_I) = 2^{-t}N(I)\sqrt{|d_K|}$ und nach Lemma 3.4.3 $d(G_{O_K}) = 2^{-t}\sqrt{|d_K|}$, somit folgt

$$\frac{d(G_I)}{d(G_{O_K})} = \frac{2^{-t}N(I)\sqrt{|d_K|}}{2^{-t}\sqrt{|d_K|}} = N(I).$$

□

Lemma 3.4.5 *Sei I ein Ideal von O_K und seien $a_1,\ a_2,\ b_1,\ b_2 \in O_K$, dann gilt $a_1\mathbb{Z} + a_2\mathbb{Z} = b_1\mathbb{Z} + b_2\mathbb{Z}$ genau dann wenn es eine Matrix $A \in \mathbb{Z}^{2\times 2}$ mit $\det A = \pm 1$ gibt, sodass $\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = A \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$.*

Der Beweis des vorgehenden Lemmas folgt unmittelbar durch nachrechnen.

Mit Hilfe des folgenden Satzes kann man zu jedem Ideal eines quadratischen Zahlkörpers eine quadratische Form definieren. Darüber hinaus gilt, dass zwei Ideale genau dann äquivalent sind, wenn die zugehörigen quadratischen Formen äquivalent sind, man erhält somit eine Bijektion zwischen den Idealklassen und den Klassen äquivalenter quadratischer Formen.

Satz 3.4.2 *Sei $d < 0$ die Diskriminante eines imaginär quadratischen Körpers $K = \mathbb{Q}(\sqrt{m})$, für jedes Ideal $I \trianglelefteq O_K$, dargestellt in der From $I = \mathbb{Z}a_1 + \mathbb{Z}a_2$, wobei man o.B.d.A annehmen kann, dass $\Im(a_1\overline{a}_2 - \overline{a}_1a_2) > 0$ ist, stelle man eine quadratische Form*

$$f_{a_1a_2}(x,y) = \frac{1}{N(I)}N_{K/\mathbb{Q}}(a_1x + a_2y) \tag{3.24}$$

auf. Für diese gilt:

(i) $f_{a_1a_2}(x,y)$ ist eine primitive, positiv definite quadratische Form mit ganzzahligen Koeffizienten und Diskriminante d.

(ii) Zwei Ideale $I = \mathbb{Z}a_1 + \mathbb{Z}a_2$ und $J = \mathbb{Z}b_1 + \mathbb{Z}b_2$ sind genau dann in derselben Idealklasse, wenn die quadratischen Formen $f_{a_1a_2}(x,y)$ und $f_{b_1b_2}(x,y)$ äquivalent sind.

(iii) Die Zuordnung $f_{a_1a_2} \mapsto$ (Klasse von $I = \mathbb{Z}a_1 + \mathbb{Z}a_2$) induziert eine Bijektion zwischen der Menge aller Klassen primitiver, positiv definiter quadratischer Formen mit Diskriminante d und der Idealklassengruppe $H(K)$.

Beweis:

(i) Zunächst soll gezeigt werden, dass die quadratische Form in (3.24) ganzzahlige Koeffizienten hat: Mit $N_{K/\mathbb{Q}}(a_1x + a_2y) = (a_1x + a_2y)(\overline{a}_1x + \overline{a}_2y) = N(a_1)x^2 + (a_1\overline{a}_2 + \overline{a}_1a_2)xy + N(a_2)y^2$ erhält man für die Quadratische Form

$$f_{a_1a_2} = \frac{N(a_1)}{N(I)}x^2 + \frac{(a_1\overline{a}_2 + \overline{a}_1a_2)}{N(I)}xy + \frac{N(a_2)}{N(I)}y^2.$$

Zur Vereinfachung soll im folgenden $N(a_1)/N(I) = a$, $N(a_2)/N(I) = c$ und $(a_1\overline{a}_2 + \overline{a}_1a_2)/N(I) = b$ gesetzt werden. Da $a_1 \in I$ folgt, dass das von a_1 erzeugte Ideal in I enthalten ist und somit, dass $I|(a_1)$. Es gibt also ein Ideal $J \triangleleft O_K$, sodass $IJ = (a_1)$ und wegen Lemma 2.2.8(i) gilt $N(a_1) = N(I)N(J)$. Das heißt $N(I)|N(a_1)$, also $a \in \mathbb{Z}$. Analog zeigt man $c \in \mathbb{Z}$.

Um nun $b \in \mathbb{Z}$ zu zeigen betrachtet man zunächst einmal die Diskriminante $d(f_{a_1a_2})$, für diese gilt:

$$d(f_{a_1a_2}) = b^2 - 4ac = \frac{(a_1\overline{a}_2 - \overline{a}_1a_2)^2}{N(I)^2} = \frac{\Delta(a_1, a_2)}{N(I)^2}$$

Wegen Lemma 3.4.4 und Lemma 3.4.3 gilt für die Norm von I

$$N(I) = \frac{d(G_I)}{d(G_{O_K})} = \left|\frac{\frac{1}{2}\begin{vmatrix} a_1 & \overline{a}_1 \\ a_2 & \overline{a}_2 \end{vmatrix}}{\frac{1}{2}\begin{vmatrix} w_1 & \overline{w}_1 \\ w_2 & \overline{w}_2 \end{vmatrix}}\right| = \frac{\sqrt{|\Delta(a_1, a_2)|}}{\sqrt{|\Delta(w_1, w_2)|}}.$$

Setzt man nun dieses Ergebnis in obige Formel für die Diskriminante der quadratischen Form ein, so erhält man

$$d(f_{a_1,a_2}) = \Delta(w_1, w_2) = d_K = d \in \mathbb{Z}.$$

Somit gilt $b^2 - 4ac \in \mathbb{Z}$ und da $a, c \in \mathbb{Z}$ und $b \in \mathbb{Q}$ folgt daraus $b \in \mathbb{Z}$.

Die quadratische Form ist klarerweise positiv definit, da $a > 0$ und $d(f_{a_1,a_2}) < 0$, es bleibt also nun noch zu zeigen, dass sie auch primitiv ist. Angenommen sie wäre es nicht, dann gebe es eine Primzahl p, sodass $p|a,\ p|b,\ p|c$ und somit auch $p^2|d = b^2 - 4ac$ gilt. Da wegen Satz 3.1.1 $d \equiv 1\ (4)$ und quadratfrei oder $d = 4m$ mit $m \equiv 2, 3\ (4)$ und quadratfrei sein muss, kann nur $p = 2$ gelten. Daraus würde

$$m = \frac{d}{4} = d\left(\frac{f_{a_1,a_2}}{2}\right) = \left(\frac{b}{2}\right)^2 - 4\left(\frac{a}{2}\frac{c}{2}\right) \equiv 0, 1 \quad (4)$$

im Widerspruch zu $m \equiv 2, 3\ (4)$.

(ii) Der Beweis der Aussage soll in zwei Schritten erfolgen. Zunächst einmal wird gezeigt werden, dass die Tatsache, dass zwei Ideale in der selben Klasse liegen, impliziert, dass die zugehörigen quadratischen Formen äquivalent sind.

Hat ein Ideal I zwei unterschiedliche Darstellungen, sprich es gibt $a_1,\ a_2 \in O_K$ und $b_1,\ b_2 \in O_K$, sodass $I = \mathbb{Z}a_1 + \mathbb{Z}a_2 = \mathbb{Z}b_1 + \mathbb{Z}b_2$ gilt, so gibt es nach Lemma 3.4.5 eine Matrix A mit $\det A = \pm 1$ und $\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = A \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$. Hat A die Darstellung

$$A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

so gilt $f_{a_1a_2}(ex + gy, fx + hy) = f_{b_1,b_2}(x, y)$, also dass die zugehörigen quadratischen Formen äquivalent sind.

Wie sich leicht nachrechnen lässt gilt $f_{ca_1ca_2} = f_{a_1a_2}$. Da aber zwei Ideale I und J genau dann äquivalent sind, wenn es Elemente $(c, d) \neq (0, 0)$ aus O_K gibt, sodass $cI = dJ$ gilt, folgt daraus unmittelbar, dass auch f_I äquivalent zu f_J ist.

Ist nun $f_{a_1a_2}$ äquivalent zu $f_{b_1b_2}$, so gibt es nach Definition eine Matrix $A \in \mathbb{Z}^{2\times 2}$ mit $\det A = \pm 1$, sodass $f_{b_1b_2}(x, y) = f_{a_1a_2}(A_{11}x+A_{12}y, A_{21}x+A_{22}y)$ gilt. Löst man nun die Gleichung $f_{b_1b_2}(1, Y) = 0$ so erhält man auf der einen Seite $-b_1/b_2$ und $-\overline{b}_1/\overline{b}_2$ und auf der anderen

$$-\frac{a_1A_{11} + a_2A_{21}}{a_1A_{12} + a_2A_{22}} \text{ und } -\frac{\overline{a}_1A_{11} + \overline{a}_2A_{21}}{\overline{a}_1A_{12} + \overline{a}_2A_{22}}.$$

Würde

$$\frac{\overline{b}_1}{\overline{b}_2} = \frac{a_1A_{11} + a_2A_{21}}{a_1A_{12} + a_2A_{22}} = \frac{A_{11}(a_1/a_2) + A_{21}}{A_{12}(a_1/a_2) + A_{22}}$$

gelten, würde $\overline{b}_1/\overline{b}_2$ in der oberen komplexen Halbebene liegen, im Widerspruch zu der Ordnung von b_1, b_2. Also muss

$$\frac{b_1}{b_2} = \frac{a_1A_{11} + a_2A_{21}}{a_1A_{12} + a_2A_{22}}$$

sein und mit einem geeignet gewählten $t \in K$ gilt dann

$$b_1 = t(a_1A_{11} + a_2A_{21}),\ b_2 = t(a_1A_{12} + a_2A_{22}).$$

Aus Lemma 3.4.5 folgt, dass $c_1 = a_1A_{11}+a_2A_{21}$ und $c_2 = a_1A_{12}+a_2A_{22}$ ebenfalls eine Basis, des zu a_1, a_2 gehörigen Ideals bilden. Schreibt man nun $t = U/V$ mit $U, V \in O_K$, so gilt $Vb_i = Uc_i$ $(i = 1, 2)$ und daraus folgt, dass die zu $f_{a_1a_2}$ und $f_{b_1b_2}$ gehörigen Ideale äquivalent sind.

(iii) Um zu zeigen, dass es eine bijektive Abbildung zwischen der Menge der Klassen quadratischer Formen und der Idealklassengruppe gibt, reicht es aus zu zeigen, dass jede quadratische Form mittels $f_{a_1 a_2}$ dargestellt werden kann. Dazu betrachtet man eine beliebige quadratische Form $f(x,y) = Ax^2 + Bxy + Cy^2$ mit $A > 0,\ B > 0,\ B^2 - 4AC = d$ und $A,\ B,\ C \in \mathbb{Z}$. Nun setzt man $a_1 := B - \sqrt{d}$ und $a_2 := 2C$ somit sind a_1 und a_2 Elemente von O_K und man kann ein Ideal I mittels $I := a_1\mathbb{Z} + a_2\mathbb{Z}$ definieren. Zunächst soll gezeigt werden, dass die durch a_1, a_2 definierte Form $f_{a_1 a_2}$ mit der ursprünglichen übereinstimmt. Ähnlich wie in (i) gilt mit Lemma 3.4.4 und Lemma 3.4.3 für die Norm von I

$$N(I) = \frac{\sqrt{\Delta(a_1, a_2)}}{\sqrt{d}} = \frac{|a_1\overline{a}_2 - \overline{a}_1 a_2|}{\sqrt{d}} = \left| \frac{(B - \sqrt{d})2C - (B + \sqrt{d})2C}{\sqrt{d}} \right| = 4C$$

Hiermit kann man leicht $N(a_1)/N(I)$ berechnen:

$$\frac{N(a_1)}{N(I)} = \frac{B^2 - d}{4C} = \frac{4AC}{4C} = A$$

B und C lassen sich analog überprüfen. Nun muss nur noch gezeigt werden, dass das oben definierte I ein Ideal von O_K ist. I ist klarerweise ein Unterring, da $a_1^2 = B^2 - 2B\sqrt{d} + d = 2Ba_1 - 2Aa_2$, $a_2^2 = 2Ca_2$ und $a_1 a_2 = 2Ca_1$ wieder in I liegen. Nun unterscheidet man zwei Fälle: Zuerst soll $d = 4m$ mit $m \equiv 2, 3\ (4)$ sein. Daraus folgt, dass $B \equiv 0\ (2)$ und $O_K = \mathbb{Z} + (\sqrt{d}/2)\mathbb{Z}$ ist. Für ein beliebiges Element $s = e + f\sqrt{d}/2$ aus O_K gilt nun $sa_1 = (e - fB/2)a_1 + Afa_2 \in I$ und $sa_2 = (e + fB/2)a_2 + fCa_1 \in I$. Analog behandelt man den Fall $d \equiv 1\ (4)$.

□

Satz 3.4.3 *Sei $d < 0$ Diskriminante eines imaginär quadratischen Körpers, dann gilt:*

$$h(\mathbb{Q}(\sqrt{d})) = h(d) \tag{3.25}$$

Beweis: Der Satz folgt unmittelbar aus Satz 3.4.2.

□

Der folgende Satz liefert einen weiteren Zusammenhang zwischen quadratischen Formen und quadratischen Zahlkörpern, einen Beweis findet man zum Beispiel in [7].

Satz 3.4.4 *Sei $I = \mathbb{Z}a_1 + \mathbb{Z}a_2$ und X die Idealklasse von $H(K)$, die I enthält, dann gilt*

$$\{f_{a_1a_2}(x,y)|x,y \in \mathbb{Z}\} = \{N(J)|J \in X^{-1}\}$$

und

$$|\{J \in X^{-1}|N(J) = m\}| = \frac{1}{\varepsilon(d)} \sum_{\{x,y|f_{a_1a_2}(x,y)=m\}} 1,$$

wobei

$$\varepsilon(d) = \begin{cases} 6 & \text{für } d = -3 \\ 4 & \text{für } d = -4 \\ 2 & \text{sonst} \end{cases}$$

ist. ($\varepsilon(d)$ ist die Anzahl der Einheitswurzeln in K)

3.5 Imaginär quadratische Zahlkörper

Ziel dieses Kapitels ist es zu zeigen, dass es für imaginär quadratische Zahlkörper, das heißt für solche mit negativer Diskriminante, nur neun Diskriminanten gibt, für die die Klassenzahl eins ist. Der hier geführte Beweis geht auf eine von A. Baker 1966 gefundene Methode zurück, die es prinzipiell erlaubt eine obere Schranke für den Betrag der möglichen zehnten Diskriminante anzugeben. Konkret für das Klassenzahlenproblem umgesetzt wurde dieser Ansatz 1969 von P. Bundschuh und P. Hock, sprich kurz nachdem Stark die Nichtexistenz einer zehnten Diskriminante erstmals bewiesen hatte. Da diese Methode nur eine obere Schranke liefert benötigt man für den vollständigen Beweis noch die von Stark gefundene untere Schranke $|d| \geq 2.2 \cdot 10^7$, die hier nicht gezeigt werden soll.

Satz 3.5.1 *Sei $d_K = d < 0$ Diskriminante eines imaginär quadratischen Zahlkörpers, dann ist die Klassenzahl $h(d) = 1$ dann und nur dann, wenn $d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$.*

Satz 3.5.2 *Sei $d < 0$ Diskriminante eines imaginär quadratischen Zahlkörpers und $h(d) = 1$, dann gilt $|d| \leq 10^{2759}$.*

Beweis: Zunächst benötigt man die folgenden Lemmata.

Lemma 3.5.1 *$-d$ ist stets Potenz einer Primzahl.*

Den Beweis dieses Lemmas findet man zum Beipiel in [7].

Lemma 3.5.2 *Sei $d < 0$ wie oben und $h(d) = 1$, dann gilt entweder $d = -4, -7, -8$ oder $-d$ ist eine Primzahl kongruent zu* 3 mod 8*.*

Beweis: Da $-d$ stets Potenz einer Primzahl ist, kann $-d$ nur $4, 8$ oder eine Primzahl sein. Nach Satz 3.1.1 muss $d \equiv 1\ (4)$ oder $d = 4m, m \equiv 2, 3\ (4)$ sein und es bleiben nur noch die Fälle $-d \equiv 7\ (8)$ und $-d \equiv 3\ (8)$ zu betrachten. Nun soll erstere Möglichkeit für $-d \neq 7$ ausgeschlossen werden.

Für den Fall $-d \equiv 7\ (8)\ ,\ -d \neq 7$, kann man $-d$ durch $8k + 7\ ,\ k \neq 0$ darstellen. Daraus folgt, dass $(1 - d)/4$ eine gerade ganze Zahl $\neq 2$ ist und somit, dass es als Produkt ac geschrieben werden kann, mit $a, c > 1$. Um nun zu einem Widerspruch zu gelangen, betrachtet man die Form $f(x, y) = ax^2 + xy + cy^2$ deren Diskriminante d ist und zeigt, dass sie nicht äquivalent zu $g(x, y) = x^2 + ((1-d)/4)y^2$ ist. Da bei äquivalenten Formen jeder Wert der von $g(x, y)$ angenommen wird, auch von $f(x, y)$ angenommen werden muss, reicht es aus zu bestätigen, dass es kein ganzzahliges Paar (x, y) gibt, sodass $f(x, y) = 1 = g(1, 0)$ ist.

Für ganzzahliges $x \neq 0$ gilt $f(x, 0) = ax^2 \neq 1$, da $a \neq 1$, analog für $x = 0, y \neq 0$. Ist nun $(x, y) \neq (0, 0)$, so erhält man wegen $8a \leq 4ac = 1 - d$ die Ungleichung

$$f(x, y) \geq \frac{-dy^2}{4a} \geq \frac{-2d}{1 - d} > 1.$$

□

Definition 3.5.1 *Die **Gammafunktion** $\Gamma(x)$ wird definiert als*

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt\ ,\ x > 0.$$

*Die **Betafunktion** $B(x)$ wird definiert als*

$$B(x, y) = \int_0^1 t^{x-1}(1 - t)^{y-1} dt.$$

Lemma 3.5.3 *Sei $d < 0$, $|d| > 163$ Diskriminante eines quadratischen Zahlkörpers, $h(d) = 1$ und $p \equiv 1 \bmod 4$ eine Primzahl, die kein Teiler von d ist, weiters sollen $X_p(m) = (m/p)$ das Legendre, $X(n) = (d/n)$ das Kroneckersymbol und $Q(x,y) = x^2 + xy + ((1-d)/4)y^2$ eine quadratische Form mit Diskriminante d bezeichnen, dann gilt für $\Re(s) > 1$*

$$\begin{aligned} &L(s,X_p)L(s,XX_p) \\ &\quad = \zeta(2s)(1-p^{-2s}) + \left(\frac{|d|}{4}\right)^{1/2-s} \\ &\quad \pi^{1/2}p^{-1}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}(p^{2-2s}-1)\zeta(2s-1) + R_p(s) \end{aligned} \tag{3.26}$$

mit

$$R_p(s) = \frac{1}{p}\left(\frac{|d|^{1/2}}{2}\right)^{1-2s}\sum_{m=0}^{p-1} X_p(Q(m,y))\sum_{k\neq 0} e^{\frac{2\pi ik}{p}(m+y/2)}J_2(ky,s)$$

und

$$J_2(N,s) = \int_{-\infty}^{\infty} e^{-\frac{\pi i N|d|^{1/2}u}{p}}(1+u^2)^{-s}du.$$

Beweis: Für $\Re(s) > 1$ konvergiert $L(s,\chi)$ absolut und daher gilt

$$\begin{aligned} L(s,X_p)L(s,XX_p) &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} X_p(n)X(m)X_p(m)(mn)^{-s} \\ &= \sum_{r=1}^{\infty} X_p(r)r^{-s}\sum_{\delta|r} X(\delta). \end{aligned}$$

Wegen $h(d) = 1$ erhält man aus Lemma 3.2.4 und Satz 3.4.4

$$\sum_{\delta|r} X(\delta) = \frac{N_Q(r)}{2},$$

wobei $N_Q(r)$ die Anzahl der Darstellungen von r durch Q bezeichnet. Somit ergibt sich

$$\begin{aligned} L(s,X_p)L(s,XX_p) &= \frac{1}{2}\sum_{r=1}^{\infty} N_Q(r)\frac{X_p(r)}{r^s} \\ &= \frac{1}{2}\sum_{x\neq 0}\frac{X_p(Q(x,0))}{Q(x,0)^s} + \frac{1}{2}\sum_{y\neq 0}\sum_{x=-\infty}^{\infty}\frac{X_p(Q(x,y))}{Q(x,y)^s} \\ &= S_1 + S_2. \end{aligned}$$

Aus dem ersten Summanden erhält man nun den ersten Term in (3.19) mittels

$$\begin{aligned}\frac{1}{2}\sum_{x\neq 0}\frac{X_p(Q(x,0))}{Q(x,0)^s} &= \frac{1}{2}\sum_{x\neq 0}\frac{X_p(x^2)}{x^{2s}}\\ &= \sum_{\substack{n\geq 1\\ p\nmid n}}\frac{1}{n^{2s}}\\ &= \zeta(2s)(1-p^{-2s}).\end{aligned}$$

Betrachtet man jetzt S_2 so erhält man

$$S_2 = \sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty}\frac{X_p(Q(x,y))}{Q(x,y)^s} = \sum_{y=1}^{\infty}\sum_{m=0}^{p-1}X_p(Q(m,y))\sum_{x=-\infty}^{\infty}\frac{1}{Q(px+m,y)^s},$$

mit der Poissonschen Summenformel, siehe etwa [3], ergibt sich

$$\sum_{x=-\infty}^{\infty}Q(px+m,y)^{-s} = \sum_{k=-\infty}^{\infty}\int_{-\infty}^{\infty}Q(pt+m,y)e^{-2\pi ikt}dt$$

und somit gilt insgesamt

$$S_2 = \sum_{y=1}^{\infty}\sum_{m=0}^{p-1}X_p(Q(m,y))\sum_{k=-\infty}^{\infty}\int_{-\infty}^{\infty}Q(pt+m,y)e^{-2\pi ikt}dt.$$

Da $Q(x,y) = (x+y/2)^2 + |d|y^2/4$ erhält man, setzt man im Integral $m + pt + y/2 = |d|^{1/2}yu/2$

$$\begin{aligned}\int_{-\infty}^{\infty}Q(pt+m,y)e^{-2\pi ikt}dt &= \\ &= \frac{|d|^{1/2}y}{2p}\left(\frac{|d|}{4}y^2\right)^{-s}\int_{-\infty}^{\infty}(1+u^2)^{-s}e^{-\frac{2\pi ik}{p}\left(\frac{1}{2}y(|d|^{1/2}u-1)-m\right)}du.\\ &= \frac{(|d|^{1/2}y/2)^{1-2s}}{p}e^{\frac{2\pi ik}{p}\left(m+\frac{y}{2}\right)}\int_{-\infty}^{\infty}e^{-\frac{2\pi i}{p}ky\frac{|d|^{1/2}}{2}u}(1+u^2)^{-s}du\end{aligned}$$

Daher ergibt sich für S_2

$$\begin{aligned}S_2 =& \frac{(|d|^{1/2}/2)^{1-2s}}{p}\sum_{y=1}^{\infty}y^{1-2s}\sum_{m=0}^{p-1}X_p(Q(m,y))\\ &\sum_{k=-\infty}^{\infty}e^{\frac{2\pi ik}{p}\left(m+\frac{y}{2}\right)}\int_{-\infty}^{\infty}e^{-\frac{2\pi i}{p}ky\frac{|d|^{1/2}}{2}u}(1+u^2)^{-s}du\end{aligned}.$$

Setzt man nun $z = ky$ so folgt

$$S_2 = \frac{(|d|^{1/2}/2)^{1-2s}}{p} \sum_{z=-\infty}^{\infty} e^{\frac{2\pi iz}{2p}} \int_{-\infty}^{\infty} e^{-\frac{2\pi i}{p} z \frac{|d|^{1/2}}{2} u} (1+u^2)^{-s} du \sum_{\substack{y|z \\ y>0}} y^{1-2s} \sum_{m=0}^{p-1} X_p(Q(m,y)) e^{\frac{2\pi imz}{py}}.$$

Betrachtet man in S_2 den Term bei $z = 0$ erhält man

$$\frac{(|d|^{1/2}/2)^{1-2s}}{p} \int_{-\infty}^{\infty} \frac{du}{(1+u^2)^s} \sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{p-1} X_p(Q(m,y))$$

und da aus den Eigenschaften der Gamma- und Betafunktion

$$\int_{-\infty}^{\infty} \frac{du}{(1+u^2)^s} = \frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}$$

folgt, gilt für diesen Term

$$\frac{(|d|^{1/2}/2)^{1-2s}}{p} \frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)} \sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{p-1} X_p(Q(m,y)).$$

Um nun (3.26) vollständig zu beweisen, genügt es

$$\sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{p-1} X_p(Q(m,y)) = (p^{2-2s}-1)\zeta(2s-1)$$

zu zeigen, da $R_p(s)$ sämtliche Terme aus S_2 für $k \neq 0$ enthält. Aus Satz 3.2.8, Satz 3.2.9 und den Rechenregeln für das Legendresymbol folgt

$$X_p(Q(m,y)) = p^{-1/2} \sum_{j=1}^{p-1} X_p(j) e^{\frac{2\pi ijQ(m,y)}{p}}$$

somit ist

$$\sum_{m=0}^{p-1} X_p(Q(m,y)) = p^{-1/2} \sum_{j=1}^{p-1} X_p(j) \sum_{m=0}^{p-1} e^{\frac{2\pi ij}{p}\left(m^2+my+\frac{1-d}{4}y^2\right)}.$$

Setzt man nun $M = (p+1)/2$ so gilt

$$Q(m,y) \equiv (m+My)^2 + |d|M^2y^2 \bmod p,$$

daraus erhält man folgende Gleichheit

$$\sum_{m=0}^{p-1} e^{\frac{2\pi ij}{p}\left(m^2+my+\frac{1-d}{4}y^2\right)} = e^{\frac{2\pi ij|d|M^2y^2}{p}} \sum_{n=0}^{p-1} e^{\frac{2\pi ijn^2}{p}}.$$

Mit Satz 3.2.8 und Satz 3.2.9 erhält man für $p \nmid j$

$$\begin{aligned}\sum_{n=0}^{p-1} e^{\frac{2\pi ijn^2}{p}} &= 1 + \sum_{x=1}^{p-1} \left(1 + \left(\frac{x}{p}\right)\right) e^{\frac{2\pi ijx}{p}} \\ &= \sum_{x=1}^{p} \left(\frac{x}{p}\right) e^{\frac{2\pi ijx}{p}} \\ &= \left(\frac{j}{p}\right) p^{1/2}.\end{aligned}$$

Da $p \equiv 1 \ (4)$ gilt nach Satz 3.2.4

$$X_p(j) = \left(\frac{p}{j}\right) = \left(\frac{j}{p}\right)$$

somit folgt

$$\begin{aligned}\sum_{m=0}^{p-1} X_p(Q(m,y)) &= \sum_{j=1}^{p-1} X_p(j) \left(\frac{j}{p}\right) e^{\frac{2\pi i}{p}(|d|M^2y^2)j} \\ &= \sum_{j=1}^{p-1} e^{\frac{2\pi i}{p}(|d|M^2y^2)j} = \begin{cases} p-1 & \text{falls} \quad p|y \\ -1 & \text{falls} \quad p \nmid y \end{cases}.\end{aligned}$$

Schließlich erhält man

$$\begin{aligned}\sum_{y=1}^{\infty} y^{1-2s} \sum_{m=0}^{p-1} X_p(Q(m,y)) &= \sum_{\substack{p|y \\ y>0}} (p-1)y^{1-2s} - \sum_{\substack{p\nmid y \\ y>0}} y^{1-2s} \\ &= \sum_{n=1}^{\infty} p(pn)^{1-2s} - \zeta(2s-1) \\ &= (p^{2-2s}-1)\zeta(2s-1)\end{aligned}.$$

□

Lemma 3.5.4 *Es gelten die Voraussetzungen des vorhergehenden Lemmas, dann folgt für* $|d| \geq 163$ *und* $p \leq 13$

$$|R_p(1)| \leq 23|d|^{-1/2} e^{-\frac{\pi|d|^{1/2}}{p}}.$$

Beweis: Aus der Definition von $R_p(s)$ folgt

$$|R_p(1)| \leq \frac{2}{p|d|^{1/2}} \sum_{y=1}^{\infty} \sum_{m=0}^{p-1} \left| \sum_{k \neq 0} e^{\frac{2\pi i k}{p}\left(m+\frac{y}{2}\right)} J_2(ky,1) \right|.$$

Integriert man die Funktion $e^{iAz}(1+z^2)^{-1}$ über den oberen Rand des Kreises $|z| = R$ im Fall $A > 0$ und über den unteren im Fall $A < 0$, so erhält man für $J_2(ky,1)$

$$J_2(ky,1) = \pi q^{|ky|},$$

wobei q als $q = e^{-\pi |d|^{1/2} p^{-1}} < 1$ definiert wird, hieraus ergibt sich

$$\begin{aligned} |R_p(1)| &\leq \frac{4\pi}{p|d|^{1/2}} \sum_{m=0}^{p-1} \sum_{y=1}^{\infty} \sum_{k=1}^{\infty} q^{ky} = 4\pi |d|^{-1/2} \sum_{y=1}^{\infty} q^y (1-q^y)^{-1} \\ &\leq 4\pi |d|^{-1/2} q (1-q)^{-2}. \end{aligned}$$

Da die Ungleichung

$$(1-q)^{-2} \leq (1 + p\pi^{-1}|d|^{-1/2})^2$$

gilt und $p \leq 13$ und $|d|^{1/2} \geq 12$ sind, erhält man insgesamt

$$R_p(1) \leq 4\pi |d|^{-1/2} \left(1 + \frac{13}{12\pi}\right)^2 q \leq 23 |d|^{-1/2} e^{-\frac{\pi |d|^{1/2}}{p}}.$$

□

Definition 3.5.2 *Unter der Höhe $H(a)$ einer algebraischen Zahl a versteht man das Maximum der Absolutbeträge der Koeffizien des Minimalpolynoms $f(x)$ von a mit ganzzahligen Koeffizienten.*

Satz 3.5.3 (Die Methode von Baker) *Seien $a_1, \ldots, a_n \in \mathbb{Q}$, $a_i > 0$, $i = 1, \ldots, n$,*

$$L(X_1, \ldots, X_n) = X_1 \log a_1 + \cdots + X_n \log a_n$$

und $A_1, \ldots, A_n$ Zahlen mit $A_j \geq 4$ mit

$$H(a_j) \leq A_j \quad \textit{für} \quad j = 1, 2, \ldots, n$$

dann folgt für $x_1, \ldots, x_n$, wenn $|x_i| \leq M$, $i = 1, \ldots, n$ für ein $M \geq 4$ gilt, dass entweder

$$L(x_1, \ldots, x_n) = 0$$

oder

$$|L(x_1,\dots,x_n)| \geq e^{-CD(\log D')(\log M)},$$

wobei C eine Konstante ist, die nur von n abhängt, man könnte zum Beispiel $C = (16n)^{200n}$ wählen, $D = (\log A_1)\cdots(\log A_n)$ und $D' = D/\log A_n$. Sind außerdem die $a_1,\dots,a_n$ und die $x_1,\dots,x_n$ algebraisch, dann folgt etweder

$$L(x_1,\dots,x_n) = 0$$

oder

$$|L(x_1,\dots,x_n)| \geq e^{-C_1 D(\log D)(\log D')(\log M)}$$

wobei D, D' wie oben gewählt werden und $C_1 = (16dn)^{200n}$, wobei d der Grad des von $a_1,\dots,a_n,x_1,\dots,x_n$ erzeugten Feldes ist.

Nun kann Satz 3.5.2 bewiesen werden. Lässt man zunächst in (3.26) s gegen 1 konvergieren, so erhält man

$$L(1,X_p)L(1,XX_p) = \frac{\pi^2}{6}(1-p^{-2}) + 2\pi|d|^{-1/2}\frac{\log p}{p} + R_p(1).$$

Setzt man in dieser Gleichung $p = 5$ und mulitpliziert sie mit $1-13^{-2} = \frac{168}{169}$ und anschließend $p = 13$ und multiplieziert mit $1-5^{-2} = \frac{24}{25}$, so erhält man nach Subtraktion der beiden enstandenen Gleichungen

$$\begin{aligned}\frac{168}{169}L(1,X_5)L(1,XX_5) - \frac{24}{25}L(1,X_13)L(1,XX_13)\\ + 2\pi|d|^{-1/2}\left(\frac{168}{845}\log 5 - \frac{24}{325}\log 13\right) = \frac{168}{169}R_5(1) - \frac{24}{25}R_{13}(1)\end{aligned}.$$

Unter der Verwendung von Lemma 3.2.13 erhält man nach kurzer Rechnung

$$L(1,X_5) = \frac{\log \alpha^2}{\sqrt{5}} \quad \text{mit} \quad \alpha = \frac{1+\sqrt{5}}{2}$$

und

$$L(1,X_{13}) = \frac{\log \beta^2}{\sqrt{13}} \quad \text{mit} \quad \beta = \frac{3+\sqrt{13}}{2}.$$

Aus der Dirichletschen Klassenzahlformel folgt

$$L(1,XX_5) = \frac{h(5d)\pi}{\sqrt{5|d|}}$$

und

$$L(1, XX_13) = \frac{h(13d)\pi}{\sqrt{13|d|}},$$

es resultiert also insgesamt

$$\begin{aligned} &840h(5d)\log\alpha - 312h(13d)\log\beta + 1680\log 5 - 624\log 13 \\ &= \frac{\sqrt{|d|}}{\pi}(4200R_5(1) - 4056R_{13}(1)). \end{aligned}$$

Wegen Satz 3.4.1 gelten die Ungleichungen

$$h(5d) \leq \frac{10|d|}{3}$$

und

$$h(13d) \leq \frac{26|d|}{3}$$

und man kann die linke Seite der letzten Gleichung in der Form

$$L = x_1\log\alpha + x_2\log\beta + \log a$$

schreiben, wobei $x_i \leq 2800|d|$, $i = 1, 2$ und $a = 5^{1680}13^{-624}$ gilt. Der Grad des von α, β und a erzeugten Körpers beträgt 4, $H(\alpha) = 1$, $H(\beta) = 3$ und $H(a) = \max(5^{1680}, 13^{624}) \leq e^{2704}$. Außerdem ist $L \neq 0$, da sonst

$$\alpha^{x_1}\beta^{x_2}a = 1$$

gelten würde, was jedoch unmöglich ist, da sonst β^{x_2} in dem Körper $\mathbb{Q}(\sqrt{2})$ liegen müßte. Man kann also Satz 3.5.3 mit $A_1 = A_2 = 4$, $A_3 = e^{2704}$, $C_1 = 192^{600} \leq e^{3155}$, $M = 2800|d|$, $D = \log^2 4 \cdot 2704 < 5197$ und $D' = \log^2 4 < 2$ anwenden und erhält für $|d| > 10^{2500}$

$$|L| \geq e^{-e^{3167}\log|d|}.$$

Andererseits liefert Lemma 3.5.4 die Abschätzung

$$\begin{aligned} |L| &\leq \sqrt{|d|}\frac{4225}{\pi}\left(\frac{23}{\sqrt{|d|}}e^{\frac{-\pi\sqrt{|d|}}{\sqrt{5}}} + \frac{23}{\sqrt{|d|}}e^{\frac{-\pi\sqrt{|d|}}{\sqrt{13}}}\right) \\ &\leq e^{12-\frac{\pi\sqrt{|d|}}{\sqrt{13}}} \end{aligned}$$

und somit

$$e^{3167}\log|d| \geq \frac{\pi}{\sqrt{13}}\sqrt{|d|} - 12 \geq 0.87\sqrt{|d|}$$

woraus $|d| \leq e^{6352} < 10^{2759}$ folgt.

□

4 Berechnung der Fundamentaleneinheit in Quadratischen Zahlkörpern

Wie das letzte Kapitel gezeigt hat, ist das Klassenzahlproblem für quadratische Zahlkörper mit negativer Diskriminante gelöst. Besitzt der Zahlkörper jedoch eine positive Diskriminante gestaltet sich die Lage schwieriger, da in diesem Fall die Klassenzahl nicht von der Anzahl der Einheiten, sondern von der fundamentalen Einheit abhängt. Ziel dieses Kapitels ist es daher einfache Algorithmen zu entwickeln, die ihre Berechnung ermöglichen.

Der folgende Satz liefert eine Charakterisierung der Einheitengruppe eines algebraischen Zahlkörpers.

Satz 4.1 (Dirichletscher Einheitensatz) *Sei U_K die Einheitengruppe und $n = r_1 + 2r_2$ der Erweiterungsgrad von K, wobei r_1 beziehungsweise r_2 die Anzahl der reellen beziehungsweise komplexen Einbettungen von K in $\mathbb{C}$ sind, dann existieren fundamentale Einheiten $\epsilon_1, \ldots, \epsilon_r$ mit $r = r_1 + r_2 - 1$, sodass jedes $\epsilon \in U_K$ mittels*

$$\epsilon = \zeta \epsilon_1^{n_1} \cdots \epsilon_r^{n_r}$$

dargestellt werden kann, wobei $n_1, \ldots, n_r \in \mathbb{Z}$ und ζ eine Einheitswurzel in O_K ist, oder anders formuliert, ist W_K die aus den Einheitswurzeln bestehende Untergruppe von U_K, dann gilt

$$U_K \simeq W_K \times \mathbb{Z}^r.$$

Folgerung 4.0.1 *Sei $K = \mathbb{Q}(\sqrt{d})$ ein reell quadratischer Zahlkörper, dann gilt $U_K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, das heißt es gibt eine fundamentale Einheit $\epsilon \in U_K$, sodass $U_K = \{\pm\epsilon^k : k \in \mathbb{Z}\}$.*

*Beweis:*Da $K \subseteq \mathbb{R}$ sind $\{\pm 1\}$ die einzigen Einheitswurzeln in K, das heißt $W_K = \{\pm 1\}$. Da es $r_1 = 2$ reelle und $2r_2 = 0$ complexe Einbettungen von K in $\mathbb{C}$ gibt, folgt somit aus dem Dirichletschen Einheitensatz, dass $U_K \simeq W_K \times \mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Da mit ϵ auch $-\epsilon, \epsilon^{-1}$ und $-\epsilon^{-1}$ fundamentale Einheiten sind, setzt man $\epsilon > 1$ fest und spricht fortan von der fundamentalen Einheit.

Mit Hilfe dieser Darstellung der Einheitengruppe eines algebraischen Zahlkörpers ist es leicht das folgende Lemma zu beweisen, das besagt, dass die sogenannte Pellsche Gleichung unendlich viele Lösungen besitzt. Ein interessantes historisches Detail zu dieser Gleichung ist, dass sie ihren Namen vielleicht zu unrecht erhalten hat. Manche Historiker bezweifeln, dass Pell einen wesentlichen Beitrag zu ihrer Lösung lieferte. Fest steht jedenfalls, dass erst Lagrange die vollständige Lösung des Problems gelang.

Lemma 4.1 *Die Gleichung*

$$x^2 - dy^2 = 1$$

[Pellsche Gleichung] hat für $d \equiv 2, 3 \mod 4$ *unendlich viele ganzzahlige Lösungen und die Gleichung*

$$x^2 - dy^2 = 4$$

hat für $d \equiv 1 \mod 4$ *unendlich viele ganzzahlige Lösungen.*

*Beweis:*Sei $d \equiv 2, 3 \mod 4$, dann gilt $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Ist $\alpha = a + b\sqrt{d} \in U_K^2$, dann folgt

$$N_K(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 = 1,$$

das heißt jedes $\alpha = a + b\sqrt{d} \in U_K^2$ lieferte eine Lösung $(a, b) \in \mathbb{Z}^2$ der Gleichung $x^2 - dy^2 = 1$ und da $U_K^2 \simeq \mathbb{Z}$ gibt es unendlich viele solcher Lösungen.

Ist nun $d \equiv 1 \mod 4$, dann gilt

$$O_K = \left\{ \frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z},\ a \equiv b \mod 2 \right\}.$$

Da $N_K(\alpha) = (a^2 - db^2)/4$ für $\alpha = (a + b\sqrt{d})/2 \in U_K^2$ folgt $a^2 - db^2 = 4$ für unendlich viele Paare $(a, b) \in \mathbb{Z}^2$.

Der folgende Satz liefert prinzipiell die Möglichkeit die fundamentale Einheit eines algebraischen Zahlkörpers zu berechnen. Dieser Ansatz ist jedoch nicht sehr praktikabel, da es das Problem auf das finden einer kleinsten positiven ganzen Zahl b, sodass $db^2 \pm 1$ beziehungsweise $db^2 \pm 4$ ein Quadrat ist, zurückführt.

Satz 4.2 *(i) Sei $d \equiv 2,3 \mod 4$ und b die kleinste, positive ganze Zahl, sodass $db^2 \pm 1$ ein Quadrat ist, dann folgt, wenn $db^2 \pm 1 = a^2$ mit $a > 0$, dass $a + b\sqrt{d}$ die fundamentale Einheit von $\mathbb{Q}(\sqrt{d})$ ist.*

(ii) Sei $d \equiv 1 \mod 4$ und b die kleinste, positive ganze Zahl, sodass $db^2 \pm 4$ ein Quadrat ist, dann folgt, wenn $db^2 \pm 4 = a^2$ mit $a > 0$, dass $(a + b\sqrt{d})/2$ die fundamentale Einheit von $\mathbb{Q}(\sqrt{d})$ ist.

Beweis:

(i) Da $db^2 \pm 1 = a^2$ gilt $N_K(a + b\sqrt{d}) = \pm 1$ und somit $a + b\sqrt{d} \in U_K$. Außerdem folgt aus $a, b > 0$, dass $a + b\sqrt{d} > 1$ und daher $a + b\sqrt{d} = \epsilon^k$ mit $k \geq 1$, wobei ϵ die fundamentale Einheit von $\mathbb{Q}(\sqrt{d})$ darstellt. Ist nun $k > 1$ so schreibt man $\epsilon = \alpha + \beta\sqrt{d}$ mit $\alpha, \beta > 0$ und erhält $a + b\sqrt{d} = (\alpha + \beta\sqrt{d})^k$, woraus $\alpha < a$ und $\beta < b$ folgt. Es gilt aber auch $d\beta^2 \pm 1 = \alpha^2$, im Widerspruch zur Minimalität von b, daher muss $a + b\sqrt{d}$ die fundamentale Einheit sein.

(ii) Der Beweis erfolg analog zu (i)

Eine weit effizientere Methode zur Berechnung der fundamentalen Einheit eines quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{d})$ lässt sich mittels Kettenbruchentwicklungen von $\sqrt{d}$ ermitteln.

Definition 4.1 *1. Unter einem endlichen Kettenbruch versteht man einen Ausdruck der Form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}$$

mit $a_0, \ldots, a_n \in \mathbb{R}$ und $a_i \geq 0$ für $1 \leq i \leq n$. Zur Vereinfachung wird im folgenden die Notation $[a_0, \ldots, a_n]$ für den obigen Ausdruck verwendet.

2. Liegen $a_0, \ldots, a_n$ in $\mathbb{Z}$ so nennt man $[a_0, \ldots, a_n]$ einen einfachen Kettenbruch.

3. Der Kettenbruch $C_k = [a_0, \ldots, a_k]$, $0 \leq k \leq n$ wird als der k-te Näherungsbruch von $[a_0, \ldots, a_n]$ bezeichnet.

Offensichtlich representiert jeder einfache, endliche Kettenbruch eine rationale Zahl, umgekehrt kann man mittels des Euklidschen Algorithmus zeigen, dass sich jede rationale Zahl als einfacher, endlicher Kettenbruch entwickeln lässt.

Die folgenden Lemmata liefern einige Eigenschaften von Kettenbrüchen.

Lemma 4.2 *Sei $[a_0, a_1, \ldots, a_n]$ ein Kettenbruch, definiert man $p_0, \ldots, p_n$ und $q_0, \ldots, q_n$ folgendermaßen rekursiv*

$$\begin{aligned} p_0 &= a_0 \\ p_1 &= a_0 a_1 + 1 \\ p_k &= a_k p_{k-1} + p_{k-2} \end{aligned}$$

und

$$\begin{aligned} q_0 &= 1 \\ q_1 &= a_1 \\ q_k &= a_k q_{k-1} + q_{k-2}, \end{aligned}$$

dann ist $C_k = p_k/q_k$ der k-te Näherungsbruch.

Beweis: Der Beweis erfolgt mittels Induktion nach k: Für $k = 0$ gilt

$$C_0 = [a_0] = \frac{p_0}{q_0}$$

und für $k = 1$

$$C_1 = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

Sei nun die Aussage für $k = n$ bewiesen, dann folgt für $k = n + 1$

$$\begin{aligned} C_{n+1} &= [a_0, \ldots, a_{n+1}] \\ &= \left[a_0, \ldots, a_n + \frac{1}{a_{n+1}}\right] \\ &= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \\ &= \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n p_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}. \end{aligned}$$

Lemma 4.3 *Sei $[a_0, a_1, \ldots, a_n]$ ein Kettenbruch und $C_k = p_k/q_k$ sein k-ter Näherungsbruch, dann gelten folgende Eigenschaften.*

(i)
$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1} \quad \textit{für} \quad k \geq 1$$

(ii)
$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}} \quad \textit{für} \quad 1 \leq k \leq n$$

(iii)
$$C_k - C_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-2}} \quad \textit{für} \quad 2 \leq k \leq n$$

(iv)
$$C_1 > C_3 > C_5 > \cdots$$
$$C_0 < C_2 < C_4 < \cdots$$

(v) Jeder ungerade Näherungsbruch C_{2j+1}, $j \geq 0$ ist größer als jeder gerade Näherungsbruch C_{2k}, $k \geq 0$.

Beweis:

(i) Der Beweis erfolgt mittels Induktion nach k. Zunächst gilt für $k = 1$

$$p_1 q_0 - p_0 q_1 = a_0 a_1 + 1 - a_0 a_1 = 1$$

sei nun die Aussage bereist für $k = n$ bewiesen, dann folgt für $k = n+1$

$$\begin{aligned} p_{n+1} q_n - p_n q_{n+1} &= (a_{n+1} p_n + p_{n-1}) q_n - p_n (a_{n+1} q_n + q_{n-1}) \\ &= p_{n-1} q_n - p_n q_{n-1} \\ &= -(-1)^{n-1} = (-1)^n \end{aligned} \quad .$$

(ii) Nach (i) gilt
$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1},$$
dividiert man nun diese Gleichung durch $q_k q_{k-1}$ so erhält man das gewünschte Ergebnis.

(iii)
$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}}$$

Da aber

$$\begin{aligned} p_k q_{k-2} - p_{k-2} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2}) \\ &= a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) = a_k (-1)^{k-2} \end{aligned}$$

gilt, folgt das Gewünschte.

(iv) Wegen (iii) gilt
$$C_k - C_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-2}},$$
somit ist $C_k < C_{k-2}$ für k ungerade und $C_k > C_{k-2}$ für k gerade.

(v) Wegen (ii) gilt
$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m} q_{2m-1}} < 0,$$
daraus folgt
$$C_{2m-1} > C_{2m}$$
und somit gilt mit (iv)
$$C_{2k} < C_{2(j+k+1)} < C_{2(j+k)+1} < C_{2j+1}.$$

Lemma 4.4 *Sei $\{a_i\}_{i \geq 0}$ eine Folge ganzer Zahlen mit $a_i \geq 0$ für $i \geq 1$ und sei $C_k = [a_0, \ldots, a_k]$, dann konvergiert die Folge $\{C_k\}$.*

Beweis: Nach Lemma 4.3 (iv) gilt
$$C_1 > C_3 > C_5 > \cdots$$
und außerdem ist $C_{2j+1} > a_0$ somit ist die $\{C_{2j+1}\}_{j \geq 0}$ fallend und nach unten beschränkt und somit konvergent gegen ein α_1. Andererseits gilt
$$C_0 < C_2 < C_4 < \cdots$$
und $C_{2j} < C_{2k+1}$ für jedes $k \geq 0$ und jedes $j \geq 0$, somit im speziellen $C_{2j} < C_1$ für alle j. Es ist also die Folge $\{C_{2j}\} j \geq 0$ wachsend und nach oben beschränkt und daher konvergent gegen ein α_2.

Nun muß nur noch $\alpha_1 = \alpha_2$ gezeigt werden. Da $a_i \geq 1$, $q_0, q_1 \geq 1$ läßt sich leicht mittels Induktion nach k zeigen, dass

$$q_k = a_k q_{k-1} + q_{k-1} \geq 2k - 3$$

gilt. Mit dieser Tatsach und Lemma 4.3 (ii) folgt

$$C_{2j+1} - C_{2j} = \frac{1}{q_{2j+1} q_{2j}} \leq \frac{1}{(4j-1)(4j-3)} \to 0 \quad \text{für} \quad j \to \infty.$$

Daher konvergieren beide Folgen gegen den selben Grenzwert $\alpha = \alpha_1 = \alpha_2$ und es gilt insgesamt

$$\lim_{j \to \infty} C_j = \alpha.$$

Bisher wurde gezeigt, dass sich jede rationale Zahl als Kettenbruch entwickeln lässt, das folgende Lemma zeigt, dass es auch für jede irrationale Zahl eine Darstellung mittels Kettenbruch gibt.

Lemma 4.5 *Sei $\alpha = \alpha_0 > 0$ eine irrationale Zahl und definiert man die Folge $\{a_i\}_{i \geq 0}$ folgendermaße rekursiv*

$$a_k = [\alpha_k], \qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k},$$

dann ist $[a_0, a_1, \ldots]$ eine Darstellung von α als einfacher Kettenbruch.

Beweis: Wie man leicht mittels Induktion nachweisen kann, ist jedes α_k irrational, somit ist $\alpha_{k+1} > 1$ und daher $a_{k+1} \geq 1$, daraus folgt, dass $[a_0, a_1, \ldots]$ ein einfacher Kettenbruch ist. Außerdem gilt

$$\begin{aligned} \alpha = \alpha_0 &= [\alpha_0] + (\alpha_0 - [\alpha_0]) = a_0 + \frac{1}{\alpha_1} \\ &= [a_0, \alpha_1] = [a_0, a_1, \alpha_2] = \cdots = [a_0, a_1, \ldots, a_k, \alpha_{k+1}] \end{aligned}$$

für alle k. Wegen Lemma 4.2 erhält man

$$\alpha = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}$$

sodass

$$\begin{aligned}|\alpha - C_k| &= \left|\frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k}\right| \\ &= \left|\frac{-(p_kq_{k-1} - p_{k-1}q_k)}{(\alpha_{k+1}q_k + q_{k-1})q_k}\right| \\ &= \left|\frac{1}{(\alpha_{k+1}q_k + q_{k-1})q_k}\right| \\ &< \frac{1}{q_k^2} \leq \frac{1}{(2k-3)^2} \to 0\end{aligned}$$

für $k \to \infty$ und somit folgt

$$\alpha = \lim_{k\to\infty} C_k = [a_0, a_1, \ldots].$$

Es besitzt also jede irrationale Zahl eine Darstellung als einfacher Kettenbrch und, wie sich leicht zeigen lässt, ist diese auch eindeutig. Somit kann jede reelle Zahl durch einen einfachen Kettenbruch ausgedrück werden, daher wird im Folgenden das Wort einfach weggelassen werden und nur noch von der Kettenbruchentwicklung beziehungsweise dem Kettenbruch einer reellen Zahl gesprochen werden.

Der folgende Satz beschreibt einige Eigenschaften von Kettenbrüche irrationaler Zahlen.

Satz 4.3 *(i) Sei α eine irrationale Zahl und seien $C_j = p_j/q_j$, $j \in \mathbb{N}$ die Näherungsbrüche der Kettenbruchentwicklung von α, gibt es zwei ganze Zahlen r und s mit $s > 0$ und eine positive ganze Zahl k sodass*

$$|s\alpha - r| < |q_k\alpha - p_k|$$

gilt, dann folgt $s \geq q_{k+1}$.

(ii) Sei α eine irrationale Zahl und r/s mit $(r, s) = 1$, $s > 0$ eine rationale Zahl, sodass

$$|\alpha - r/s| < \frac{1}{2s^2}$$

gilt, dann ist r/s ein Näherungsbruch der Kettenbruchentwicklung von α.

Beweis:

(i) Angenommen es gelte $1 \leq s < q_{k+1}$:
Für jedes $k \geq 0$ betrachtet man das lineare Gleichungssystem

$$\begin{aligned} p_k x + p_{k+1} y &= r \\ q_k x + q_{k+1} y &= s, \end{aligned}$$

mittels Gaußelimination ergibt sich

$$\begin{aligned} (p_{k+1}q_k - p_k q_{k+1})y &= rq_k - sp_k \\ (p_k q_{k+1} - p_{k+1}q_k)x &= rq_{k+1} - sp_{k+1}. \end{aligned}$$

Nach Lemma 4.3 (i) gilt $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$ und somit ergibt sich als einzige Lösung zu dem obigen Gleichungssystem

$$\begin{aligned} x &= (-1)^k(sp_{k+1} - rq_{k+1}) \\ y &= (-1)^k(rq_k - sp_k). \end{aligned}$$

Ziel ist es nun zu zeigen, dass x und y beide ungleich Null sind und entgegengesetztes Vorzeichen haben.

Angenommen $x = 0$, dann folgt

$$\frac{r}{s} = \frac{p_{k+1}}{q_{k+1}}$$

und da wegen Lemma 4.3 (i) $(p_{k+1}, q_{k+1}) = 1$ gilt, muß $q_{k+1}|s$ und somit $q_{k+1} \leq s$ im Widerspruch zu der Annahme $1 \leq s < q_{k+1}$.

Sei nun $y = 0$, dann ist $r = p_k x$ und $s = q_k x$. Daraus folgt

$$|s\alpha - r| = |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|$$

im Widerspruch zur Annahme.

Ist nun $y < 0$, so folgt, da $q_k x = s - q_{k+1}y$ und $q_j \geq 0$ für alle $j \geq 0$, $x > 0$, ist andererseits $y > 0$, dann gilt wegen $q_{k+1}y \geq q_{k+1} > s$, $q_k x = s - q_{k+1}y < 0$ und somit $x < 0$.

Aus Lemma 4.3 folgt, dass für gerades k

$$\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$$

und für ungerades k

$$\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k}$$

gilt. In beiden Fällen haben $q_k\alpha - p_k$ und $q_{k+1}\alpha - p_{k+1}$ unterschiedliche Vorzeichen und somit ist das Vorzeichen von $x(q_k\alpha - p_k)$ und $y(q_{k+1}\alpha - p_{k+1})$ gleich. Insgesamt folgt

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1}y)\alpha - (p_k x + p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| \\ &\geq |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &\geq |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k| \end{aligned}$$

wiederum im Widerspruch zur Annahme.

(ii) Angenommen r/s ist kein Näherungsbruch der Kettenbruchentwicklung von α, das heißt es gibt kein n, sodass $r/s = p_n/q_n$ gilt. Sei nun k die größte nichtnegative ganze Zahl mit $s \geq q_k$, ein solches k muß es geben, da $s \geq q_0 = 1$ und $q_k \to \infty$ für $k \to \infty$, dann gilt $q_k \leq s \leq q_{k+1}$ und wegen (i) folgt daraus

$$|q_k\alpha - p_k| \leq |s\alpha - r| = s|\alpha - r/s| < \frac{1}{2s}$$

und somit

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}.$$

Da $r/s \neq p_k/q_k$, folgt $|sp_k - rq_k| \geq 1$. Daraus erhält man

$$\begin{aligned} \frac{1}{sq_k} &\leq \frac{|sp_k - rq_k|}{sq_k} \\ &= \left|\frac{p_k}{q_k} - \frac{r}{s}\right| \\ &= \left|\frac{p_k}{q_k} - \frac{r}{s} + \alpha - \alpha\right| \\ &\leq \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{r}{s}\right| \\ &< \frac{1}{2sq_k} + \frac{1}{2s^2} \end{aligned}$$

und das impliziert

$$\frac{1}{2sq_k} < \frac{1}{2s^2}$$

und somit $q_k > s$ im Widerspruch zur Annahme.

Lemma 4.6 *Sei d eine positive ganze Zahl, kein perfekts Quadrat, dann ist x/y, $x, y > 0 \in \mathbb{Z}$ ein Näherungsbruch der Kettenbruchentwicklung von $\sqrt{d}$, wenn $|x^2 - dy^2| < \sqrt{d}$ gilt.*

Beweis: Angenommen $0 < x^2 - dy^2 < \sqrt{d}$, dann folgt

$$(x + y\sqrt{d})(x - y\sqrt{d}) > 0$$

und somit

$$x > y\sqrt{d}.$$

Insgesamt erhält man

$$\begin{aligned}\left|\sqrt{d} - \frac{x}{y}\right| &= \frac{x}{y} - \sqrt{d} = \frac{x - y\sqrt{d}}{y} \\ &= \frac{x^2 - dy^2}{y(x + y\sqrt{d})} < \frac{x^2 - dy^2}{y(2y\sqrt{d})} < \frac{1}{2y^2}.\end{aligned}$$

Daher kann Satz 4.3 (ii) angewendet werden und somit ist x/y ein Näherungsbruch der Kettenbruchentwicklung von $\sqrt{d}$.

Ist nun $-\sqrt{d} < x^2 - dy^2 < 0$, dann gilt

$$0 < y^2 - \frac{1}{d}x^2 < \frac{1}{\sqrt{d}}$$

und daher

$$y > \frac{x}{\sqrt{d}}.$$

Hieraus ergibt sich

$$\begin{aligned}\left|\frac{1}{\sqrt{d}} - \frac{y}{x}\right| &= \frac{y}{x} - \frac{1}{\sqrt{d}} = \frac{y - x/\sqrt{d}}{x} \\ &= \frac{y^2 - x^2/d}{x(y + x/\sqrt{d})} < \frac{y^2 - x^2/d}{2x^2/\sqrt{d}} < \frac{1}{2x^2}.\end{aligned}$$

Deswegen ist y/x ein Näherungsbruch der Kettenbruchentwicklung von $1/\sqrt{d}$.

Ist nun α eine irrationale Zahl mit Kettenbruchentwicklung $[a_0, a_1, \ldots]$, dann folgt $1/\alpha = [0, a_0, a_1, \ldots]$, daher ist der $k+1$-te Näherungsbruch von $1/\alpha$ der Kehrwert des k-ten Näherungsbruches von α für alle k. Daraus folgt, dass x/y ein Näherungsbruch von $\sqrt{d}$ ist.

Irrationale Zahlen haben immer unendliche Kettenbruchentwicklungen. Es gibt allerdings unter ihnen solche, die eine periodische Entwicklung besitzen. Ziel der nächsten beiden Lemmata ist es, zu zeigen, dass alle irrationalen Zahlen mit quadratischem Minimalpolynom in solche Kettenbrüche entwickelt werden können.

Definition 4.2 *Ein Kettenbruch heißt periodisch mit Periode k, wenn es einen Index N gibt, sodass $a_n = a_{n+k}$ für alle $n \geq N$ gilt. Ein solcher Kettenbruch wird in der Form $[a_0, \ldots, a_{N-1}, \overline{a_N, a_{N+1}, \ldots, a_{N+k-1}}]$ geschrieben.*

Lemma 4.7 *Sei α eine irrationale Zahl mit Minimalpolynom vom Grad 2 über $\mathbb{Q}$, dann gibt es ganze Zahlen P_0, Q_0 und d mit $Q_0|(d - P_0^2)$ sodass*

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0}.$$

Definiert man weiters

$$\begin{aligned} \alpha_k &= \frac{P_k + \sqrt{d}}{Q_k}, \\ a_k &= [\alpha_k], \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k}, \end{aligned}$$

dann ist $[a_0, a_1, a_2, \ldots]$ die Kettenbruchentwicklung von α.

Beweis: Da α irrational mit quadratischem Minimalpolynom ist, gibt es ganze Zahlen a, b, e, f, $e, f > 0$, e kein perfektes Quadrat, sodass

$$\alpha = \frac{a + b\sqrt{e}}{f} = \frac{af + \sqrt{eb^2 f^2}}{f^2}$$

gilt und klarerweise $f^2|(a^2 f^2 - eb^2 f^2)$. Man kann also $P_0 = af$, $Q_0 = f^2$ und $d = eb^2 f^2$ setzen. Da d kein perfektes Quadrat ist, gilt $Q_k \neq 0$ für alle k und somit ist die Folge wohldefiniert. Um zu zeigen, dass $[a_0, a_1, \ldots]$ die Kettenbruchentwicklung von α ist genügt es wegen Lemma 4.5 $\alpha_{k+1} =$

$1/(\alpha_k - a_k)$ nachzuweisen:

$$\begin{aligned}
\alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k \\
&= \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k} \\
&= \frac{\sqrt{d} - P_{k+1}}{Q_k} \\
&= \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} \\
&= \frac{Q_{k+1}}{\sqrt{d} + P_{k+1}} \\
&= \frac{1}{\alpha_{k+1}}
\end{aligned}$$

Lemma 4.8 *Sei α eine irrationale Zahl mit quadratischem Minimalpolynom, dann hat α eine periodische Kettenbruchentwicklung.*

Beweis: Nach Lemma 4.7 kann man α in der Form

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0}$$

mit $Q_0|(P_0^2 - d)$ schreiben und mittels

$$\begin{aligned}
\alpha_k &= \frac{P_k + \sqrt{d}}{Q_k}, \\
a_k &= [\alpha_k], \\
P_{k+1} &= a_k Q_k - P_k, \\
Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k},
\end{aligned}$$

rekursiv die Kettenbruchzerlegung von α bestimmen.

Nach Lemma 4.2 gilt nun

$$\alpha = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}$$

und wenn α' die Konjungierte von α über $\mathbb{Q}$ bezeichnet, folgt

$$\alpha' = \frac{\alpha'_k p_{k-1} + p_{k-2}}{\alpha'_k q_{k-1} + q_{k-2}}.$$

Hieraus erhält man durch Umformungen

$$\alpha'_k = -\frac{q_{k-2}}{q_{k-1}} \left(\frac{\alpha' - C_{k-2}}{\alpha' - C_{k-1}} \right).$$

Da $C_{k-1}, C_{k-2} \to \alpha$ für $k \to \infty$ ergibt sich daraus

$$\frac{\alpha' - C_{k-2}}{\alpha' - C_{k-1}} \to 1$$

und daher gilt $\alpha'_k < 0$ für genügend großes k. Es folgt, da $\alpha_k > 0$, dass $\alpha_k - \alpha'_k = 2\sqrt{d}/Q_k > 0$ ab einem Index. Nach Definition gilt $Q_k Q_{k+1} = d - P_{k+1}^2$ und somit erhält man aus dem bisherigen

$$Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 \leq d$$

und

$$P_{k+1}^2 \leq d - Q_k \leq d$$

für genügend großes k. Daher gibt es nur endlich viele mögliche Werte für P_k und Q_k und deswegen muß es zwei Indices $i < j$ geben mit $P_i = P_j$ und $Q_i = Q_j$, dann gilt aber auch $a_i = a_j$ und da die a_i rekursiv definiert sind folgt daraus

$$\alpha = [a_0, a_1, \ldots, a_{i-1}, \overline{a_i, \ldots, a_{j-1}}].$$

Lemma 4.9 *Sei d eine positive ganze Zahl, aber kein perfektes Quadrat und $\alpha = \sqrt{d}$ dann gilt*

$$p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k \quad \textit{für} \quad k \geq 1$$

wobei p_k/q_k der k-te Näherungsbruch von α ist und Q_k wie in Lemma 4.7 definiert wird.

Beweis: Laut Definition gilt

$$p_0^2 - dq_0^2 = [\sqrt{d}]^2 - d = -Q_1.$$

Angenommen $k \geq 2$, dann folgt

$$\sqrt{d} = \alpha = [a_0, a_1, \ldots, a_{k-1}, \alpha_k] = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}.$$

Wegen $\alpha_k = (P_k + \sqrt{d})/Q_k$ ergibt sich

$$\sqrt{d} = \frac{(P_k + \sqrt{d})p_{k-1} + Q_k p_{k-2}}{(P_k + \sqrt{d})q_{k-1} + Q_k q_{k-2}}$$

und daraus folgt

$$dq_{k-1} + (P_k q_{k-1} + Q_k q_{k-2})\sqrt{d} = P_k p_{k-1} + Q_k p_{k-2} + p_{k-1}\sqrt{d}.$$

Vergleicht man nun die Koeffizienten über $\mathbb{Q}(\sqrt{d})$ erhält man

$$dq_{k-1} = P_k p_{k-1} Q_k p_{k-2}$$

und

$$p_{k-1} = P_k q_{k-1} + Q_k q_{k-2}.$$

Aus diesen beiden Gleichungen und Lemma 4.3 ergibt sich

$$p_{k-1}^2 - dq_{k-1}^2 = (p_{k-1}q_{k-2} - p_{k-2}q_{k-1})Q_k = (-1)^k Q_k.$$

Definition 4.3 *Ein Kettenbruch der Form* $[\overline{a_0, a_1, \ldots, a_n}]$ *heißt rein periodisch mit Periode* n*.*

Für den Beweis der folgenden beiden Lemmata siehe [4] und [8].

Lemma 4.10 *Sei* d *kein perfektes Quadrat, dann besitzt* $\sqrt{d}$ *eine Kettenbruchentwicklung der Form* $[a_0, \overline{a_1, \ldots, a_n}]$*.*

Lemma 4.11 *Sei* n *die Periode der Kettenbruchentwicklung von* $\sqrt{d}$*, dann ist* n *die kleinste, positive ganze Zahl mit* $Q_n = 1$*, außerdem gilt* $Q_k \neq -1$ *für alle* k*.*

Folgerung 4.0.2 $(-1)^k Q_k = \pm 1$ *dann und nur dann, wenn* $n|k$*.*

Nach diesen Vorbereitungen ist es nun möglich eine Darstellung der fundamentalen Einheit mittels Kettenbrüchen für quadratische Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ mit $d \equiv 2, 3 \bmod 4$ anzugeben.

Satz 4.4 *Sei n die Periode der Kettenbruchentwicklung von $\sqrt{d}$, dann folgt:*

(i) Alle ganz zahligen Lösungen der Gleichung $x^2 - dy^2 = \pm 1$ sind gegeben durch

$$x + y\sqrt{d} = \pm(p_{n-1} + q_{n-1}\sqrt{d})^l : l \in \mathbb{Z},$$

wobei p_{n-1}/q_{n-1} der $(n-1)$-te Näherungsbruch von $\sqrt{d}$ ist.

(ii) Ist d quadratfrei und gilt $d \equiv 2, 3 \mod 4$, dann ist $p_{n-1} + q_{n-1}\sqrt{d}$ die fundamentale Einheit von $\mathbb{Q}(\sqrt{d})$.

Beweis:

(i) Ist (x, y) eine Lösung der Gleichung $x^2 - dy^2 = \pm 1$, dann

$$(x + y\sqrt{d})^{-1} = \pm(x - y\sqrt{d}),$$

außerdem gilt, ist eines der vier Paare $\pm(a, \pm b)$ eine Lösung der Gleichung $x^2 - dy^2 = \pm 1$, dann sind alle vier Lösungen, daher genügt es zu zeigen, dass alle positiven Lösungen durch

$$x + y\sqrt{d} = (p_{n-1} + q_{n-1}\sqrt{d})^m : m > 0$$

gegeben sind. Wegen Lemma 4.6 folgt, aus $x^2 - dy^2 = \pm 1$, $x = p_{k-1}$ und $y = q_{k-1}$ für ein k. Weiters gilt mit Lemma 4.9

$$p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k = \pm 1$$

und somit $Q_k = \pm 1$. Hieraus folgt mit der Folgerung zu Lemma 4.11 $n|k$. Da

$$p_{n-1} < p_{2n-1} < \cdots \quad \text{und} \quad q_{n-1} < q_{2n-1} < \cdots$$

ist $x_1 = p_{n-1}$, $y_1 = q_{n-1}$ die kleinste positive Lösung. Nun soll gezeigt werden, dass alle positiven Lösungen (x_m, y_m) gegeben sind durch

$$x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m, m > 0.$$

Betrachtet man die Konjungierte $x_m - y_m\sqrt{d} = (x_1 - y_1\sqrt{d})^m$, so erhält man

$$(x_m + y_m\sqrt{d})(x_m - y_m\sqrt{d}) = (x_1^2 - dy_1^2)^m = (\pm 1)^m = \pm 1$$

(x_m, y_m) ist also tatsächlich eine Lösung.

Angenommen es gäbe eine positive Lösung (X, Y), die nicht von dieser Form ist, dann existiert eine ganze Zahl $\kappa \geq 0$, sodass

$$(x_1 + y_1\sqrt{d})^\kappa < X + Y\sqrt{d} < (x_1 + y_1\sqrt{d})^{\kappa+1}$$

oder auch

$$1 < (x_1 + y_1\sqrt{d})^{-\kappa}(X + Y\sqrt{d}) < x_1 + y_1\sqrt{d}.$$

Wegen $x_1^2 - y_1^2 d = \pm 1$ erhält man $(x_1 + y_1\sqrt{d})^{-\kappa} = [\pm(x_1 - y_1\sqrt{d})]^\kappa$. Definiert man zwei ganze Zahlen s und t mittels

$$s + t\sqrt{d} = (x_1 + y_1\sqrt{d})^{-\kappa}(X + Y\sqrt{d}) = \pm(x_1 - y_1\sqrt{d})^\kappa(X + Y\sqrt{d}),$$

ergibt sich

$$\begin{aligned} s^2 - dt^2 &= [\pm(x_1 - y_1\sqrt{d})^\kappa(X + Y\sqrt{d})][\pm(x_1 + y_1\sqrt{d})^\kappa(X - Y\sqrt{d})] \\ &= X^2 - dY^2 = \pm 1. \end{aligned}$$

Daher ist (s, t) eine Lösung der Gleichung und es gilt

$$1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d}$$

Hieraus erhält man

$$0 < (x_1 + y_1\sqrt{d})^{-1} < (s + t\sqrt{d})^{-1} < 1 < s + t\sqrt{d}$$

und somit folgt

$$\begin{aligned} 2s &= s + t\sqrt{d} \pm [\pm(s - t\sqrt{d})] = s + t\sqrt{d} \pm (s + t\sqrt{d})^{-1} > 0 \\ 2t\sqrt{d} &= s + t\sqrt{d} \mp [\pm(s - t\sqrt{d})] > 0. \end{aligned}$$

Daher ist (s, t) eine positive Lösung und damit muß nach der Annahme $s \geq x_1$, $t \geq y_1$ gelten, im Widerspruch zu $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$.

(ii) Da $p_{n-1} + q_{n-1}\sqrt{d} > 1$ folgt die Tatsache direkt aus (i).

Für quadratische Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ mit $d \not\equiv 2, 3 \bmod 4$ gibt es noch keine allgemeinen Resultate die Darstellung der fundamentalen Einheit mittels Kettenbrüchen betreffend. Allerdings gibt es Ergebnisse für Spezialfälle. Betrachtet man statt der Kettenbruchentwicklung von $\sqrt{d}$ jene von $\omega_d = (1 + \sqrt{d})/2$ und hat diese Periode 3, 4 oder 5, so ist eine Darstllung der fundamentalen Einheit möglich. Die folgenden drei Sätze liefern diese

Darstellungen, ihre Beweise sollen hier enfallen, sie können in [9] und [10] nachgelesen werden.

In den folgenden Sätzen sollen $K = \mathbb{Q}(\sqrt{d})$ ein quadrtischer Zahlkörper mit $d \equiv 1 \mod 4$, d quadratfrei und $\varepsilon_d = (T_d + U_d\sqrt{d})/2$ seine fundamentale Einheit sein, außerdem soll k_d die Periode der Kettenbruchentwicklung von $\omega_d = (1 + \sqrt{d})/2$ bezeichnen.

Satz 4.5 *Ist $k_d = 3$, so gilt für ungerades a und positive ganze Zahlen l und r*

$$\omega_d = [(a+1)/2, \overline{l, l, a}],$$
$$(T_d, U_d) = ((l^2+1)^2 r + l(l^2+3), l^2+1)$$

mit $a = (l^2+1)r + l$ und darüberhinaus

$$d = (l^2+1)^2 r^2 + 2l(l^2+3)r + l^2 + 4.$$

Ist a gerade, so erhält man

$$\omega_d = [a/2, \overline{1, 1, a-1}],$$

$$(T_d, U_d) = (2a, 2)$$

und

$$d = a^2 + 1.$$

Satz 4.6 *Ist $k_d = 4$, dann gilt für gerades a und ganzzahliges $l \geq 1$, l ungerade*

$$\omega_d = [a/2, \overline{1, l, 1, a-1}],$$
$$(T_d, U_d) = (A^2 r + B, A)$$

und

$$d = A^2 r^2 + 2Br + C$$

wobei $A = l + 2$, $B = A^2 - 2$, $C = (A+2)(A-2)$ und r die eindeutig bestimmte gerade ganze Zahl mit $r > 0$ ist, die $a = Ar + A - 1$ erfüllt. Dieser Fall kann nur für $d \equiv 5 \mod 8$ auftreten. Ist hingegen a ungerade, so gilt mit ganzzahligem $l \geq 1$ und $v \geq 1$

$$\omega_d = [(a+1)/2, \overline{l, v, l, a}],$$

$$(T_d, U_d) = (l(A+1)(Ar + sl) + 2A, l(A+1))$$

und

$$d = (A+2)(A-2)r^2 + 2sl(A+2)r + s(sl^2+4)$$

mit $A = vl+1$ *und* r *und* s *sind die eindeutig durch die Gleichungen*

$$\begin{aligned} v &= -r + ls \\ a &= Ar + ls \end{aligned}$$

bestimmten positiven ganzen Zahlen.

Satz 4.7 *Ist* $k_d = 5$*, dann gilt für gerades* a *und ganzzahliges* $l \geq 0$

$$\omega_d = [a/2, \overline{1, l, l, 1, a-1}],$$

$$(T_d, U_d) = (A^2 r + B, A)$$

und

$$d = A^2 r^2 + 2Br + C$$

wobei $A = l^2 + 2l + 2$*,* $B = (l^2+l)A + l^2$*,* $C = (l^2+3)l^2 + 2(l^2-1)l + 1$ *und* r *die eindeutig bestimmte nicht negative ganze Zahl ist, die* $a = Ar + l^2 + l$ *erfüllt. Ist hingegen* a *ungerade, so gilt mit ganzzahligem* $l \geq 2$ *und* $v > 0$

$$\omega_d = [(a+1)/2, \overline{l, v, v, l, a}],$$

$$(T_d, U_d) = (a(A^2 + l^2) + 2(vA + l), A^2 + l^2)$$

und

$$d = A^2 r^2 + 2Br + C$$

mit $A = vl + 1$*,* $B = slA + 2v$*,* $C = s(sl^2 + 4)$ *und* r *und* s *sind die eindeutig durch die Gleichungen*

$$\begin{aligned} Ar + ls &= a \\ lr - As &= -v^2 - 1 \end{aligned}$$

bestimmten positiven ganzen Zahlen.

Mit Hilfe dieser Ergebnisse ist es möglich einige reell quadratische Zahlkörper mit Klassenzahl 1 zu bestimmen.

Satz 4.8 *1. Ist* $k_d = 3$*, dann gibt es genau 11 reell quadratische Zahlkörper mit Klassenzahl* 1*, nämlich jene mit*

$$d \in \{17, 37, 61, 101, 197, 317, 461, 557, 667, 773, 1877\}$$

2. *Ist* $k_d = 4$ *und* a *gerade, dann gibt es genau 5 reell quadratische Zahlkörper mit Klassenzahl* 1*, nämlich jene mit*

$$d \in \{69, 213, 413, 717, 1077\}$$

3. *Ist* $k_d = 5$ *und* a *gerade, dann gibt es genau fünf* d*'s mit einer möglichen Ausnahme, sodass der reell quadratische Zahlkörper* $K = \mathbb{Q}(\sqrt{d})$ *Klassenzahl* 1 *besitzt, nämlich jene mit*

$$d \in \{41, 149, 157, 269, 941\}$$

4. *Ist* $k_d = 5$ *und* a *ungerade, dann gibt es für* $d \leq 50000$ *genau 7 reell quadratische Zahlkörper mit Klassenzahl* 1*, nämlich jene mit*

$$d \in \{181, 397, 1013, 2477, 2693, 3533, 4253\}$$

Literatur

[1] Tom M. Apostol. *Introduction to Analytic Number Theory*, Springer-Verlag, New York, Heidelberg, Berlin, 1976

[2] P. Bundschuh. *Einführung in die Zahlentheorie*, Springer-Verlag, New York, Berlin, Heidelberg, 1988

[3] J. Elstrodt. *Maß- und Integrationstheorie*, Springer-Verlag, New York, Berlin, Heidelberg, 1999

[4] J. Esmonde, M. Ram Murty. *Problems in Algebraic Number Theory*, Springer-Verlag, New York, Berlin, Heidelberg, 1999

[5] K. Ireland, M. Rosen. *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, Berlin, Heidelberg, 1990

[6] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*, PWN-Polish Scientific Publishers, Warszawa, Springer-Verlag, New York, Berlin, Heidelberg, 1990

[7] W. Narkiewicz. *Classical Problems in Number Theory*, PWN-Polish Scientific Publishers, Warszawa, 1986

[8] H.M. Stark. *An Introduction to Number Theory*, Markham Publishing Company, Chicago, 1970

[9] K. Tomita. *Explicit Representation of Fundamental Units of Some Quadratic Fields*, Proc. Japan Acad. Ser. A Math. Sci. 71, 41-43, 1995

[10] K. Tomita. *Explicit Representation of Fundamental Units of Some Quadratic Fields, II*, Journal of Number Theory 63, 275-285, 1997