Quadratische Zahlkörper und die Geschlechtertheorie

Candy Walter

Bachelorarbeit

Gottfried Wilhelm Leibniz Universität Hannover
Fakultät für Mathematik und Physik
Institut für Algebra, Zahlentheorie und Diskrete Mathematik

Inhaltsverzeichnis

Vorwort

Diese Arbeit soll auf Grundlage der quadratischen Zahlkörper in einige bedeutende Abschnitte der algebraischen Zahlentheorie einführen. Vorausgesetzt werden dabei die Kenntnisse der linearen Algebra (Vektorräume, lineare Abbildungen, Polynom und Polynomringe, Matrizenrechnung etc.), sowie der Umgang mit Begriffen aus der elementaren Zahlentheorie (Kongruenzrechnen, eindeutige Primfaktorzerlegung, quadratische Reste, quadratisches Reziprozitätsgesetz etc.). Es werden in dieser Arbeit drei wesentliche Konzepte behandelt. Zum ersten wird der quadratische Zahlkörper eingeführt um darauf aufbauend die Dedekindsche Idealentheorie und die der Geschlechter zu entwickeln. Dabei werden die Theorien natürlich nur soweit behandelt, wie für die jeweilige Fragestellung nötig ist. Die Beschränkung auf quadratische Zahlkörper liegt deren Einfachheit zugrunde und gibt einen systematischen Einblick in Theorien, die auf den allgemeinen Zahlkörper übertragen oder weiterentwickelt werden können. Ziel dieser Arbeit soll jedoch nicht nur die Entwicklung der einzelnen Theorien sein, sondern auch wie mit deren Hilfe konkrete Probleme in den Griff zu bekommen sind. So zeigt sich, dass die Geschlechtertheorie (einer der schwierigsten Abschnitte, die Gauss in seiner Disquisitiones Arithmeticae behandelt) in vielen Fällen eine befriedigende Antwort auf die Frage nach der Darstellung von Primzahlen durch nicht äquivalente, binäre quadratische Formen mit gleicher Diskriminante geben kann. Im Verlauf der Arbeit werde ich immer wieder auf die historischen Zusammenhänge bei der Entwicklung der einzelnen Theorien aufmerksam machen und z.B. die geniale Schöpfung der idealen Zahlen durch Edmund Kummer beschreiben um anschließend den Fundamentalsatz der elementaren Zahlentheorie zu Verallgemeinern. Es lohnen sich dies bezüglich Arbeiten von Kummer ab 1845 anzusehen, welche André Weil in seinen Werken [We1] und [We2,Seite 381] zusammengetragen hat. Bei der Ausarbeitung habe ich mich an den verschiedensten Literaturen orientiert, wie beispielsweise an den Originalliteraturen von Dirichlet [Di] und Gauss [DA]. Gerade die Literatur von Dirichlet gibt einen hervorragenden Einblick in die Arbeiten von Gauss wieder und stellt in vereinfachter Weise deren Definitionen und Sätze brilliant dar. Meines Erachtens nach ist es noch heute vielen modernen zahlentheoretischen Lehrbüchern weit überlegen und daher sehr zu empfehlen.

Bedanken möchte ich mich an dieser Stelle bei all denjenigen, die mich im Verlauf der Arbeit unterstützt haben. Ein besonderer Dank geht an Herrn Timm Sabatino für sein gründliches Korrekturlesen.

Hannover, September 2009 *Candy Walter*

1 Quadratische Zahlkörper

Die Theorie der quadratischen Zahlkörper entwickelte sich aus dem Studium der binären quadratischen Formen. Euler und Fermat hatten bei ihren Untersuchungen zu diophantischen Gleichungen viele fundamentale Einzelergebnisse zusammengetragen, welche anschließend Raum für weitere Forschungen boten. In seiner Disquisitiones Arithmeticae knüpft Gauss im Abschnitt V an die Arbeiten von Pierre de Fermat, Leonhard Euler und Joseph Louis Lagrange an und behandelt dort ausgiebig die Theorie der binären quadratischen Formen. Obwohl sich Gauss bei seiner Darstellung im Bereich der ganzen Zahlen bewegt, ist es aus heutiger Sicht eleganter den Körper der rationalen Zahlen so quadratisch zu erweitern, dass eine Zerlegung der quadratischen Formen in Linearfaktoren vorgenommen werden kann. Eine solche Zerlegung sieht dann wie folgt aus: $x^2 - 5y^2 = \left(x + y\sqrt{5}\right)\left(x - y\sqrt{5}\right)$. Somit wird die Theorie der quadratischen Zahlkörper zu einem Bestandteil der Theorie der binären quadratischen Formen. Wir können auf verschiedene Art den Körper $\mathbb{Q}$ der rationalen Zahlen zu einem umfassenden Körper $K \subseteq \mathbb{C}$ erweitern. Betrachten wir etwa den Ring $\mathcal{O}$ der ganzalgebraischen Zahlen, das sind bekanntlich jene komplexen Zahlen α, die Nullstelle eines nichttrivial normierten Polynoms mit ganzzahligen Koeffizienten sind. Dann ist es sinnvoll nur so viele der Zahlen hinzuzunehmen, wie für ein gegebenes Problem benötigt wird. Sei K der kleinste Teilkörper vom Körper $\overline{\mathbb{Q}}$ der algebraischen Zahlen und seien $\alpha_1, \ldots, \alpha_n$ endlich viele algebraische Zahlen, die in K enthalten sind. Dann schreibt man $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ und sagt der Körper K ist ein Erweiterungskörper oder eine Körpererweiterung von $\mathbb{Q}$, der durch Adjunktion der Elemente $\alpha_1, \ldots, \alpha_n$ aus $\mathbb{Q}$ entsteht. Insbesondere ist $(K, +)$ eine abelsche Gruppe und da die Multiplikation von Elementen aus K mit den Skalaren aus $\mathbb{Q}$ erklärt ist über

$$\cdot : \begin{cases} \mathbb{Q} \times K \to K \\ (\eta, \alpha) \mapsto \eta\alpha, \end{cases}$$

erhalten wir aus den Körperaxiomen für $\mathbb{Q}$ unmittelbar die aus der Linearen Algebra bekannten Vektorraumaxiome, so dass wir K als ein Vektorraum über $\mathbb{Q}$ auffassen können, d.h. für $\eta, \mu \in \mathbb{Q}$ und $\alpha, \beta \in K$ gilt

$$\eta(\alpha + \beta) = \eta\alpha + \eta\beta, \;\; (\eta + \mu)\alpha = \eta\alpha + \mu\alpha, \;\; (\eta\mu)\alpha = \eta(\mu\alpha), \;\; 1\alpha = \alpha.$$

Der Körper K besitzt über $\mathbb{Q}$ endlichen Grad, sodass K als $\mathbb{Q}$-Vektorraum endlich dimensional ist. Wird $K := \mathbb{Q}(\alpha)$ von einem algebraischen Element erzeugt, dann hat $\mathbb{Q}(\alpha)$ eine Basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ und folglich die Vektorraumdimension $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) := [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, wobei n gleich dem Grad des Minimalpolynoms f_α entspricht, das α als Nullstelle hat. (Selbstverständlich hat ein quadratischen Zahlkörper Grad 2 über $\mathbb{Q}$, siehe [Be,Satz 4.3]). Körper, die über $\mathbb{Q}$ einen endlichen Grad besitzen, heißen *Zahlkörper*. Für einen Zahlkörper $\mathbb{Q}(\alpha)$ bezeichnet $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Q}(\alpha) \cap \mathcal{O}$ den *Ganzheitsring* von $\mathbb{Q}(\alpha)$ bzw. den ganzen Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\alpha)$. Somit besteht $\mathcal{O}_{\mathbb{Q}(\alpha)}$ aus allen Elementen, die in $\mathbb{Q}(\alpha)$ ganzalgebraisch sind, d.h. es ist $\mathcal{O}_{\mathbb{Q}(\alpha)} := \{\alpha \in \mathbb{Q}(\alpha) \mid f_\alpha \in \mathbb{Z}[X]\}$. Wir hatten zu Beginn des Kapitels bereits von einer quadratischen Erweiterung der rationalen Zahlen

gesprochen. Wir gelangen damit zu den *quadratischen Zahlkörpern*. Solche entstehen also aus $\mathbb{Q}$ durch Adjunktion der Quadratwurzel $\sqrt{d}$. Sei im Folgenden d eine von 0 und 1 verschieden quadratfreie ganze Zahl, dann heißt die Menge

$$\mathbb{Q}\left(\sqrt{d}\right) := \left\{x + y\sqrt{d} \in \mathbb{C}, \quad x,y \in \mathbb{Q}\right\}$$

ein quadratischer Zahlkörper. Ist $d > 0$, so heißt $\mathbb{Q}(\sqrt{d})$ *reellquadratisch* und für $d < 0$ *imaginärquadratisch*. Wobei $\sqrt{d} \in \mathbb{C}$ eine (willkürlich, aber fest gewählte) komplexe Lösung der Gleichung $X^2 = d$ ist. Die andere Lösung ist natürlich $-\sqrt{d} \in \mathbb{C}$. Nun überlegt man sich leicht, dass jedes Element von $\mathbb{Q}(\sqrt{d})$ Nullstelle eines Polynoms $f \in \mathbb{Q}[X]$ vom Grad ≤ 2 ist. Also ist jedes Element von $\mathbb{Q}(\sqrt{d})$ algebraisch. Damit erhalten wir einen Turm von Körpern:

$$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{d}) \subsetneq \overline{\mathbb{Q}} \subsetneq \mathbb{C}.$$

Insbesondere ist $\left\{1, \sqrt{d}\right\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{d})$, d.h. es ist

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{d}.$$

Wir wollen nun die wichtigen Begriffe der Norm und Spur einführen. Vorher ist es jedoch geschickt den zu $\mathbb{Q}(\sqrt{d})$ isomorphen Restklassenkörper

$$\mathbb{Q}[X] / (X^2 - d)\,\mathbb{Q}[X]$$

als den quadratischen Zahlenkörper aufzufassen. Diesen können wir nun mühelos in

$$\mathbb{Q}(\sqrt{d})_{\mathbb{R}} := \mathbb{R}[X] / (X^2 - d)\,\mathbb{R}[X] \cong \begin{cases} \mathbb{C}, & d < 0 \\ \mathbb{R} \times \mathbb{R}, & d > 0 \end{cases}$$

einbetten. Damit erhalten wir für die Einbettung von $\mathbb{Q}(\sqrt{d})$ nach $\mathbb{R} \times \mathbb{R}$ konkret:

$$x + y\sqrt{d} \;\mapsto\; \left(x + y\sqrt{d}, x - y\sqrt{d}\right)$$

Der Körper $\mathbb{Q}(\sqrt{d})$ besitzt genau zwei Körperautomorphismen, diese ist zum einen die identische Abbildung:

$$id_{\mathbb{Q}(\sqrt{d})} : \mathbb{Q}\left(\sqrt{d}\right) \;\to\; \mathbb{Q}\left(\sqrt{d}\right),\; x+y\sqrt{d} \;\mapsto\; x+y\sqrt{d}$$

und zum anderen die Konjugationsabbildung:

$$\sigma : \mathbb{Q}\left(\sqrt{d}\right) \;\to\; \mathbb{Q}\left(\sqrt{d}\right),\; x+y\sqrt{d} \;\mapsto\; x-y\sqrt{d}.$$

Wir wollen dies mit dem nachfolgenden Satz festhalten.

Satz 1.1 *Für ein quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ gilt es genau die zwei Körperautomorphismen:*

$$\sigma : \mathbb{Q}\left(\sqrt{d}\right) \;\to\; \mathbb{Q}\left(\sqrt{d}\right),\; x{+}y\sqrt{d} \;\mapsto\; x{-}y\sqrt{d}$$

und

$$id_{\mathbb{Q}(\sqrt{d})} : \mathbb{Q}\left(\sqrt{d}\right) \;\to\; \mathbb{Q}\left(\sqrt{d}\right),\; x{+}y\sqrt{d} \;\mapsto\; x{+}y\sqrt{d}.$$

Beweis: Es ist $\left\{1, \sqrt{d}\right\}$ eine Basis von $\mathbb{Q}(\sqrt{d})$, damit ist σ die lineare Fortsetzung der Zuordnung $1 \mapsto 1$ und $\sqrt{d} \mapsto -\sqrt{d}$. σ ist folglich eine lineare Abbildung mit der Darstellungsmatrix

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Bzgl. Addition ist die Relationstreue klar:

$$\sigma(\alpha_1 + \alpha_2) = \sigma(\alpha_1) + \sigma(\alpha_2).$$

für zwei Zahlen $\alpha_1 = x_1 + y_1\sqrt{d}$ und $\alpha_2 = x_2 + y_2\sqrt{d}$ mit $x_1, x_2, y_1, y_2 \in \mathbb{Q}$. Aber auch bezüglich der Multiplikation ist σ relationstreu:

$$\begin{aligned} \sigma(\alpha_1\alpha_2) &= \sigma\left(x_1x_2 + y_1y_2d + (x_1y_2 + x_2y_1)\sqrt{d}\right) \\ &= x_1x_2 + y_1y_2d - (x_1y_2 + x_2y_1)\sqrt{d} \\ &= x_1x_2 + (-y_1)(-y_2)d + (x_1(-y_2) + x_2(-y_1))\sqrt{d} \\ &= \sigma(\alpha_1)\,\sigma(\alpha_2). \end{aligned}$$

Also ist σ der Körperautomorphismus von $\mathbb{Q}(\sqrt{d})$. Die Fixpunktmenge ist offensichtlich $\mathbb{Q}$. Man sieht zudem, dass σ bijektiv ist, da die Determinante von A mit $\det(A) = -1 \neq 0$ nicht verschwindet. Folglich ist die Darstellungsmatrix invertierbar. Zudem hält jeder Körperautomorphismus τ von $\mathbb{Q}(\sqrt{d})$ die 1 fest und somit auch alle Elemente des kleinsten Teilkörpers $\mathbb{Q}$ von $\mathbb{Q}(\sqrt{d})$. Insbesondere ist τ ein Körperautomorphismus des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\sqrt{d})$ mit $\tau(1) = 1$. Dieser ist durch das Bild von $\sqrt{d}$ bereits festgelegt, und Aufgrund der Verträglichkeit von τ bezüglich der Multiplikation ist $\tau(\sqrt{d})^2 = \tau(\sqrt{d})\tau(\sqrt{d}) = \sqrt{d}\sqrt{d} = d$, also $\tau(\sqrt{d}) = \pm\sqrt{d}$ und damit $\tau = \sigma$ oder $\tau = id_{\mathbb{Q}(\sqrt{d})}$. □

Insbesondere ist $Aut\left(\mathbb{Q}(\sqrt{d})\right) = \{id_{\mathbb{Q}(\sqrt{d})}, \sigma\}$ eine *Galoisgruppe*[1] der Ordnung 2.

Für $\alpha := x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ heißt $\sigma(\alpha) := \alpha' = x - y\sqrt{d}$ das konjugierte Element zu α. Die beiden Größen *Norm* und *Spur* eines quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ lassen sich nun aus seinem Körperautomorphismus σ darstellen über die Abbildungen:

[1] Nach französischer Mathematiker Évariste Galois (1811–1832), der Alter von 20 Jahren bei einem Duell ums Leben kam.

$$N : \mathbb{Q}(\sqrt{d}) \ \to \ \mathbb{Q}\,,\, \alpha \ \mapsto \ \alpha\sigma(\alpha) \ \text{ und } Sp : \mathbb{Q}(\sqrt{d}) \ \to \ \mathbb{Q}\,,\, \alpha \ \mapsto \ \alpha+\sigma(\alpha)\,.$$

Da die Einbettung σ einen Ringhomomorphismus bildet, wird die Spur additiv und die Norm multiplikativ. Durch Einsetzen erhalten wir sofort

$$N(\alpha) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2 \text{ sowie } Sp\,(\alpha) = (x - y\sqrt{d}) + (x + y\sqrt{d}) = 2x.$$

Die Norm ist damit einfach eine quadratische Form auf $\mathbb{Q}(\sqrt{d})$. Aufgrund der Tatsache, dass die ganzalgebraischen Zahlen einen Ring $\mathcal{O}$ bilden, ist offensichtlich die Menge $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ebenfalls ein Ring. Dieser übernimmt eine analoge Rolle in $\mathbb{Q}(\sqrt{d})$, wie der Ring $\mathbb{Z}$ in $\mathbb{Q}$ und es gilt $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$. Also ist $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Unterring von $\mathbb{Q}(\sqrt{d})$. Damit sind alle Elemente der Form $x + y\sqrt{d}$, $x,y \in \mathbb{Z}$ stets ganz bzw. ganzalgebraisch und wir erhalten eine Inklusion von Ringen: $\mathbb{Z}\left[\sqrt{d}\right] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Das diese nicht notwendigerweise isomorph zueinander sind, zeigt das nachfolgende

Beispiel 1.2. Betrachten wir die dritten Einheitswurzel $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$. Diese ist eine Nullstelle des Polynoms $\varphi_3 = X^2 + X + 1 \in \mathbb{Z}\,[X]$ und somit eine ganzalgebraische Zahl. Also ist

$$\zeta_3 = \tfrac{-1+\sqrt{-3}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}, \text{ aber } \zeta_3 = \tfrac{-1+\sqrt{-3}}{2} \notin \mathbb{Z}\left[\sqrt{-3}\right].$$

Wir wollen uns nun damit beschäftigen, die ganzalgebraischen Zahlen in einem quadratischen Zahlkörper zu identifizieren. Beispielsweise ist die Zahl $\alpha = 1 + \frac{1}{2}\sqrt{5} \in \mathbb{Q}(\sqrt{5})$, aber wie man leicht nachrechnet ist $\alpha \notin \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. Es gibt nun eine sehr einfache Möglichkeit, die Zahlen α zu charakterisieren für die $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gilt. Dazu betrachten wir das folgende

Lemma 1.3. *Eine Zahl $\alpha := x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ liegt genau dann in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, wenn seine Spur und Norm ganze Zahlen sind.*

Beweis: " $\Rightarrow$ " Sei $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und σ der aus Satz 1.1 beschrieben Körperautomorphismus von $\mathbb{Q}(\sqrt{d})$. Es ist α ganzalgebraisch, also Nullstellen eines normierten Polynoms $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}\,[X]$. Aus Satz 1.1 folgt, dass die Abbildung σ bzgl. der Addition und Multiplikation relationstreu ist. Zudem ist σ $\mathbb{Q}$-linear und somit gilt für alle $f\,(X)$

$f\,(\sigma(\alpha)) = \sum_{i=0}^{n} a_i\sigma(\alpha)^i = \sum_{i=0}^{n} a_i\sigma(\alpha^i) = \sum_{i=0}^{n} \sigma(a_i\alpha)^i = \sigma\,(\sum_{i=0}^{n} a_i\alpha^i) = \sigma\,(f(\alpha)) = \sigma(0) = 0.$

Damit annulliert das ganzzahlige Polynom f neben α auch die Konjugation $\sigma(\alpha)$. D.h., $\sigma(\alpha)$ ist ganzalgebraisch und damit ist $\sigma(\alpha) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Folglich erhalten wir aus den Ringeigenschaften von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, dass $\alpha + \sigma(\alpha) = Sp(\alpha) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$ und $\alpha \cdot \sigma(\alpha) = N(\alpha) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$.

" $\Leftarrow$ " Sind nun $N(\alpha)$ und $Sp(\alpha)$ Elemente aus $\mathbb{Z}$ für $\alpha \in \mathbb{Q}(\sqrt{d})$, dann folgt aus dem Satz von CAYLEY-HAMILTON[2], dass α als Nullstelle des ganzzahlig normierten Polynoms $f(X) = (X-\alpha)(X-\sigma(\alpha)) = X^2 - Sp(\alpha) + N(\alpha)$ ganzalgebraisch ist. □

Die Richtigkeit der Aussage bleibt natürlich auch für $y = 0$ bestehen. Denn aus der Norm erhalten wir, dass mit $x^2 \in \mathbb{Z}$ auch $x \in \mathbb{Z}$ ist. Wir erhalten also ein einfaches Kriterium, um zu entscheiden, ob eine Zahl $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ ganzalgebraisch ist oder nicht. Es bleibt noch die Frage nach der Form der ganzalgebraischen Elemente aus $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Dabei hängen die vielfältigen Varianten der Elemente x und y von der Kongruenzklasse d modulo 4 ab. Als quadratfreie Zahl kann d von vornherein nur $\equiv$ 1,2,3 mod 4 sein. Es gilt nun

Satz 1.4. *Es sei $d \in \mathbb{Z}\setminus\{0,1\}$ quadratfrei und $\mathbb{Q}(\sqrt{d})$ der zugehörige quadratische Zahlkörper, dann gilt*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} x + y\sqrt{d},\ x,y \in \mathbb{Z}, & falls\ d \equiv 2,3 \bmod 4 \\ \frac{1}{2}\left(x + y\sqrt{d}\right),\ x,y \in \mathbb{Z},\ x \equiv y \bmod 2, & falls\ d \equiv 1 \bmod 4 \end{cases}.$$

Beweis: Sei $\alpha = r + s\sqrt{d}$ mit $r,s \in \mathbb{Q}$. Ist $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, dann folgt nach Lemma 1.3, dass $N(\alpha), Sp(\alpha) \in \mathbb{Z}$ bzw. $r^2 - ds^2,\ 2r \in \mathbb{Z}$ gilt. Setzen wir $2r \in \mathbb{Z}$ in die Norm: $(2r)^2 - d(2s)^2$, dann ist $4s^2d$ ganz und durch die Quadratfreiheit von d müssen somit auch $4s^2$ und schließlich $2s$ ganz sein. Dies sieht man folgendermaßen ein. Sei $4s^2 = \frac{a^2}{b^2}$ mit teilerfremden ganzen Zahlen a und $b > 0$. Da $4s^2d$ ganz ist, folgt $b^2 | da^2$. Wegen der Teilerfremdheit von a und b muss dann $b^2|d$ sein. Die Quadratfreiheit von d liefert, dass b nur die Werte ± 1 annehmen kann. Also ist $2s$ ganz und wir dürfen

$$2r = x,\ 2s = y \ \text{ bzw. } \ r = \frac{x}{2},\ s = \frac{y}{2} \text{ mit } x,y \in \mathbb{Z}. \tag{1}$$

schreiben. Wir nutzen nun aus, dass die Norm $N(\alpha) = r^2 - ds^2$ ganz ist und erhalten, dass $x^2 - dy^2 \equiv 0 \bmod 4$ sein muss.

Betrachten wir nun

1. Ist $d \equiv 2 \bmod 4$, dann folgt $2|x$, $4|x^2$ und $2|y$, also folgt aus (1), dass $r,s \in \mathbb{Z}$ sind. Damit hat jede ganze Zahl die Form $r + s\sqrt{d}$ mit $r,s \in \mathbb{Z}$.

2. Ist $d \equiv 3 \bmod 4$, dann folgt $0 \equiv x^2 - dy^2 \equiv x^2 + y^2 \bmod 4$ nur dann, wenn x,y gerade Zahlen sind. Also folgt wieder aus (1), dass $r,s \in \mathbb{Z}$ sind und jede ganze Zahl die Form $r + s\sqrt{d}$ mit $r,s \in \mathbb{Z}$ hat.

[2] Der aus der linearen Algebra bekannte Satz von CAYLEY-HAMILTON besagt, dass jede quadratische Matrix Nullstelle ihres charakteristischen Polynoms ist. [Fi, Seite 251]

3. Bleibt noch $d \equiv 1 \bmod 4$. Dann rechnet man leicht nach, dass die Kongruenz $0 \equiv x^2 - dy^2 \equiv x^2 - y^2 \bmod 4$ nur dann erfüllt ist, wenn $x \equiv y \bmod 2$ gilt. Damit haben alle ganzen Zahlen die Form $\frac{1}{2}\left(x + y\sqrt{d}\right)$ wobei x und y entweder beide gerade oder ungerade sind. Eine einfache Rechnung zeigt schließlich, dass diese Zahlen ganz sind.

□

Beispielsweise ist die dritte Einheitswurzel wegen $d = -3 \equiv 1 \bmod 4$

$$\zeta = \frac{1}{2}\left(-1 + \sqrt{-3}\right) \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$$

vom Typ $\frac{1}{2}\left(x + y\sqrt{d}\right)$. Wohingegen die ganzen Gaußschen Zahlen im Körper $\mathbb{Q}[i]$ aufgrund der Kongruenz $-1 \equiv 3 \bmod 4$ die Form $x + y\sqrt{d}$ besitzen.

Wie wir bereits wissen, besteht der Körper $\mathbb{Q}(\sqrt{d})$ aus allen $\mathbb{Q}$-Linearkombinationen der Elemente von 1 und $\sqrt{d}$. Es stellt sich daher die Frage, ob eine ähnliche Basis auch für den Ring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ existiert, d.h. gibt es ein $\omega \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ derart, sodass $\{1, \omega\}$ eine $\mathbb{Z}$-Basis bildet und folglich $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ aus allen $\mathbb{Z}$-Linearkombinationen der Element 1 und ω besteht. Das dies in der Tat so ist, ist eine einfache Folgerung vom Satz 1.4, siehe dazu [Fo,Seite219]. In diesem Fall schreiben wir $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} := \mathbb{Z} \oplus \omega\mathbb{Z}$ und nennen $\{1, \omega\}$ eine *Ganzheitsbasis* von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, also ist $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein freies $\mathbb{Z}$-Modul von Rang 2 und es gilt

Korollar 1.5. *Es ist* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} \oplus \omega\mathbb{Z}$ mit

$$\omega := \begin{cases} \sqrt{d}, & falls \;\; d \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{d}}{2}, & falls \;\; d \equiv 1 \bmod 4 \end{cases}$$

Einen ersten wesentlichen Unterschied von reell- und imaginärquadratischen Zahlkörpern besteht bezüglich ihrer Einheiten. So ist z.B. die Einheitengruppe $\mathbb{Z}^\times = \{-1, 1\}$ des Rings $\mathbb{Z}$ die zyklische Gruppe der Ordnung 2. Die Beschreibung der *Einheitengruppe* $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$ des Ganzheitsrings $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ hängt jedoch davon ab, ob $\mathbb{Q}(\sqrt{d})$ reell- oder imaginärquadratischen ist. So ist die Einheitengruppe für imaginärquadratische Zahlkörper endlich und wir können sie beschreiben mit

Satz 1.6. *Sei $d < 0$ und $\mathbb{Q}(\sqrt{d})$ der zugehörige quadratische Zahlkörper. Für die Einheitengruppe $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$ imaginärquadratischer Zahlkörper gilt*

$$\mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})} := \begin{cases} \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}, & falls \;\; d = -1 \\ \left\{\pm 1, \frac{1 \pm \sqrt{-3}}{2}, \frac{-1 \pm \sqrt{-3}}{2}\right\} \cong \mathbb{Z}/6\mathbb{Z}, & falls \;\; d = -3 \\ \{-1, 1\} \cong \mathbb{Z}/2\mathbb{Z}, & sonst. \end{cases}$$

Beweis: Wir zeigen zuerst, dass ein Element $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ genau dann eine Einheit ist, wenn $N(\alpha) \in \{-1, 1\}$ gilt. Sei zunächst $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ eine Einheit. Dann ist $\beta := \alpha^{-1} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und damit $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. Da $N(\alpha)$ und $N(\beta)$ ganze Zahlen sind, deren Produkt 1 ist, muss entweder $N(\alpha) = N(\beta) = 1$ oder $N(\alpha) = N(\beta) = -1$ sein. Also ist $N(\alpha) = \mathbb{Z}^\times = \{1, -1\}$. Sei nun $N(\alpha) = \{-1, 1\}$. Dann ist $\beta := N(\alpha)\sigma(\alpha) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und $\beta\alpha = N(\alpha)\sigma(\alpha)\alpha = N(\alpha)N(\alpha) = N(\alpha)^2 = 1$. Also ist $\alpha \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$.

Sei $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Nachdem was wir eben gezeigten haben ist $\alpha \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$ gleichbedeutend mit $|N(\alpha)| = 1$. Betrachten wir als erstes den Fall $d \equiv 1 \mod 4$. Dann ist nach Satz 1.4 $\alpha = \frac{(x+y\sqrt{d})}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $x, y \in \mathbb{Z}$ mit $x \equiv y \mod 2$. Aus der Norm von α erhalten wir nun $N(\alpha) = \alpha\sigma(\alpha) = \frac{x^2-y^2d}{4}$. Da nach Voraussetzung $d < 0$ ist, wird $N(\alpha)$ nicht negativ und wir erhalten nur endlich vielen Fällen mit $N(\alpha) = 1$. Dies gilt für $(x, y) \in \{(2, 0), (-2, 0)\}$ und wenn $d = -3$ ist, dann gilt zusätzlich $(x, y) \in \{(1, 1), (-1, 1), (-1, -1), (1, -1)\}$. Man rechnet nun nach, dass diese Werte die angegebenen Einheiten liefern. Ist nun $d \not\equiv 1 \mod 4$, dann folgt wieder aus Satz 1.4, dass $\alpha = x + y\sqrt{d}$, $x,y \in \mathbb{Z}$ gilt. Für die Norm erhalten wir diesmal $N(\alpha) = x^2 - y^2d$. Mit dem selben Argument wie eben wird $N(\alpha)$ nicht negativ und es existieren wiederum nur endlich viele Fälle mit $N(\alpha) = 1$, nämlich für $(x, y) \in \{(-1, 0), (1, 0)\}$ und im Falle $d = -1$ erhalten wir zusätzlich $(x, y) \in \{(0, -1), (0, 1)\}$. Einsetzen der Werte in $\alpha = x + y\sqrt{d}$ liefert das gewünschte. Damit haben wir alle Einheiten für $d < 0$ bestimmt und den Satz bewiesen.□

Im Falle des reellquadratischen Zahlkörpers ist die Beschreibung der Einheitengruppe sehr viel aufwändiger und soll an dieser Stelle nicht weiter behandelt werden. Es zeigt sich aber, dass jeder reellquadratische Zahlkörper unendlich viele Einheiten besitzt, siehe etwa [Art98, Satz 11.9]. Dabei läuft die Bestimmung der Einheitengruppe auf die Lösung der Pellsche-Gleichung $x^2 - dy^2 = \pm 1$ hinaus. Man kann nun mittels des Dirichletschen Schubfachprinzips zeigen, dass diese Gleichung unendlich viele Einheiten (Lösungen) liefert, siehe [Sa, Satz 8.1]. Da des Schubfachprinzip bedauerlicherweise nicht konstruktiv ist, gelingt die Bestimmung der Einheiten bis heute nur mittels der Kettenbruchapproximation.

Wir wollen nun wissen, inwieweit die Gültigkeit von Sätzen aus der elementaren Zahlentheorie mit denen in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ verträglich sind. Betrachten wir beispielsweise den Ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, in diesem kann die Zahl 21 auf zwei verschiedene Weisen zerlegt werden. So ist einerseits $21 = 3 \cdot 7$ und andererseits $21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Dass die Zahlen $3,\ 7\ , 1 \pm 2\sqrt{-5}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ alle irreduzibel und nicht zueinander assoziiert[3] sind, sieht man mit Hilfe der Norm folgendermaßen ein. Angenommen die Zahl 3 wäre zerlegbar. Etwa mit $3 = \alpha \cdot \beta$, wobei $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ keine Einheiten seien. Dann ist $N_{\mathbb{Q}(\sqrt{-5})}(3) = N_{\mathbb{Q}(\sqrt{-5})}(\alpha)N_{\mathbb{Q}(\sqrt{-5})}(\beta) = 9$ und folglich müssen $N_{\mathbb{Q}(\sqrt{-5})}(\alpha) = N_{\mathbb{Q}(\sqrt{-5})}(\beta) = \pm 3$ sein.

[3] In einem Integritätsring R mit Eins heißen zwei Elemente $a, b \in R$ zueinander assoziiert, wenn eine Einheit $\varepsilon \in R$ existiert, so dass $b = a \cdot \varepsilon$ gilt, d.h., wenn a und b sich Wechselseitig teilen.

Nach Korollar 1.5 sind α, β von der Form $x + y\sqrt{-5}$ mit $x, y \in \mathbb{Z}$ und damit folgt nach Lemma 1.3, dass die Norm $N_{\mathbb{Q}(\sqrt{-5})}(x + y\sqrt{-5}) = x^2 + 5y^2 \in \mathbb{Z}$ ist. Nun ist die Gleichung $x^2 + 5y^2 = \pm 3$ aber offensichtlich unlösbar in den ganzen Zahlen, was im Widerspruch zu unserer Annahme steht. Also ist die Zahl 3 in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ irreduzibel und man beweist analog, dass es auch die Zahlen $7\ , 1 \pm 2\sqrt{-5}$ sind. Dass die Zahlen 3 und 7 nicht zueinander assoziiert sind, ist klar. Genauso können $1 + 2\sqrt{-5}$ und $1 - 2\sqrt{-5}$ als Konjugierte nicht zueinander assoziiert sein. Angenommen, die Zahlen 3 und 7 seien zu $1 \pm 2\sqrt{-5}$ assoziiert, dann wären die Brüche $\frac{1\pm2\sqrt{-5}}{3}, \frac{1\pm2\sqrt{-5}}{7} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$. Da aber sowohl die Spur von $\frac{1\pm2\sqrt{-5}}{3}$ als auch von $\frac{1\pm2\sqrt{-5}}{7}$ nicht ganzzahlig sind, können die Elemente $\frac{1\pm2\sqrt{-5}}{3}, \frac{1\pm2\sqrt{-5}}{7}$ somit nicht in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ liegen. Also sind die Zahlen nicht zueinander assoziiert. Folglich liegen für die Zahl 21 zwei verschiedene Primfaktorzerlegungen in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ vor. Wir sehen also, dass der Fundamentalsatz der Zahlentheorie und damit die Eindeutigkeit der Primfaktorzerlegung im Allgemeinen nicht mehr vorausgesetzt werden kann. Mit diesem Problem wollen wir uns Folgenden beschäftigen.

Zusammenfassung

Wir haben im ersten Kapitel den quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ eingeführt und dessen Ganzheitsring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ kennen gelernt. Außerdem wissen wir, dass $\{1, \omega\}$ eine Ganzheitsbasis des Rings $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ist, und dass ein quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ mit der identischen Abbildung und der Konjugationabbildung genau zwei Körperautomorphismen besitzt. Zudem haben wir die wichtigen Begriffe der Norm und Spur eingeführt und die Einheitengruppe $\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{d})}$ imaginärquadratischer Zahlkörper beschrieben.

2 Die Dedekindsche Idealtheorie

Es war der deutsche Mathematiker Peter Dirichlet (1805-1859), der im Jahre 1843 Ernst Eduard Kummer (1810-1893) auf die Nichteindeutigkeit der Primfaktorzerlegung in gewissen Zahlenringen aufmerksam machte. Kummer hatte bei seinem vermeintlichen Beweis zur Fermatschen-Vermutung, welcher die algebraischen Zahlen einbezog, den Hauptsatz der Zahlentheorie auch für alle algebraischen Zahlen als erwiesen angesehen, sodass diese ebenfalls eine eindeutige Zerlegung wie die gewöhnlichen ganzen Zahlen besitzen. Dass dies aber schon im Ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ nicht mehr gegeben ist, hatten wir bereits bei der Zahl 21 gesehen. Geleitet von den komplexen Zahlen bestand Kummers Absicht nun darin einen erweiterten Bereich neuer „***idealer Zahlen***“ zu schaffen, sodass diese sich eindeutig in das Produkt „***idealer Primzahlen***“ zerlegen lassen. Er konnte schließlich mit seiner 1847 veröffentlichten Arbeit *„Über die Zerlegung der aus Wurzeln der Einheit gebildeten komplexen Zahlen in ihre Primfaktoren“* [Wuß,Seite 223] einen Weg aufzeigen, mit der Mehrdeutigkeit der Primfaktorzerlegung umzugehen und eine Analogie zum Hauptsatz der Arithmetik wieder herstellen. Kummer publizierte noch im gleichen Jahr die Arbeit *„Beweis des Fermatschen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl idealer Primzahlen λ“* [Wuß,Seite 223]. Damit zeigte sich, wie wirkungsvoll die idealen Primzahlen beim Grossen-Fermatschen-Satz waren, denn

zuvor konnten EULER, DIRICHLET, LEGENDRE und LAME' lediglich die Primzahlexponenten 3, 5 und 7 abhandeln. Die Entwicklung der Idealtheorie durch EDMUND KUMMER ist bis heute eine der fundamentalsten Errungenschaften in der Geschichte der Zahlentheorie.

Verfolgen wir nun die Kummersche Idealtheorie und versuchen mit Hilfe der idealen Primzahlen in unserem obigen Beispiel im Ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ für die Zahl 21 eine eindeutige Primfaktorzerlegung wieder herzustellen. Es ist $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Setzen sich nun die rechten Faktoren aus idealen Primzahlen $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ zusammen mit

$$3 = \mathfrak{p}_1, \mathfrak{p}_2, \quad 7 = \mathfrak{p}_3, \mathfrak{p}_4, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1, \mathfrak{p}_3, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_2, \mathfrak{p}_4$$

dann erhalten wir die eindeutige Zerlegung: $21 = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4)$ in ideale Primzahlen. Aber was bedeuten nun diese idealen Zahlen und für was stehen sie? Sie sind in jedem Fall keine Zahlen eines erweiterten Ringes von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Die von KUMMER entwickelte Theorie der idealen Zahlen wurde durch den deutschen Mathematiker RICHARD DEDEKIND (1831-1916) systematisiert und man bezeichnet heute die idealen Zahlen einfach als die Dedekindschen *Ideale* des Ringes $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Ziel dieses Kapitels wird es sein, das Fundamentaltheorem der Dedekindschen Idealtheorie zu beweisen. Er ist eine Verallgemeinerung des Satzes der eindeutigen Primfaktorzerlegung. Bevor wir jedoch das Theorem beweisen können, müssen wir noch einige Grundlagen schaffen und neue Techniken sammeln.

Bekanntlich heißt eine nichtleere Teilmenge $\mathfrak{a}$ von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Ideal, wenn $\mathfrak{a}$ eine Untergruppe von $(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}, +)$ ist und für alle $a \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})},\ r \in \mathfrak{a}$ stets folgt $ra \in \mathfrak{a}$. Ist $\mathfrak{a}$ ein Ideal von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, dann schreiben wir kurz $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Ideale, die von einem Element a erzeugt werden, nennt man *Hauptideale*. Diese haben die Gestallt

$$\mathfrak{a} := (a) = a\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \left\{ a\alpha | \alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \right\}$$

und bestehen offensichtlich aus allen vielfachen von a. Insbesondere heißt $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Hauptidealring, wenn jedes Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Hauptideal ist. Unter den Hauptidealringen von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ sind die euklidischen und die faktoriellen Ringe sicherlich am interessantesten. Denn es gilt: „*Jeder euklidische Ring ist ein Hauptidealring*" und „*Jeder Hauptidealring ist faktoriell*", siehe [KaMe, Satz 17.1 und 17.4].Wenn also der Ganzheitsring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ euklidisch ist, dann ist er ein Hauptidealring und somit faktoriell. Für den imaginärquadratischen Fall ($d < 0$) weiß man heute, dass $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ nur für die von GAUSS in Art.303[4] vermuteten Werte

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

[4] „Es scheint kein Zweifel, dass die angegebenen Folgen abbrechen[...]". „Ein strenger beweis dieser Feststellung dürfte jedoch äußerst schwierig sein".

ein Hauptidealring ist. Einen ersten unvollständigen Beweis für die Vermutung lieferte 1952 der deutsche Hobbymathemathematiker KURT HEEGNER (1893-1965). 1967 konnte jedoch der amerikanische Zahlentheoretiker HAROLD MEAD STARK in seiner Arbeit [Michigan Math.J.14,1-27] einen vollständigen Beweis für die Vermutung von GAUSS liefern. Dieser sehr tiefgehende Satz benutzt die Theorie der elliptischen Kurven und eine spezielle Konstruktion von Punkten auf diesen Kurven, die man heute als Heegner Punkte bezeichnet. Für den reellquadratischen Fall ist die Sache jedoch nicht so einfach und es liegen bisher keine ähnlichen Resultate wie für $(d < 0)$ vor. Man weiß jedoch, dass für

$$d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 23, 29, 31, 33,$$
$$37,38,41,43,46,47,53,57,59,61,62,67,69,71,73,77,83,86,89,93,94,97$$

der Ganzheitsring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ faktoriell ist. Und aus den Arbeiten von H. CHATLAND und H.DAVENPORT [Canad.J.Math.2(1950),289-296] erhalten wir die 16 Werte:

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

für die $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ euklidisch ist. Für die Operationen der Addition und Multiplikation auf der Menge der Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gilt, dass die Summe definiert ist durch

$$\mathfrak{a} + \mathfrak{b} := \{a + b | a \in \mathfrak{a},\ b \in \mathfrak{b}\} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

Sie ist das kleinste $\mathfrak{a}$ und $\mathfrak{b}$ umfassende Ideal, also der größte gemeinsame Teiler von $\mathfrak{a}$ und $\mathfrak{b}$. Es ist leicht zu zeigen, dass gilt $\mathfrak{a} + \mathfrak{b} = \text{ggT}(\mathfrak{a}, \mathfrak{b})$, siehe [Schmidt,Satz 6.2.7]. Typischerweise bezeichnet man die Summe von Hauptidealen $(a_1) + \ldots + (a_n)$ mit $(a_1, \ldots, a_n)$. Für die Definition des Produktideals $\mathfrak{ab}$ ist es notwendig alle endlichen Summen von Produkten der Form

$$\mathfrak{ab} := \{\textstyle\sum_i a_i b_i | a_i \in \mathfrak{a},\ b \in \mathfrak{b}\} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$$

zuzulassen, denn die Menge der Produkte $ab,\ a \in \mathfrak{a},\ \text{b} \in \mathfrak{b}$ ist im Allgemeinen kein Ideal. Man verifiziert nun sehr leicht, dass $(a_1, ..., a_n)(b_1, ..., b_n) = (a_1 b_1, ..., a_n b_n)$ gilt, und dass insbesondere $(a)(b) = (ab)$ ist. Der Nachweis folgt einfach aus der Beachtung der Definition des Produktideals und trivialen Äquivalenzumformungen.

Bemerkung 2.1. Die Multiplikation von Idealen ist sowohl kommutativ als auch assoziativ und das neutrale Element ist $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (1)$.

2.1 Normideal

Wir wollen uns nun mit der *Idealnorm* beschäftigen, diese wird im Folgenden eine sehr wichtige Rolle spielen. Dafür definieren wir zu einem Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ deren komplex Konjugiertes Ideal durch

$$\mathfrak{a}' := \{\alpha' | \alpha \in \mathfrak{a}\} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

Man verifiziert ohne Probleme, dass $(\mathfrak{ab})' = \mathfrak{a}'\mathfrak{b}'$ gilt.

Lemma 2.1.1 *Sei $\mathfrak{a}$ ein Ideal von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Dann ist $\mathfrak{a}$ eine endlich erzeugte abelsche Gruppe. Jedes Ideal ist Summe endlich vieler Hauptideale.*

Beweis: Es ist $(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}, +)$ eine endlich erzeugte abelsche Gruppe mit Ganzheitsbasis $\{1, \omega\}$. Daher ist auch jedes Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ als Untergruppe der (additiven) Gruppe $(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}, +)$ endlich erzeugt, denn jede Untergruppe einer endlich erzeugten abelschen Gruppe ist endlich erzeugt, siehe [Schmidt,Satz 5.2.4]. Ist das Ideal $\mathfrak{a}$ durch seine Elemente $a_1, \ldots, a_r$ als abelsche Gruppe erzeugt, dann gilt insbesondere $\mathfrak{a} = (a_1, \ldots, a_r) = (a_1) + \ldots + (a_r)$. □

Ringe, bei denen jedes Ideale endlich erzeugt ist, heißen *Noethersche Ringe*[5]. Insbesondere ist somit $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein noetherscher Ring. In vielen Fällen werden die Eigenschaften noetherschen Ringe ausgenutzt:

Bemerkung 2.1.2. Ist $(0) \neq \mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Ideal mit $\mathfrak{a} = \mathbb{Z}n \oplus \mathbb{Z}v$ und gilt $v = a + m\omega$ mit $m, n \in \mathbb{N}$ minimal und $a \in \mathbb{Z}$, so gelten $m|n \in \mathbb{N}$, $m|a \in \mathbb{Z}$ (also ist $a = mb$ für ein $b \in \mathbb{Z}$) und $n|m \cdot N(b + \omega)$. Insbesondere wird jedes Ideal in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ von höchstens zwei Elementen erzeugt. Ein Ideal $\mathfrak{a}$ besitzt demnach eine $\mathbb{Z}$-Basis der Form $\{n, m(b + \omega)\}$ mit $m|a$. Zum Beweis siehe [Ma,Bem.12.2].

Hauptlemma 2.1.3. *Sei $\mathfrak{a}$ ein von (0) verschiedenes Ideal von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, dann existiert (ein eindeutig bestimmtes) $a \in \mathbb{N}, a > 0$, mit*

$$\mathfrak{a}\mathfrak{a}' = (a) = a\mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

Beweis: Nach Bemerkung 2.1.2 finden wir $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ als Erzeuger für das Ideal $\mathfrak{a}$. Setzen wir $\mathfrak{a} := (\alpha, \beta)$, dann ist $\mathfrak{a}' := (\alpha', \beta')$ und wir erhalten für das Produktideal

$$\mathfrak{a}\mathfrak{a}' = (\alpha, \beta)(\alpha', \beta') = (\alpha\alpha', \alpha'\beta, \alpha\beta', \beta\beta')$$

die vier Erzeuger $\alpha\alpha', \alpha'\beta, \alpha\beta', \beta\beta'$.
Hier folgt nach Lemma 1.3

$$\alpha\alpha' = N(\alpha),\ \beta\beta' = N(\beta) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z} \text{ und } Sp(\alpha\beta') = \alpha\beta' + \alpha'\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$$

Wir setzen nun $a :=\text{ggT}(\alpha\alpha', \beta\beta', \alpha\beta' + \alpha'\beta)$ und behaupten, dass

$$\mathfrak{a}\mathfrak{a}' = a\mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

[5] Benannt nach der deutschen Mathematikerin Amalie Emmy Noether (1882-1935), die heute als Mitbegründerin der modernen Algebra gilt.

Betrachten wir zuerst die Inklusion " $\supseteq$ " Dann ist klar, da $\mathbb{Z}$ ein Hauptidealring ist, dass a eine Linearkombination von $\alpha\alpha', \beta\beta', \alpha\beta' + \alpha'\beta \in \mathfrak{a}\mathfrak{a}'$ mit Koeffizienten in $\mathbb{Z}$ ist. Bleibt noch " $\subseteq$ " zu zeigen. Nun ist per Definition a ein Teiler von $\alpha\alpha', \beta\beta', \alpha\beta' + \alpha'\beta$. Offensichtlich ist $\alpha\alpha', \beta\beta' \in a\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Wir zeigen, dass auch $\alpha'\beta, \alpha\beta' \in a\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ oder äquivalent dazu $x := \frac{\alpha\beta'}{a} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und $x' = \frac{\alpha'\beta}{a} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gilt. Aus der Norm und Spur von x bzw.x' folgt

$$N(x') = N(x) = xx' = \frac{\alpha\alpha'}{a}\frac{\beta\beta'}{a} \in \mathbb{Z} \text{ und } Sp(x') = Sp(x) = x + x' = \frac{\alpha\beta'}{a} + \frac{\alpha'\beta}{a} \in \mathbb{Z}.$$

Nach Lemma 1.3 sind somit $x, x' \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, d.h alle vier Erzeuger sind vielfache von a. Damit erhalten wir $\mathfrak{a}\mathfrak{a}' = a\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und das Lemma ist bewiesen. □

Wir sind nun in der Lage die Norm eines Ideals $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ zu definieren:

$$N(\mathfrak{a}) := a \in \mathbb{N} \setminus \{0\} \quad \Rightarrow \quad \mathfrak{a}\mathfrak{a}' := (N(\mathfrak{a})).$$

Für zwei Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ wird die Idealnorm wegen $(N(\mathfrak{a}\mathfrak{b})) = (\mathfrak{a}\mathfrak{b})(\mathfrak{a}\mathfrak{b})' = (\mathfrak{a}\mathfrak{a}')(\mathfrak{b}\mathfrak{b}') = (N(\mathfrak{a}))(N(\mathfrak{b}))$ multiplikativ. Man verifiziert ebenfalls ohne Probleme

$$N(\mathfrak{a}) = 1 \;\Leftrightarrow\; \mathfrak{a} = 1 \text{ und } N(\mathfrak{a}) = 0 \;\Leftrightarrow\; \mathfrak{a} = 0.$$

Es lassen sich nun einige wichtige Folgerungen aus dem Hauptlemma für die Multiplikation und die Teilbarkeit von Idealen ableiten. So kann beispielsweise die aus der linearen Algebra bekannte Kürzungsregel auch für Ideale verallgemeinert einführen werden. Analog zum Zahlfall sagen wir, auch bei der Teilbarkeit von Idealen, dass ein Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ durch ein Ideal $\mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ teilbar ist, wenn ein Ideal $\mathfrak{c} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ existiert, sodass $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ gilt. Es ist schon bemerkenswert, dass wir an dieser Stelle vom „Kürzen" sprechen dürfen. Denn bisher steht uns zu einem Ideal $\mathfrak{a}$ ja noch kein inverses Ideal $\mathfrak{a}^{-1}$ zur Verfügung. Dass wir es dennoch dürfen, zeigt dass folgende

Korollar 2.1.4

i) *(Kürzungsregel für Ideale). Seien* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *von* (0) *verschiedene Ideale in* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. *Gilt* $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, *dann folgt* $\mathfrak{b} = \mathfrak{c}$.

ii) *Für zwei von* (0) *verschiedene Ideale* $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *gilt* $\mathfrak{a}|\mathfrak{b} \;\Leftrightarrow\; \mathfrak{b} \subseteq \mathfrak{a}$.

Beweis: Zu i) Ist $\mathfrak{a} = (\alpha)$ ein Hauptideal, dann folgt $\alpha\mathfrak{b} = \mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c} = \alpha\mathfrak{c}$. Für jedes $\beta \in \mathfrak{b}$ ist daher $\alpha\beta \in \alpha\mathfrak{c}$ und es existiert folglich ein $\gamma \in \mathfrak{c}$, so dass $\alpha\beta = \alpha\gamma$. Multiplikation beider Seiten der Gleichung mit α^{-1} liefert $\beta = \gamma \in \mathfrak{c}$. Daher ist $\mathfrak{b} \subseteq \mathfrak{c}$, also $\mathfrak{b} = \mathfrak{c}$. Ist $\mathfrak{a}$ ein Hauptideal, dann ist die Kürzungsregel richtig. Ist $\mathfrak{a}$ hingegen ein beliebiges Ideal, dann folgt aus der Gleichung $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ durch Multiplikation beider Seiten mit $\mathfrak{a}'$ und unter Berücksichtigung des Hauptlemmas 2.1.3 die Gleichung $a\mathfrak{b} = \mathfrak{a}\mathfrak{a}'\mathfrak{b} = \mathfrak{a}\mathfrak{a}'\mathfrak{c} = a\mathfrak{c}$. Da in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ aus $ab = ac$ stets $b = c$ folgt, gilt daher $\mathfrak{b} = \mathfrak{c}$.
Zu ii) Aus $\mathfrak{a}$ teilt $\mathfrak{b}$ folgt die Existenz eines Ideals $\mathfrak{c}$ mit $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Da nun $\mathfrak{c} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gilt, folgt $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathfrak{a}$. Ist nun $\mathfrak{b} \subseteq \mathfrak{a}$ gegeben. Dann liefert Multiplikation beider Seiten

der Relation mit $\mathfrak{a}'$ gerade $\mathfrak{a}'\mathfrak{b} \subseteq \mathfrak{a}'\mathfrak{a} = (a)$. Damit folgt, dass a jedes Element von $\mathfrak{a}'\mathfrak{b}$ teilt. D.h. es existiert ein $\mathfrak{c}$ mit $\mathfrak{c} = \frac{1}{a}\mathfrak{a}'\mathfrak{b} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Offensichtlich erfüllt $\mathfrak{c}$ die Eigenschaften eines Ideals und wir erhalten $a\mathfrak{c} = \mathfrak{a}'\mathfrak{b}$ bzw. $\mathfrak{a}'\mathfrak{a}\mathfrak{c} = \mathfrak{a}'\mathfrak{b}$. Aus der Kürzungsregel folgt nun $\mathfrak{a}|\mathfrak{b}$ und damit die Behauptung. □

Bemerkung 2.1.5. Aus Teil i) des Korollars 2.1.4 erhalten wir insbesondere, dass die Ideale von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ eine Halbgruppe mit Kürzungsregel bilden.

2.2 Primideale und Maximalideale

Primideale übernehmen in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ die analoge Rolle, wie die Primzahlen in $\mathbb{Z}$. Wir werden sie daher durch zwei äquivalente Eigenschaften charakterisieren:

Proposition 2.2.1 *Ein Ideal $\mathfrak{p} \neq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ heißt Primideal, wenn die beiden nachfolgenden Bedingungen erfüllt sind.*

i) Für alle Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ mit $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$ folgt stets, $\mathfrak{p}|\mathfrak{a}$ oder $\mathfrak{p}|\mathfrak{b}$.

ii) $\forall a, b \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ mit $a \cdot b \in \mathfrak{p}$ folgt, $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

Beweis: *i)* $\Rightarrow$ *ii)* Sei $a, b \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Ist $a \cdot b \in \mathfrak{p}$ gegeben. Dann impliziert $(a) \cdot (b) \subseteq \mathfrak{p}$ bereits $(a) \subseteq \mathfrak{p}$ oder $(b) \subseteq \mathfrak{p}$ und damit ist $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
ii) $\Rightarrow$ *i)* Wir übersetzen die Teilbarkeit wie nach Korollar 2.1.4 (ii) in Inklusionen. Sei also $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ gegeben und sei $\mathfrak{b} \not\subseteq \mathfrak{p}$. Ist $b \in \mathfrak{b}\backslash\mathfrak{p}$, dann folgt $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ für jedes $a \in \mathfrak{a}$. Dann muss $a \in \mathfrak{p}$ sein und damit $\mathfrak{a} \subseteq \mathfrak{p}$, also $\mathfrak{p}|\mathfrak{a}$. □

Aufgrund der Tatsache, dass $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Integritätsring ist, können wir den Fall $\mathfrak{p} = (0)$ im Gegensatz zu $\mathfrak{p} = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ nicht ausschließen. Denn in der Tat, ist aufgrund der Nullteilerfreiheit das Nullideal stets ein Primideal. Dass die Primideale von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ sehr eng mit den Primzahlen in $\mathbb{Z}$ zusammenhängen, zeigt uns das folgende

Lemma 2.2.2. *Ist $\mathfrak{p} \triangleleft \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein von (0) verschiedenes Primideal. Dann gilt $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p.*

Beweis: Seien $\alpha, \beta \in \mathbb{Z}$ mit $\alpha\beta \in \mathfrak{p} \cap \mathbb{Z}$. Wenn $\mathfrak{p}$ Primideal ist, folgt $\alpha \in \mathfrak{p} \cap \mathbb{Z}$ oder $\beta \in \mathfrak{p} \cap \mathbb{Z}$, wodurch auch $\mathfrak{p} \cap \mathbb{Z}$ Primideal in $\mathbb{Z}$ ist. Noch zu zeigen bleibt, dass $\mathfrak{p} \cap \mathbb{Z}$ nicht das Nullideal ist. Finden wir ein von Null verschiedenes Element in $\mathfrak{p} \cap \mathbb{Z}$, dann sind wir fertig. Sei $\alpha \in \mathfrak{p}$, $\alpha \neq 0$ und sei $f_\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ das Minimalpolynom von α. Da f_α Minimalpolynom ist, folgt $a_0 \neq 0$. Zudem ist $a_0 \in \mathfrak{p} \cap \mathbb{Z}$, da $a_0 \in \mathbb{Z}[\alpha] \subset \mathfrak{p}$. Also haben wir ein von nullverschiedenes Element in $\mathfrak{p} \cap \mathbb{Z}$ gefunden und damit das Lemma bewiesen. □

Eine besonders zentrale Rolle unter den Primidealen nehmen die *Maximalideale* ein. Ein Ideal $\mathfrak{m} \subsetneq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ heißt Maximalideal, wenn es kein Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gibt. Dass

jedes Maximalideal ein Primideal ist, sieht man leicht ein. Denn ist $\mathfrak{m}$ ein Maximalideal und $a, b \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ mit $ab \in \mathfrak{m}$. Ist o.B.d.A. $a \notin \mathfrak{m}$, dann ist das Ideal $\mathfrak{m} + (a)$ echt größer als $\mathfrak{m}$. Wegen der Maximalität von $\mathfrak{m}$ ist dann $\mathfrak{m}+(a) = (1) = \text{ggT}(\mathfrak{m}, (a))$. Daher existiert ein $m \in \mathfrak{m}$ und ein $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, sodass $m+\alpha a = 1$ ist und damit $b = b \cdot 1 = mb+\alpha ab \in \mathfrak{m}$.

Das auch die Umkehrung gilt, ist der Inhalt vom nachfolgenden

Satz 2.2.3. *Jedes von* (0) *verschiedene Primideal* $\mathfrak{p} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *ist maximal.*

Beweis: Nach Lemma 2.2.2 gilt $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p. Betrachten wir nun den injektiven Ringhomomorphismus

$$\mathbb{Z}/p\mathbb{Z} \ \rightarrow \ \mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{p},$$

der durch die Einbettung $\mathbb{Z} \hookrightarrow \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gegeben ist und betrachten $\mathbb{Z}/p\mathbb{Z}$ als Teilring von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{p}$. Sei $\alpha \in \mathfrak{p}, \alpha \neq 0$ und sei $f_\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ das Minimalpolynom von α, dann ist

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Reduzieren wir die Gleichung modulo $\mathfrak{p}$, dann folgt für $\bar{\alpha} = \alpha + \mathfrak{p} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{p}$

$$\bar{\alpha}^n + \bar{a}_{n-1}\bar{\alpha}^{n-1} + \ldots + \bar{a}_1\bar{\alpha} + \bar{a}_0 = 0.$$

wobei $\bar{a}_0, \ldots, \bar{a}_{n-1} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$ die Restklassen der a_i modulo $\mathfrak{p}$, $\mathrm{i} = 0, \ldots, n-1$. Da bekanntlich $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, hat $\bar{\alpha}$ für $\bar{\alpha} \neq 0$ ein Inverses in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{p}$. Denn sei i der erste Index für den gilt, $\bar{a}_i \neq 0$, dann ist $-(\bar{a}_i)^{-1}(\bar{\alpha}^{n-i-1} + \bar{a}_{n-1}\bar{\alpha}^{n-i-2} + \ldots + \bar{a}_{i+1})$ das Inverse zu $\bar{\alpha}$. Damit ist $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{p}$ ein Körper und $\mathfrak{p}$ ein maximales Ideal. □

Wir wollen nun den Hauptsatz der Dedekindschen Idealentheorie beweisen.

Theorem 2.2.4. *Jedes Ideal* $\mathfrak{a} \neq (0)$ *im Ganzheitsring* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *hat eine bis auf die Reihenfolge eindeutige Zerlegung in ein Produkt von Primidealen.*

Beweis: Wir zeigen zunächst, dass für jedes Ideal $\mathfrak{a} \neq (0)$ ein Produkt von Primidealen existiert. Ist $\mathfrak{a}$ nicht selbst maximal, also Primideal, dann ist $\mathfrak{a}$ in einem echt größeren Ideal $\mathfrak{b}$ enthalten, siehe [Wol96, Satz 3.11(4)], also $\mathfrak{a} \subseteq \mathfrak{b}$. Nach Korollar 2.1.4 (ii) folgt dann $\mathfrak{b}|\mathfrak{a}$. Also gibt es ein $\mathfrak{c}$ mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Sind nun $\mathfrak{b}$ und $\mathfrak{c}$ maximal, also Primideale, dann sind wir fertig. Andernfalls machen wir weiter und erhalten, wegen $N(\mathfrak{a}) = N(\mathfrak{b}\mathfrak{c}) = N(\mathfrak{b})N(\mathfrak{c})$ mit $1 < N(\mathfrak{b}), N(\mathfrak{c}) < N(\mathfrak{a})$ etc., dass dieses Prozess nach endlich vielen Schritten abbricht, da die Norm als natürliche Zahl nicht beliebig kein werden kann. Also lässt sich jedes Ideal in ein Produkt von Primidealen zerlegen. Bleibt noch die Eindeutigkeit. Angenommen $\mathfrak{a}$ hätte zwei Primidealzerlegungen. Dann zeigen wir, dass beide bis auf die Reihenfolge identisch sind. Seien also

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{q}_1 \cdots \mathfrak{q}_l$$

zwei Primidealzerlegungen des ganzen Ideals $\mathfrak{a}$. Da $\mathfrak{p}_i, \mathfrak{q}_j$ Primideale sind, teilt o.B.d.A. $\mathfrak{p}_1$, nach Proposition 2.2.1 (i), eines der Primideale im Produkt $\mathfrak{q}_1 \cdots \mathfrak{q}_l$, etwa $\mathfrak{q}_1$. Da Primideale Maximalideale sind, folgt $\mathfrak{p}_1 = \mathfrak{q}_1$. Die Kürzungsregel liefert dann $\mathfrak{p}_2 \cdots \mathfrak{p}_k = \mathfrak{q}_2 \cdots \mathfrak{q}_l$. Nach endlich vielen Wiederholungen erhalten wir schließlich, dass $\mathfrak{p}_k = \mathfrak{q}_l$ gilt. Also stimmen $\mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{q}_1 \cdots \mathfrak{q}_l$ bis auf die Reihenfolge überein und das Theorem ist bewiesen. □

Bemerkung 2.2.5. Das Theorem ist auf andere Ganzheitsringe übertragbar. Die Voraussetzung ist jedoch, dass sich alles nur dort abspielt. Denn in den meisten anderen Ringen ist dennoch keine eindeutige Primidealzerlegung gegeben. Betrachtet man beispielsweise den Ring $\mathbb{Z}\left[\sqrt{-3}\right]$, dann gibt es keine eindeutige Zerlegung in Primideale. Denn es ist $(2)(2) = (1+\sqrt{-3})(1-\sqrt{-3})$ und das Ideal (2) ist *irreduzibel*[6]. Damit kann nicht $(2) = (1+\sqrt{-3})$ sein, da sonst $\frac{1}{2}(1+\sqrt{-3}) \in \mathbb{Z}\left[\sqrt{-3}\right]$ wäre.

Wir interessieren uns nun für die Primidealzerlegung der beiden Hauptidealringe $2\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ und $3\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$. Seien $\mathfrak{p}_1 = (2, 1+\sqrt{-5})$, $\mathfrak{p}_2 = (3, 1-\sqrt{-5})$ und $\mathfrak{p}_3 = (3, 1-\sqrt{-5})$ Primideale in $\mathbb{Z}\left[\sqrt{-5}\right]$. Dann ist

1.
$$\begin{aligned}\mathfrak{p}_1^2 &= (2\cdot 2, 2(1+\sqrt{-5}), 2(1+\sqrt{-5}), -4+2\sqrt{-5}) \\ &= (4, 2(1+\sqrt{-5}), -4+2\sqrt{-5}) \\ &= (2)(2, 1+\sqrt{-5}, -2+\sqrt{-5})\end{aligned}$$

nun ist aber im letzten Ideal $\sqrt{-5} = 2 + (-2+\sqrt{-5})$ und damit auch $1 = (1+\sqrt{-5}) - \sqrt{-5}$ enthalten. Folglich ist $\mathfrak{p}_1^2 = (2)(1) = (2) = 2\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$.

2.
$$\begin{aligned}\mathfrak{p}_2\mathfrak{p}_3 &= (9, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), 6) \\ &= (3)(3, 1+\sqrt{-5}, 1-\sqrt{-5}, 2) \\ &= (3)(1) = (3) = 3\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}\end{aligned}.$$

Wir sehen also, dass die von den Primzahlen in $\mathbb{Z}$ erzeugten Hauptideale keine Primideale bleiben. Zudem kann in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ das Hauptideal $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ in ein Produkt von Primidealen zerfallen oder die Potenz eines einzigen Primideals von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ sein. Für viele Anwendungen ist wichtig zu wissen, auf welche Weise ein Hauptideal in Primideale zerfällt. Das man die Zerlegung von Hauptidealen beschreiben kann, ist der Inhalt des nachfolgenden Abschnitts.

2.3 Zerlegungsgesetz

Dass die Primidealzerlegung eines Hauptideals $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, für eine Primzahl p, nicht willkürlich sein kann, folgt schon aus der Norm $N(p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) = p^2$. D.h. $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ zerfällt entweder

[6] Ein Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ heißt irreduzibel oder unzerlegbar, wenn für $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ mit $\mathfrak{a}|\mathfrak{b}$ stets $\mathfrak{a} = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ oder $\mathfrak{a} = \mathfrak{b}$ gilt.

in ein Primideal oder in das Produkt zweier (nicht notwendigerweise verschiedener) Primideale der Norm p. Eine ungerade Primzahl p heißt in $\mathbb{Q}(\sqrt{d})$

- **träge**, wenn $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathfrak{p}$ ein Primideal ist,
- **zerlegt**, wenn $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathfrak{p}\mathfrak{p}'$ mit Primideale $\mathfrak{p} \neq \mathfrak{p}' \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$,
- **verzweigt**, wenn $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathfrak{p}^2$ für ein Primideal $\mathfrak{p} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Man findet nun ohne großen Aufwand, siehe etwa [StPi,Seite 155], für $d \neq 0, 1$ die *Diskriminante* eines quadratischen Zahlkörpers:

$$\Delta_{\mathbb{Q}(\sqrt{d})} := \begin{cases} 4d, & \textit{falls} \quad d \equiv 2, 3 \bmod 4 \\ d, & \textit{falls} \quad d \equiv 1 \bmod 4 \end{cases}$$

Man Beachte, dass stets $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta_{\mathbb{Q}(\sqrt{d})}})$ gilt.

Mit Hilfe der Diskriminante und des Legende-Symbols können wir eine übersichtliche Beschreibung über das Verhalten von ungraden Primzahlen in einem quadratischen Zahlkörpers geben:

Satz 2.3.1. (Zerlegungsgesetz) *Für eine ungrade Primzahl p in $\mathbb{Q}(\sqrt{d})$gilt:*

- Ist $p|\Delta_{\mathbb{Q}(\sqrt{d})}$, dann ist $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (p, \sqrt{d})^2$ und p ist verzweigt,
- Ist $\left(\frac{\Delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = +1$, dann ist p zerlegt,
- Ist $\left(\frac{\Delta_{\mathbb{Q}(\sqrt{d})}}{p}\right) = -1$, dann ist p träge.

Beweis: Sei zunächst $\delta := \Delta_{\mathbb{Q}(\sqrt{d})}$. Ist $p|\delta$, dann folgt, da p ungrade ist, dass auch $p|d$ ist. Also ist

$$(p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = (p)(p, \sqrt{d}, \tfrac{d}{p}) = (p) = p\mathcal{O}_{\mathbb{Q}(\sqrt{d})},$$

denn aus der Teilerfremdheit von p und $\frac{d}{p}$ folgt, für das Ideal $(p, \sqrt{d}, \frac{d}{p}) = (1)$.
Ist nun $\left(\frac{\delta}{p}\right) = +1$. Dann folgt, dass δ und wegen $\delta = d$ oder $\delta = 4d$, dass auch d quadratischer Rest modulo p ist. Es existiert daher ein $a \in \mathbb{Z}$ mit $a^2 \equiv d \mod p$. Definieren wir $\mathfrak{p} := (p, a + \sqrt{d})$, dann ist

$$\begin{aligned} \mathfrak{p}\mathfrak{p}' &= (p, a + \sqrt{d})(p, a - \sqrt{d}) \\ &= (p^2, p(a + \sqrt{d}), p(a - \sqrt{d}), a^2 - d) \\ &= p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}(p, a + \sqrt{d}, a - \sqrt{d}, \tfrac{a^2-d}{p}). \end{aligned}$$

Nun ist wegen $2\sqrt{d} = a + \sqrt{d} - (a - \sqrt{d})$ und damit auch $4d = (2\sqrt{d})^2$ im letzten Ideal enthalten. Aus der Teilerfremdheit von p und $4d$ erhalten wir schließlich, dass das letzte Ideal der Gleichung das Einsideal ist. Damit folgt $\mathfrak{p}\mathfrak{p}' = p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ mit $\mathfrak{p} \neq \mathfrak{p}'$. Wäre nämlich $\mathfrak{p} = \mathfrak{p}'$, dann folgte wie eben $4d \in \mathfrak{p}$ und $\mathfrak{p} = (1)$ im Widerspruch. Also sind $\mathfrak{p}, \mathfrak{p}'$ verschiedene Primideale. Bleibt noch $\left(\frac{\delta}{p}\right) = -1$ zu zeigen. Angenommen es gäbe ein Ideal $\mathfrak{p}$ der Norm p, dann hätte $\mathfrak{p}$, nach Bemerkung 2.1.2, die Gestalt $\mathfrak{p} = (p, b + \omega)$ und es wäre $p|N(b + \omega)$. Setzen wir nach Korollar 1.5 $\omega = \sqrt{d}$, dann folgt $N(b + \sqrt{d}) = b^2 - d \equiv 0 \mod p$, also erhalten wir die quadratische Kongruenz $b^2 \equiv d \mod p$. Aus dem Legende-Symbol folgt nun, $\left(\frac{\delta}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{d}{p}\right) = +1$ im Widerspruch zur Voraussetzung. Für $\omega = \frac{1}{2}(1 + \sqrt{d})$ verfahren wir analog und erhalten diesmal die quadratische Kongruenz $(2b + 1)^2 \equiv d \mod p$ und wie eben einen Widerspruch zur Voraussetzung. □

Bemerkung 2.3.2. Die Primzahl 2 hatten wir ausgeschlossen. Es gilt aber, dass 2 in $\mathbb{Q}(\sqrt{d})$ träge ist, wenn $d \equiv 5 \bmod 8$. Sie ist zerlegt, wenn $d \equiv 1 \mod 8$, und sie ist verzweigt, falls $d \equiv 2, 3 \mod 4$.

Betrachten wir beispielsweise $\left(\frac{-15}{37}\right)$. Dann erhalten wir durch mehrfache Anwendung des quadratischen Reziprozitätsgesetzes, dass die Primzahl 37 in $\mathbb{Q}(\sqrt{-15})$ träge ist. Denn $\left(\frac{-15}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{3}{37}\right)\left(\frac{5}{37}\right) = (-1)^{18}\left(\frac{1}{8}\right)\left(\frac{2}{5}\right) = 1 \cdot 1 \cdot (-1) = -1$.

Zusammenfassung

Wir haben in diesem Kaptitel ideale Zahlen und ideale Primzahlen kennen gelernt. Mit Hilfe des Normideals konnten wir den Hauptsatz der Dedekindschen Idealentheorie beweisen, d.h. im Ganzheitsring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ist die Primidealzerlegung eindeutig. Zudem bilden Ideale in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ eine Halbgruppe mit Kürzungsregel und Primzahlen sind in $\mathbb{Q}(\sqrt{d})$ verzweigt, zerlegt oder träge, je nachdem ob $\left(\Delta_{\mathbb{Q}(\sqrt{d})} \middle/ p\right) = 0, +1$ oder -1 ist.

3 Die Idealklassengruppe

Wir wollen nun auf der Menge der Ideale eine mit der Idealmultiplikation verträglich Äquivalenzrelation einführen. Dabei heißen zwei von (0) verschiedene Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ äquivalent (im Zeichen $\mathfrak{a} \sim \mathfrak{b}$), wenn es von Null verschiedene Elemente $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gibt mit $\mathfrak{a}\alpha = \beta\mathfrak{b}$. Man rechnet nun leicht nach, dass Reflexivität, Symmetrie und Transitivität erfüllt sind, also tatsächlich eine Äquivalenzrelation gegeben ist. Die Menge der Äquivalenzklassen bzgl. $\sim$ ist definiert durch

$$Cl_{\mathbb{Q}(\sqrt{d})} := \left\{ [\mathfrak{a}] \,|\, \mathfrak{a} \triangleleft \mathcal{O}_{\mathbb{Q}(\sqrt{d})}, \mathfrak{a} \neq (0) \right\},$$

und heißt die *Idealklasse* der von (0) verschiedenen Ideale $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Das diese Menge eine abelsche Gruppe bildet ist der Inhalt vom nachfolgenden

Satz 3.1. *Die Idealklassen $Cl_{\mathbb{Q}(\sqrt{d})}$ bilden bezüglich der Idealmultiplikation $(\mathfrak{a},\mathfrak{b}) \to \mathfrak{a}\cdot\mathfrak{b}$ eine abelsche Gruppe. Das neutrale Element von $Cl_{\mathbb{Q}(\sqrt{d})}$ ist die Klasse der Hauptideale $\left[\mathcal{O}_{\mathbb{Q}(\sqrt{d})}\right] = [1]$.*

Beweis: Aus den Äquivalenzrelationen $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{c} \sim \mathfrak{d}$ folgt, $\mathfrak{a}\alpha = \beta\mathfrak{b}$ und $\mathfrak{c}\gamma = \lambda\mathfrak{d}$ mit$\alpha,\beta,\lambda,\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Damit erhalten wir $\mathfrak{a}\mathfrak{c}\alpha\gamma = \beta\mathfrak{b}\mathfrak{c}\gamma = \beta\lambda\mathfrak{b}\mathfrak{d}$. Also ist $[\mathfrak{a}\mathfrak{c}] = [\mathfrak{b}\mathfrak{d}]$ und somit die Verknüpfung der Idealklassen wohldefiniert. Assoziativ- und Kommutativgesetz gelten, denn nach Bemerkung 2.1 gelten sie schon für die Idealmultiplikation. Klar ist danach auch, dass $\left[\mathcal{O}_{\mathbb{Q}(\sqrt{d})}\right]$ das neutrale Element von $Cl_{\mathbb{Q}(\sqrt{d})}$ ist. Nun folgt aus dem Hauptlemma 2.1.3, dass $\mathfrak{a}\mathfrak{a}' = (a)$ für $a \in \mathbb{N}, a > 0$ ein Hauptideal ist. Dies impliziert $[\mathfrak{a}]\,[\mathfrak{a}'] = \left[\mathcal{O}_{\mathbb{Q}(\sqrt{d})}\right] = [1]$, denn die Klasse des Hauptideals (a) ist gerade das neutrale Element von $Cl_{\mathbb{Q}(\sqrt{d})}$. Also folgt die Existenz des Inversen mit $[\mathfrak{a}'] = [\mathfrak{a}]^{-1}$. □

Damit bilden die Idealklassen eine abelsche Gruppe, die so genannte *Idealklassengruppe* $Cl_{\mathbb{Q}(\sqrt{d})}$ von $\mathbb{Q}(\sqrt{d})$. Diese ist neben der Einheitengruppe die wichtigste Invariante eines Zahlkörpers. Die Ordnung von $Cl_{\mathbb{Q}(\sqrt{d})}$ heißt die *Klassenzahl* von $\mathbb{Q}(\sqrt{d})$ und wird mit $h_{\mathbb{Q}(\sqrt{d})} := \#Cl_{\mathbb{Q}(\sqrt{d})}$ bezeichnet. Das wesentliche Ziel dieses Kapitels ist es, die Endlichkeit der Idealklassengruppe eines quadratischen Zahlkörpers zu beweisen. Es ist aber eine bemerkenswerte Tatsache, dass in allen Ganzheitsringen die Klassenzahl endlich ist. Da die Idealklassengruppe eine zentrale Invariante des Ganzheitsrings $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ist, misst sie im gewissen Sinne die Größe, wie weit dieser davon abweicht, ein Hauptidealring zu sein, d.h. um wie viel komplizierter die Arithmetik beim Übergang von Zahlen zu Idealen wird. Ist $h_{\mathbb{Q}(\sqrt{d})} = 1$, dann ist jedes Ideal ein Hauptideal und damit $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Hauptidealring, siehe [Art98,Seite490]. Insbesondere ist für $h_{\mathbb{Q}(\sqrt{d})} = 1$, der Satz der eindeutigen Primzerlegung im klassischen Sinne erfüllt. Mit Hilfe der Klassenzahlberechnung haben wir also die Möglichkeit zu entscheiden, ob ein gegebener Ganzheitsring ein Hauptidealring ist oder nicht. Um die Endlichkeit der Idealklassengruppe beweisen zu können, müssen wir zeigen, dass jede Idealklasse ein Ideal mit beschränkter Norm besitzt. Wir führen zunächst den Begriff des primitiven Ideals ein. Ein Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ heißt primitives Ideal, wenn es durch kein Ideal der Form $(m) \neq (1)$ mit $m \in \mathbb{Z}$ teilbar ist. Offenbar wird jede Idealklasse von einem primitiven Ideal erzeugt. Nach Bemerkung 2.1.2 besitzt ein Ideal $\mathfrak{a}$ eine $\mathbb{Z}$-Basis der Form $\{n, m(b+\omega)\}$ mit $m|a$. Insbesondere ist $\mathfrak{a}$ primitiv genau dann, wenn $m = 1$ ist, d.h. ist $\mathfrak{a}$ primitiv, dann gibt es $n \in \mathbb{N}$ und $b \in \mathbb{Z}$ mit $\mathfrak{a} = n\mathbb{Z} \oplus (b+\omega)\mathbb{Z}$ und es gilt $N(\mathfrak{a}) = n$.

Theorem 3.2. *Sei $d \in \mathbb{Z}\setminus\{0,1\}$ quadratfrei und wie oben $\Delta_{\mathbb{Q}(\sqrt{d})}$ die Diskriminante des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ mit Ganzheitsring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega]$. Die Gauß-Schranke $\mu_{\mathbb{Q}(\sqrt{d})}$ ist gegeben durch*

$$\mu_{\mathbb{Q}(\sqrt{d})} := \begin{cases} \sqrt{\frac{\Delta_{\mathbb{Q}(\sqrt{d})}}{5}}, & \textit{falls} \quad \Delta_{\mathbb{Q}(\sqrt{d})} > 0, \\ \sqrt{\frac{-\Delta_{\mathbb{Q}(\sqrt{d})}}{3}}, & \textit{falls} \quad \Delta_{\mathbb{Q}(\sqrt{d})} < 0. \end{cases}$$

Dann enthält jede Idealklasse von $\mathbb{Q}(\sqrt{d})$ ein von (0) verschiedenes ganzes Ideal mit Norm $\leq \mu_{\mathbb{Q}(\sqrt{d})}$. Insbesondere ist die Anzahl $h_{\mathbb{Q}(\sqrt{d})}$ aller Idealklassen endlich.

Beweis: Sei $a = [\mathfrak{a}]$ eine von einem Ideal $\mathfrak{a}$ erzeugte Idealklasse. Und sei o.B.d.A $\mathfrak{a}$ ein primitives Ideal. Es ist also $\mathfrak{a} = (\alpha, \beta)$ mit $N(\mathfrak{a}) = \alpha$ und $\beta = b + \omega = s + \frac{1}{2}\sqrt{\Delta_{\mathbb{Q}(\sqrt{d})}}$ für ein $s \in \mathbb{Q}$ mit $2s \in \mathbb{Z}$. Ist nun $\alpha^2 \leq \mu_{\mathbb{Q}(\sqrt{d})}$ dann sind wir fertig, ansonsten liefert der euklidische Algorithmus für das Paar (s, α) ein $q \in \mathbb{Z}$ mit $s - q\alpha = r$ und

$$\begin{aligned} |r| &\leq \tfrac{\alpha}{2} \quad \textit{falls} \quad \Delta_{\mathbb{Q}(\sqrt{d})} < 0, \\ \tfrac{\alpha}{2} \leq |r| &\leq \alpha \quad \textit{falls} \quad \Delta_{\mathbb{Q}(\sqrt{d})} > 0. \end{aligned}$$

Setzen wir $\beta_1 := r + \frac{1}{2}\sqrt{\Delta_{\mathbb{Q}(\sqrt{d})}}$, dann erhalten wir die Abschätzung

$$\beta_1 \in \mathfrak{a}, \ \ |N(\beta_1)| \leq \tfrac{1}{4}(\alpha^2 - \Delta_{\mathbb{Q}(\sqrt{d})}) < \alpha^2.$$

Denn für $\Delta_{\mathbb{Q}(\sqrt{d})} < 0$ ist $|N(\beta_1)| = \left| r^2 - \frac{\Delta_{\mathbb{Q}(\sqrt{d})}}{4} \right| \leq \frac{\alpha^2 + |\Delta_{\mathbb{Q}(\sqrt{d})}|}{4} < 1$, da $\alpha^2 > \mu_{\mathbb{Q}(\sqrt{d})} = \frac{|\Delta_{\mathbb{Q}(\sqrt{d})}|}{3}$. Während für $\Delta_{\mathbb{Q}(\sqrt{d})} > 0$ gilt, dass $-\alpha^2 = \frac{\alpha^2 - 5\alpha^2}{4} < r^2 - \frac{\Delta_{\mathbb{Q}(\sqrt{d})}}{4} < \alpha^2$ ist. Damit ist $\mathfrak{a}_1 := \frac{1}{\alpha}\beta_1'\mathfrak{a} \sim \mathfrak{a}$ ein ganzes Ideal mit $[\mathfrak{a}_1] = [\mathfrak{a}]$ und $N(\mathfrak{a}_1) < N(\mathfrak{a})$. Iteration dieses Schritts liefert, nach endlich vielen Wiederholungen, ein Ideal mit Norm $\leq \Delta_{\mathbb{Q}(\sqrt{d})}$, denn nach jedem Schritt wird die Norm um mindestens 1 kleiner, d.h., wir sind nach endlich vielen Schritten fertig. Bleibt noch zu zeigen, dass das Ideal $\mathfrak{a}_1$ ganz ist. Es ist $\frac{1}{\alpha}\beta_1'\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \ \Leftrightarrow \ \beta_1'\mathfrak{a} \subseteq \alpha\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (\alpha) = \mathfrak{a}\mathfrak{a}'$. Die Kürzungsregel liefert dann das gewünschte mit $(\beta_1') \subseteq \mathfrak{a}'$. □

Wenn wir uns den Beweis anschauen, stellen wir fest, dass der wesendliche Punkt darin besteht, dass jede Idealklasse ein ganzes Ideal mit beschränkter Norm enthält. Dabei erweist sich die Kenntnis einer möglichst kleinen Schranke, wie etwa der Gauss-Schranke, bei der expliziten Berechnung der Klassenzahl als äußerst effizient. Denn umso kleiner eine Schranke ist, um so weniger Ideale müssen auf Äquivalenz geprüft werden. In der Literatur findet man häufig, anstatt der Gauß-Schranke, die so genannte Minkowski[7]-Schranke:

$$c_{\mathbb{Q}(\sqrt{d})} := \tfrac{1}{2}\left(\tfrac{4}{\pi}\right)^s \sqrt{\left|\Delta_{\mathbb{Q}(\sqrt{d})}\right|},$$

wobei $s = 0$ für $\Delta_{\mathbb{Q}(\sqrt{d})} > 0$ und $s = 1$ für $\Delta_{\mathbb{Q}(\sqrt{d})} < 0$ ist. Mittels der Minkowski-Theorie („Geometrie der Zahlen“) kann ebenfalls die Endlichkeit der Idealklassen bewiesen werden. Der Aufwand dazu ist jedoch bei weitem höher und kann daher hier nicht behandelt werden, wir verweisen auf [Neu,§4-6].

[7] Hermann Minkowski (1846-1909) war ein deutscher Mathematiker und Physiker, der unter anderen große Dienste zur Relativitätstheorie leistete.

Bemerkung 3.3. Ist $\mu_{\mathbb{Q}(\sqrt{d})} \leq 2$, dann ist $h_{\mathbb{Q}(\sqrt{d})} = 1$. Beweis: Nach Voraussetzung enthält jede Idealklasse ein ganzes von (0) verschiedenes Ideal $\mathfrak{a}$ mit Norm < 2, also $N(\mathfrak{a}) = 1$, und damit ist $\mathfrak{a} = \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (1)$, d.h. die Idealklasse enthält das Einsideal.

Theorem 3.2 legt uns folgende Vorgehensweise zur Bestimmung der Klassenzahlen nahe. Zuerst bestimmen wir alle Ideale $\mathfrak{a} \neq (0)$ mit Norm $N(\mathfrak{a}) \leq \mu_{\mathbb{Q}(\sqrt{d})}$. Sinnvollerweise sucht man zunächst alle Primideale mit dieser Eigenschaft, was im Wesentlichen auf Primidealzerlegung führt. Unter diesen sortieren wir nun alle Hauptideale aus, und überprüfen den Rest modulo Hauptideale.

Beispiel 3.4. Wir bestimmen die Klassenzahl von $\mathbb{Q}(\sqrt{-15})$. Da $-15 \equiv 1 \mod 4$ folgt $\Delta_{\mathbb{Q}(\sqrt{-15})} = d = -15$. Die Gauss-Schranke ist $\mu_{\mathbb{Q}(\sqrt{-15})} = \sqrt{\frac{|-15|}{3}}$, d.h. wir haben Ideale der Norm ≤ 2 zu untersuchen. Aus Bemerkung 2.3.2 folgt wegen $-15 \equiv 1 \mod 8$, dass die Primzahl 2 in $\mathbb{Q}(\sqrt{-15})$ zerlegt ist. Also gibt es zwei ganze Ideale $\mathfrak{p}, \mathfrak{p}'$ mit Norm 2, nämlich die zwei Primteiler von $2\mathcal{O}_{\mathbb{Q}(\sqrt{-15})}$. Wenn diese Hauptideale wären, dann müsste ihre Norm gleichzeitig mit dem Normbetrag einer Zahl $b \in \mathcal{O}_{\mathbb{Q}(\sqrt{-15})}$ übereinstimmen. Nach Korollar 1.5 hat jedes $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{-15})}$ die Form $\alpha = \frac{1}{2}(a + b\sqrt{-15})$, $a, b \in \mathbb{Z}$. Dann ist $N(\alpha) = \frac{a^2+15b^2}{4}$ und es folgt sofort, dass die Gleichung $\frac{a^2+15b^2}{4} = 2$ in den ganzen Zahlen keine Lösung hat. Also können $\mathfrak{p}, \mathfrak{p}'$ keine Hauptideale sein und damit gilt $[\mathfrak{p}], [\mathfrak{p}'] \neq [1]$. Zu überprüfen bleibt noch, ob die Ideale $\mathfrak{p}, \mathfrak{p}'$ Äquivalent modulo Hautideale sind. Ist $c = \frac{1+\sqrt{-15}}{2}$, dann ist $c' = \frac{1-\sqrt{-15}}{2}$. Nun gilt $cc' = 4 = 2^2$. Aus der Eindeutigkeit der Primidealzerlegung folgt nun, dass $\mathfrak{p}^2 = c\mathcal{O}_{\mathbb{Q}(\sqrt{-15})}$ und $\mathfrak{p}'^2 = c'\mathcal{O}_{\mathbb{Q}(\sqrt{-15})}$ gelten muss. D.h., dass die Idealklassen $[\mathfrak{p}]$ und $[\mathfrak{p}']$ beide die Ordnung zwei in $Cl_{\mathbb{Q}(\sqrt{-15})}$ haben, denn sowohl $\mathfrak{p}^2$ als auch $\mathfrak{p}'^2$ sind beides Hauptideale. Aus $\mathfrak{p}\mathfrak{p}' = 2\mathcal{O}_{\mathbb{Q}(\sqrt{-15})}$ folgt nun, dass $[\mathfrak{p}] = [\mathfrak{p}']$ ist, denn es ist $[\mathfrak{p}] = [\mathfrak{p}]^{-1}$. Also hat $Cl_{\mathbb{Q}(\sqrt{-15})}$die Klassenzahl 2.

Im Allgemeinen wird es jedoch sehr schwierig sein die Klassenzahl eines quadratschen Zahlkörpers zu bestimmen, denn die Überprüfung der Äquivalenz ist bei großen Diskriminanten äußerst aufwändig. In solchen Fällen wird man sich Algorithmen bedienen oder ganz auf ein Computeralgebrasystem zurückgreifen [StPi,19]. In der Arbeit von Karl Schaffstein [Schaff] findet man eine Auflistung der Klassenzahlen reellquadratischer Zahlkörper für Primzahldiskriminante unter 12000. Interessant ist, dass die meisten dieser Zahlkörper die Klassenzahl 1 haben. Bis heute ist es jedoch unklar, ob es unendlich viele reellquadratischer Zahlkörper mit Klassenzahl 1 gibt. Es ist noch nicht einmal bekannt, ob überhaupt unendlich viele Zahlkörper mit Klassenzahl 1 existieren. In dem Buch von Paulo Ribenboim [Ri,§3,Seite149] findet man einen bemerkenswerten Satz, der einen Zusammenhang von primzahlerzeugenden Polynomen und Klassenzahlen quadratischer Zahlkörper angibt.

Satz 3.5. *Sei p eine Primzahl und $f_p(X) = X^2 + X + p$. Die folgenden Bedingungen sind äquivalent:*

- $p = 2, 3, 5, 11, 17, 41$.

- $\mathbb{Q}(\sqrt{1-4p})$ *hat Klassenzahl* 1.

Der Satz zeigt einen ersten engen Zusammenhang zwischen den Primzahlen und Klassenzahlen quadratischer Zahlkörper.

3.1 Binäre quadratische Formen

Im fünften Abschnitt der Disquisitiones Arithmeticae systematisierte Gauss die Resultate von Euler, Legendre und Lagrange und entwickelte eine ausgiebige Theorie, die weit darüber hinausgeht, was seine Vorgänger geleistet hatten. So teilt Gauss die binären quadratischen Formen mit gleicher Diskriminante in Klassen $h(D)$ ein und Dirichlet und Dedekind konnten zeigen, dass diese Einteilung genau den Idealklassen quadratischer Zahlkörper entspricht. Die Theorie der binär quadratischen Formen wird in der elementaren Zahlentheorie ausgiebig behandelt. Die nachfolgenden Sätze findet man unter andern in [SchFr,273 pp] oder [Sa,Ka.5]

Eine binäre quadratische Form (oder einfach nur Form)[8]

$$f : \mathbb{Z}^2 \to \mathbb{Z}, \;\; (x,y) \;\mapsto\; ax^2 + bxy + cy^2 \text{ mit } a,b,c \in \mathbb{Z}$$

ist ein homogenes Polynom vom Grad 2 mit den Unbestimmten x und y. Die Abkürzung $Q := \langle a,b,c\rangle$ beschreibt die Abhängigkeit der Form f von ihren Koeffizienten. Die Diskriminante von Q ist definiert über $D = \delta_f := b^2 - 4ac$. Ist $\delta_f < 0$, dann nimmt Q nur positive Werte für $a > 0$ bzw. nur negative Werte für $a < 0$ an. In diesem Fall heißt Q *positiv* bzw. *negativ definit*. Ist $\delta_f > 0$, dann nimmt Q positive und negative Werte an und heißt *indefinit*. Für $D < 0$ genügt es positiv definite Formen zu betrachten, da die negativ definiten Formen aus den positiv definiten durch Multiplikation mit -1 hervorgehen. Eine Form heißt primitiv oder einfach, wenn zusätzlich $\mathrm{ggT}(a,b,c) = 1$ gilt. Die beiden Formen $x^2 + 5y^2$ und $2x^2 + 2xy + 3y^2$ sind primitiv und ihre Diskriminante ist -20. Für eine beliebige Diskriminante $D < 0$ mit $D \equiv 0,1 \mod 4$ sei $\mathcal{Q}_D$ die Menge aller primitiven Formen, d.h.

$$\mathcal{Q} := \bigcup \{\mathcal{Q}_D | D \equiv 0,1 \; mod \; 4\}$$

Die Elemente(Formen) der Menge $\mathcal{Q}_D$ lassen sich nun wie folgt in zwei Hauptformen einteilen:

$$f(x,y) := \begin{cases} x^2 - \frac{D}{4}y^2, & falls \quad D \equiv 0 \bmod 4 \\ x^2 + xy + \frac{1-D}{4}y^2, & falls \quad D \equiv 1 \bmod 4 \end{cases}$$

Man nennt D eine Fundamentaldiskriminante, wenn jede Form mit Diskriminante D primitiv ist. Offensichtlich passiert dies genau dann, wenn

[8] In Zukunft schreiben wir statt binär quadratischer Form einfach nur Form und meinen ohne o.B.d.A. dasselbe.

$$D \equiv \begin{cases} 1 \bmod 4 & \text{mit} \quad D \quad \textit{quadratfrei} \\ 0 \bmod 4 & \text{mit} \quad D = 4D' \quad \textit{quadratfrei und} \quad D' \equiv 2, 3 \bmod 4 \end{cases}$$

Zwei quadratische Formen f und g heißen *echt äquivalent* (oder *isomorph*), wenn ihre zugehörigen symmetrischen Matrizen

$$F = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \text{ und } G = \begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix}$$

durch eine *unimodulare*[9] Transformation auseinander hervorgehen. Also wenn eine Matrix $T \in SL_2(\mathbb{Z})$ mit $\det(T) = 1$ existiert, sodass gilt $G = T^t FT$. Wobei wir im Gegensatz zur *gewöhnlichen Äquivalenz* die Determinante -1 nicht zu lassen. Man zeigt ohne Probleme, dass die Äquivalenz von Formen eine Äquivalenzrelation auf der Menge aller binär quadratischen Formen definiert: $f \sim g$. Insbesondere notieren wir

Lemma 3.1.1. *Für (echt) äquivalente Formen f und g gilt:*

1. *f und g haben dieselbe Wertemenge für $x, y \in \mathbb{Z}$.*
2. *f und g haben dieselbe Diskriminante: $\delta_f = \delta_g$.*

Der Begriff, der echten Äquivalenz, wurde von Gauss eingeführt und spielt bei der Komposition von Formklassen eine wichtige Rolle. Einer der wichtigsten Sätze in der Theorie der binär quadratischen Formen ist der Reduktionssatz von Lagrange.

Satz 3.1.2. *Jede positiv, definite quadratische Form f ist (echt) äquivalent zu genau einer Form $f(x, y) = a_0x^2 + b_0xy + c_0y^2 \in \mathbb{Z}[x, y]$ mit*

$$-a_0 < b_0 \leq a_0 < c_0 \textit{ oder } 0 \leq b_0 \leq a_0 = c_0.$$

Eine Form, die eine der beiden Relationen genügen, nennt man eine *reduzierte* positiv definite Form mit Diskriminante D. Nun folgt aus der Ungleichung von Satz 3.1.2, $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$, also ist $a \leq \sqrt{-D/3}$. Und da die Wertemenge für b beschränkt ist, und c für a, b, D eindeutig bestimmt, erhalten wir

Satz 3.1.3. *Die Klassenzahl $h(D)$ der echten Äquivalenzklassen positiv, definiter primitiver Formen mit Diskriminante $D < 0$ in $\mathbb{Z}[x, y]$ ist endlich.*

Insbesondere enthält jede Klasse positiv definiter primitiver Formen genau eine reduzierte Form. Für $D = -3$ erhalten wir beispielsweise $a = 1$ und zudem $b = \pm 1$. Also die beiden Formen

$$f_1(x, y) = x^2 + xy + y^2 \text{ bzw. } f_2(x, y) = x^2 - xy + y^2.$$

[9] Man nennt eine Matrix $T \in SL_2(\mathbb{Z})$ unimodular, wenn $\det(T) = 1$.

Da nun $f_1(x,y) = f_2(-x,y)$ gilt, sind beide Formen echt äquivalent, d.h. es gibt für $D=-3$ genau eine Äquivalenzklasse quadratischer Formen. Damit gilt für die Klassenzahl $h(-3)=1$. Gauss selbst hat bereits Klassenzahlen für $|D|<10000$ bestimmt. Er hatte aber im Gegensatz zur Definition von Legendre nur die Formen

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

mit geraden mittleren Koeffizienten betrachtet, also nur solche Formen $f(x,y)$ mit $D \equiv 0 \mod 4$.

E. Landau[10] konnte zudem in seiner Arbeit [La1903] folgendes Beweisen

Für eine natürliche Zahl n ist die Klassenzahl $h(-4n)=1 \quad \Leftrightarrow \quad n \in \{1,2,3,4,7\}$.

In dem Buch [Cox,Seite29] von David A. Cox ist die folgende kleine Auflistung von reduzierten quadratischen Formen mit negativer Diskriminante D und zugehöriger Klassenzahl zu finden.

D	$h(D)$	Reduzierte Formen mit Diskriminante D
-3	1	x^2+xy+y^2
-4	1	x^2+y^2
-8	1	x^2+2y^2
-12	1	x^2+3y^2
-20	2	$x^2+5y^2, 2x^2+2xy+3y^2$
-28	1	x^2+7y^2
-56	4	$x^2+14y^2, 2x^2+7y^2, 3x^2 \pm 2xy + 5y^2$
-108	3	$x^2+27y^2, 4x^2 \pm 2xy + 7y^2$
-256	4	$x^2+64y^2, 4x^2+4xy+17y^2, 5x^2 \pm 2xy + 13y^2$

Tabelle 1: Diskriminante, Klassenzahl, reduzierte quadratische Formen

Eine der fundamentalsten Endeckungen in der Zahlentheorie ist ohne Zweifel der Zwei-Quadrate-Satz und die Frage, welche natürlichen Zahlen m sich als Summe von zwei Quadraten darstellen lassen. Pierre de Fermat erkannte, dass der entscheidende Weg zur Lösung des Problems mittels Primzahlen[11] in den Griff zu bekommen sein müsste und stellte um 1640 die Frage, welche Primzahlen sich als Summe zweier Quadrate darstellen lassen:

$$p = x^2 + y^2,\ x,y \in \mathbb{Z}$$

[10] Edmund Landau (1877-1939) war ein deutscher Mathematiker, der unter anderem durch Arbeiten zu Primzahlen bekannt wurde. Empfehlenswert ist das Handbuch der Lehre von der Verteilung der Primzahlen

[11] Ohne Einschränkungen strechen wir nur von positiven Primzahlen.

Nach systematischem Probieren fand Fermat schnell die folgende Liste

Ohne Lösung: $3, 7, 11, 19, 23, 31, 43, 47, 59, 67, \ldots$
Mit Lösung: $5 = 2^2 + 1^2,\ 13 = 3^2 + 2^2,\ 17 = 4^2 + 1^2,\ 29 = 5^2 + 2^2,\ \ldots$

Fermat vermutete, dass eine Primzahl p genau dann Summe zweier Quadrate $x^2 + y^2$ ist, wenn $p = 2$ oder $p \equiv 1 \mod 4$. Hundert Jahre später publizierte Euler den erste Beweis dieser Vermutung:

Für jede Primzahl p, ist die Form $x^2 + y^2$,$x, y \in \mathbb{Z}$ *genau dann erfüllt, wenn* $p = 2$ *oder* $p \equiv 1 \mod 4$ *ist.*

Mit Hilfe des Legende-Symbols kann die Bedingung wie folgt ausdrückt werden mit $(-1/p) = +1$. Alle Formen mit Diskriminante $D = -8$, bilden eine einzige Klasse, da nur eine primitive, reduzierte Form mit $x^2 + 2y^2,\ x, y \in \mathbb{Z}$ vorhanden ist, siehe Tabelle 1. Fragen wir nun nach allen durch diese Form darstellbaren ungeraden Zahlen $m \in \mathbb{N}$, dann ist die erste Bedingung, dass -2 ein quadratischer Rest von m sein muss. Dazu ist erforderlich und hinreichend, dass jede in m aufgehende Primzahl p der Legendre Bedingung $(-2/p) = +1$ genügt. Also ist $p \equiv 1, 3 \mod 8$. D.h. für jede Primzahl p lässt sich durch die Form $x^2 + 2y^2,\ x, y \in \mathbb{Z}$ genau dann darstellen, wenn $p = 2$ oder $(-2/p) = +1$ bzw. $p \equiv 1, 3 \mod 8$. Analog erhalten wir zur Diskriminante $D = -12$ die einzige primitive, reduzierte Form mit $x^2 + 3y^2,\ x, y \in \mathbb{Z}$. Jede Primzahl p mit $p = 3$ oder $(-3/p) = +1$ bzw. $p \equiv 1 \mod 3$ lässt sich über diese darstellen.

3.2 Die Form $x^2 + 5y^2$

Betrachten wir nun die Determinante $D = -20$. Dann gibt es die primitiven, reduzierten Formen mit x^2+5y^2 und $2x^2+2xy+3y^2$ wobei $x, y \in \mathbb{Z}$. Beide Formen können nicht (echt) äquivalent sein, denn für $x = 1$ und $y = 0$ ist 1 ein Wert der ersten aber nicht der zweiten Form. Suchen wir wieder nach allen ungerade, durch 5 nicht teilbaren, natürlichen Zahlen m, welche sich durch die Formen darstellen lassen, dann ist eine erforderliche Bedingung, dass jede in m aufgehende Primzahl p der Legendre Bedingung $(-5/p) = +1$ genügen muss. Also solche Primzahlen, für die gilt $p \equiv 1, 3, 7, 9 \mod 20$. Es bleibt jedoch unklar, durch welche der reduzierten Formen eine Darstellung der Primzahlen erfolgt. 1744 vermutete Euler, aufgrund experimentellen Untersuchungen[12], dass die Form $x^2 + 5y^2$ genau die Primzahlen p darstellt, für die $p = 5$ oder $p \equiv 1, 9 \mod 20$ gilt. Euler war jedoch nicht in der Lage diese Vermutung zu beweisen, und in der Tat ist sie ein Spezialfall des von Euler gefundenen quadratischen Reziprozitätsgesetzes, welches 1801 von Gauss bewiesen wurde. Ähnliche Probleme werden immer dort auftreten, wo es nicht äquivalente Formen mit gleicher Diskriminante gibt. Die Vermutung Eulers, ist ein Spezialfall der

[12] Veröffentlicht in seiner Arbeit von 1744 Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum, Opera Omnia (1) 2, Seite 194-222.

Geschlechtertheorie, mit der wir uns im nächsten Kapitel beschäftigen werden.

Zusammenfassung

Wir haben in diesem Kapitel auf die Menge der ganzen Ideale eine, mit der Idealmultiplikation, verträgliche Äquivalenzrelation eingeführt, wobei von (0) verschiedene Ideale $\mathfrak{a}$ und $\mathfrak{b}$ äquivalent heißen, wenn es $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \setminus \{0\}$ gibt mit $\mathfrak{a}\alpha = \mathfrak{b}\beta$. Die Äquivalenzklassen heißen Idealklassen und bilden bezüglich der Idealmultiplikation eine endlich abelsche Gruppe. Die Klassenzahl $h_{\mathbb{Q}(\sqrt{d})}$ ist ein Maß für die Nichteindeutigkeit der Faktorzerlegung von Elementen in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Und nur für $h_{\mathbb{Q}(\sqrt{d})} = 1$ ist der Ring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Hauptidealring. Wir haben einige wichtige Sätze und Definitionen aus der Theorie der binär quadratischen Formen wiederholt und gesehen, dass es bei nicht äquivalenten Formen mit gleicher Diskriminante zu Problemen bei der Darstellbarkeit von Primzahlen kommen kann.

4 Komposition und Geschlechter

Einer der wichtigsten Beiträge die Gauss zur Theorie der binären quadratischen Formen geleistet hat, ist die der Komposition von Formen bzw. Formklassen. Legendre hatte diese bereist als einen Spezialfall umschrieben.

Eine quadratische Form F ist *Komposition* zweier Formen f_1 und f_2, wenn ganzzahlige *Bilinearformen*

$$B_i(x, y, z, w) = a_i xz + b_i xw + c_i yz + e_i yw, \qquad i = 1, 2$$

existieren, sodass $f_1(x, y)f_2(z, w) = F(B_1(x, y, z, w), B_2(x, y, z, w))$ für alle $x, y, z, w \in \mathbb{Z}$ gilt.

Die Wichtigkeit der Komposition für das Darstellungsproblem fällt sofort auf. Denn wird eine Zahl n durch eine Form f_1 und eine Zahl m durch eine andere Form f_2 dargestellt, und ist F die Komposition der Formen f_1 und f_2, dann stellt F das Produkt nm dar. Nun ist die Komposition zweier Formen nicht eindeutig bestimmt, denn im allgemeinen besitzen zwei quadratische Formen f_1, f_2 viele verschiedene Kompositionen. Zudem ist die Komposition in dieser Form nicht geeignet, um auf der Menge der Äquivalenzklassen eine Gruppenstruktur zu definieren, denn es ist sehr wahrscheinlich, dass zwei Kompositionen F_1, F_2 von f_1, f_2 in zwei verschiedene Äquivalenzklassen fallen. Für dieses Problem führte Gauss den Begriff der *direkten Komposition* ein. Ist F Komposition von f_1, f_2 und sind $a_1, b_1, \ldots, e_2 \in \mathbb{Z}$ die Koeffizienten der Bilinearformen B_1, B_2, dann gilt

$$a_1b_2 - a_2b_1 = \pm f_1(1, 0), \qquad a_1c_2 - a_2c_1 = \pm f_2(1, 0).$$

Nun ist die Komposition direkt, wenn beide Gleichungen mit ‘+‘ erfüllt sind. Dieser Kompositionsbegriff definiert auf der Menge der Äquivalenzklassen eine Gruppenstruktur.

4.1 Komposition von echten Äquivalenzklassen primitiver Formen

In der Disquisitiones Arithmeticae behandelt Gauss die Theorie der Kompositionen in den Art.234-245. Zu Beginn schreibt er, dass es sich dabei um einen „anderen sehr wichtigen, bisher noch von niemanden berührten Gegenstand“ handele. Die nachfolgende Definition der *Komposition von Formen* geht auf Gauß zurück.

Definition 4.1.1. *Die Form F heißt aus den Formen f_1 und f_2 komponiert, wenn es ganze Zahlen $p, p', p'', p''', q, q', q'', q'''$ mit*

$$\mathrm{ggT}(pq' - qp', pq'' - qp'', pq''' - qp''', p'q'' - q'p'', p'q''' - q'p''', p''q''' - q''p''') = 1$$

gibt, sodass

$$F(pxx' + p'xy' + p''yx' + p'''yy', qxx' + q'xy' + q''yx' + q'''yy') = f_1(x, y)f_2(x', y')$$

mit ganzen Zahlen x, x', y, y'.

Die Formen f_1 und f_2 unterliegen keinen Einschränkungen, d.h. insbesondere können somit die Diskriminanten verschieden sein. Nun leitet Gauss zunächst sechs Folgerungen her [DA,Art.235], und zeigte exemplarisch [DA,Art.236], wie sich F aus f_1 und f_2 berechnen lässt. Danach beweist er in vier Sätzen [DA,Art.237-240] unter anderem, dass die *Komposition als Verknüpfung der Formklassen* angesehen werden kann, weil die Form F nur bis auf Äquivalenz bestimmt ist und weil das Komponieren von Formen, die zu f_1 bzw. f_2 äquivalent sind, eine Form aus der Äquivalenzklasse von F ergibt. Als ein Nebenergebnis leitete Gauss zudem das Kommutativgesetz und Assoziativgesetz ab. Bei weiteren Untersuchungen verwendete Gauss nur Formen mit derselben Diskriminante und erreichte schließlich durch einfache Einschränkungen, dass die Form F gleiche Diskriminante hat wie die komponierten Formen f_1 und f_2. Somit konnte er die Koeffizienten von $F := \langle a_3, b_3, c_3\rangle$ aus denen von $f_1 := \langle a_1, b_1, c_1\rangle$ und $f_2 := \langle a_2, b_2, c_2\rangle$ berechnen und damit zeigen, dass es zu jeder beliebigen Diskriminante eine reduzierte Form („Hauptform“) gibt, sodass diese mit einer beliebigen Form f mit derselben Diskriminante komponiert eine zu f äquivalente Form ergibt. Damit liefert die Komposition einer primitiven Form $\langle a, b, c\rangle$ mit $\langle a, -b, c\rangle$ immer eine zur Hauptform äquivalente Form. Fasst man alles zusammen, dann hatte Gauss gerade gezeigt, dass die Klassen der primitiven Formen mit gegebener Diskriminante D zusammen mit der Komposition, welche mit beliebigen Repräsentanten der Klasse auszuführen sind, eine im heutigen Sinne endlich abelsche Gruppe bilden. Die so genannte *Klassengruppe* zur Diskriminante D. Basierend auf den Veröffentlichungen der Disquisitiones Arithmeticae gelang es Dirichlet, die Arbeiten von Gauss zu vereinfachen und in vielen Teilen zu erweitern. Unter anderem entwickelte er 1839 eine analytische Methode zur Bestimmung der Anzahl von echten Äquivalenzklassen primitiver Formen einer gegebenen Diskriminante. Wir geben im Sinne von Dirichlet [Di] das folgende

Theorem 4.1.2. *Es seien $f_1 := \langle a_1, b_1, c_1\rangle$ und $f_2 := \langle a_2, b_2, c_2\rangle$ zwei primitive, positiv definite Formen mit negativer Diskriminante $D \equiv 0, 1 \mod 4$. Ist ϕ:=ggT(a_1, a_2, q) mit $q := \frac{b_1+b_2}{2}$ und sind $u, v, w \in \mathbb{Z}$, die die Linearkombination $a_1u + a_2v + qw = \phi$ erfüllen, dann stellt $F := \langle a_3, b_3, c_3\rangle$ mit*

$$\begin{cases} a_3 := \frac{a_1 a_2}{\phi^2} \\ b_3 := b_2 + 2\frac{a_2}{\phi} \bmod\Big((q - b_2)v - c_2 w, \frac{a_1}{\phi}\Big) \\ c_3 := \frac{b_3^2 - D}{4a_3} \end{cases}$$

eine aus f_1 *und* f_2 *komponierten Form mit Diskriminante* D *dar. Die Kompositionen von Formen, welche zu* f_1 *bzw.* f_2 *äquivalent sind, ergibt eine primitive, positive definite Form aus der echten Äquivalentsklasse von* F*. Die Menge* $C(D)$ *dieser Formenklassen zusammen mit der durch Komposition beliebiger Repräsentanten der Klasse erklärten Verknüpfungen stellt eine endlich abelsche Gruppe da, deren Ordnung die Klassenzahl* $h(D)$ *ist und deren neutrales Element diejenigen Klasse ist, die die Hauptform*

$$\begin{array}{ll} x^2 - \frac{D}{4}y^2, & \textit{falls} \quad D \equiv 0 \bmod 4 \\ x^2 + xy + \frac{1-D}{4}y^2 4, & \textit{falls} \quad D \equiv 1 \bmod 4 \end{array}$$

enthält, und bei der die Klasse mit der reduzierten Form $\langle a, b, c\rangle$ *zu der Klasse mit der Form* $\langle a, -b, c\rangle$ *invers ist.*

Wir haben oben bereits gesehen, dass es für das Darstellungsproblem immer günstig ist, wenn für die Klassenzahl $h(D) = 1$ gilt. In diesem Fall besitzt die Klasse genau eine reduzierte Form und wir können Primzahlen, die durch diese Dargestellt werden eindeutig zuordnen. Leider ist dies aber nun äußerst selten der Fall. Landau hatte gezeigt, dass $h(-4n) = 1$ genau dann erfüllt ist, wenn $n = \{1, 2, 3, 4, 7\}$ gilt. Um nun über Klassenzahlen $h(D) > 1$ etwas aussagen zu können, müssen wir neben der Einteilung von quadratischen Formen in Äquivalenzklasse eine gröbere Einteilung definieren. Dazu aber gleich mehr.

Da die Elemente der Klassengruppe $C(D)$ mit Ordnung ≤ 2 eine wichtige Rolle spielen werden geben wir den nachfolgende Satz an, der Auskunft über die Anzahl der Element mit Ordnung ≤ 2 aus der Klassengruppe $C(D)$ gibt. Einen schönen Beweis dieser Aussage findet man unter anderem in [Cox, Po.3.11].

Satz 4.1.3. *Ist* r *die Anzahl der verschiedenen Primteiler der Diskriminante* D *von* $\mathbb{Q}(\sqrt{d})$*. Dann hat die Klassengruppe* $C(D)$ *genau* 2^{r-1} *Elemente der Ordnung* ≤ 2*.*

Bemerkung 4.1.4. Die Elemente aus $C(D)$ mit Ordnung ≤ 2 lassen sich einfach bestimmen, denn eine reduzierte Form $f(x, y) = ax^2 + bxy + cy^2$ mit Diskriminante D hat in der Klassengruppe $C(D)$ genau dann Ordnung ≤ 2, wenn $b = 0, a = b$ oder $a = c$ gilt. Siehe dazu etwa die Ausführungen in [Cox,La.3.10].

4.2 Klassenzahl im engeren Sinne

Durch Ergänzungen zu DIRICHLETS Arbeiten *„Vorlesung über Zahlentheorie“* gelang es DEDEKIND eine durchschaubare Interpretation der Kompositionen von echten Äquivalenzklassen primitiver Formen zu präsentieren und somit eine Verbindung zwischen Formen und Idealen in quadratischen Zahlkörpern herzustellen. Um auf den Zusammenhang zwischen Formen und Idealen in quadratischen Zahlkörper eingehen zu können beginnen wir mit der folgenden

Bemerkung 4.2.1. Sei $\mathbb{Q}(\sqrt{d})$ reellquadratisch. Dann heißt ein $\alpha \in \mathbb{Q}(\sqrt{d})^\times$ *total positiv* (im Zeichen $\alpha \gg 0$), wenn $\alpha > 0$ und $\alpha' > 0$ gilt. Während in imaginärquadratischen Zahlkörpern alle von 0 verschiedenen Elemente total positiv sind. α heißt total negativ, wenn $-\alpha$ total positiv ist. Für α' schreiben wir auch in manchen Fällen α^σ, wobei $\sigma : \sqrt{d} \mapsto -\sqrt{d}$ die in Kapitel 1 bestimmte Konjugationsabbildung von $\mathbb{Q}(\sqrt{d})$ ist.

Wir erinnern uns, dass zwei von (0) verschiedene Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ äquivalent im „gewöhnlichen Sinne“ heißen, wenn es von Null verschiedene Elemente $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gibt mit $\mathfrak{a}\alpha = \beta\mathfrak{b}$. Sie heißen nun äquivalent im „engeren Sinne“ (im Zeichen $\mathfrak{a} \overset{+}{\sim} \mathfrak{b}$), wenn $\mathfrak{a} = \lambda\mathfrak{b}$ für ein $\lambda \gg 0$ ist. Die beiden Äquivalenzbegriffe fallen für imaginärquadratische Zahlkörper zusammen, denn dort sind alle Zahlen $\neq 0$ total positiv. Die Menge der Äquivalenzklassen im engeren Sinne wird mit $Cl^+_{\mathbb{Q}(\sqrt{d})}$ bezeichnet und ihre Ordnung $h^+_{\mathbb{Q}(\sqrt{d})}$ heißt die Klassenzahl im engeren Sinne. Betrachten wir die von dem Ideal $(\sqrt{d})$ mit $d > 0$ erzeugte Idealklasse, dann ist diese ganz offensichtlich ein Hauptideal im gewöhnlichen Sinne. Aber ein Hauptideal im engeren Sinne ist sie nur dann, wenn es ein $\lambda \gg 0$ gibt, sodass $(\sqrt{d}) = \lambda\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ gilt, d.h., wenn das Ideal von einem total positiven Element erzeugt wird. Nun ist aber die Zahl $\alpha = \sqrt{d}$ wegen $\alpha' = -\sqrt{d}$ nicht total positiv. Wir sehen also, dass in reellquadratischen Zahlkörpern die Äquivalenzbegriffe verschieden sein können. Um nun die Unterschiede bzw. Gemeinsamkeiten zu untersuchen betrachten wir als erstes die Abbildung:

$$Cl^+_{\mathbb{Q}(\sqrt{d})} \to Cl_{\mathbb{Q}(\sqrt{d})} : \ [\mathfrak{a}]^+ \ \mapsto \ [\mathfrak{a}]$$

und ordnen der von $\mathfrak{a}$ erzeugten Idealklasse $[\mathfrak{a}]^+$ im engeren Sinne die Idealklasse $[\mathfrak{a}]$ im gewöhnlichen Sinne zu. Die Umkehrabbildung:

$$Cl_{\mathbb{Q}(\sqrt{d})} \to Cl^+_{\mathbb{Q}(\sqrt{d})} : \ [\mathfrak{a}] \ \mapsto \ [\mathfrak{a}]^+$$

ist im Allgemeinen nicht wohldefiniert, da $\mathfrak{a} \sim \mathfrak{b}$ sein kann, ohne dass $\mathfrak{a} \overset{+}{\sim} \mathfrak{b}$ gilt, d.h. die Abbildung $Cl^+_{\mathbb{Q}(\sqrt{d})} \to Cl_{\mathbb{Q}(\sqrt{d})}$ ist ein surjektiver Homomorphismus mit einem Kern, der aus einem oder zwei Elementen besteht. Wir können somit $Cl_{\mathbb{Q}(\sqrt{d})}$ nicht als Untergruppe von $Cl^+_{\mathbb{Q}(\sqrt{d})}$ auffassen. Genauere Auskunft gibt die folgende

Proposition 4.2.2. *Es sei* $\left\langle \sqrt{d} \right\rangle$ *die Untergruppe* $\left\{ 1, \left[(\sqrt{d}) \right]^+ \right\}$ *der Klassengruppe* $Cl^+_{\mathbb{Q}(\sqrt{d})}$ *im engeren Sinne. Dann ist die folgende Sequenz endlich abelscher Gruppen exakt:*

$$1 \longrightarrow \left\langle \sqrt{d} \right\rangle \xrightarrow{\kappa} Cl^+_{\mathbb{Q}(\sqrt{d})} \xrightarrow{\pi} Cl_{\mathbb{Q}(\sqrt{d})} \longrightarrow 1$$

Beweis: Es folgt sofort, dass $\kappa : \left\langle \sqrt{d} \right\rangle \to Cl^+_{\mathbb{Q}(\sqrt{d})}$ injektiv, $\pi : Cl^+_{\mathbb{Q}(\sqrt{d})} \to Cl_{\mathbb{Q}(\sqrt{d})}$ surjektiv und dass $Bild(\kappa) \subseteq Kern(\pi)$ ist. Zu zeigen bleibt lediglich, dass $Kern(\pi) \subseteq Bild(\kappa)$. Und das geht wie folgt. Sei $[\mathfrak{a}]^+ \in Kern(\pi)$. Dann ist $\mathfrak{a} = \alpha \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ für ein $\alpha \in \mathbb{Q}(\sqrt{d})^\times$. Ist zudem $N(\alpha) > 0$, dann können wir $\alpha \gg 0$ wählen und finden $[\mathfrak{a}]^+ = 1$. Ist aber $N(\alpha) < 0$, beispielsweise mit $\alpha > 0$ und $\alpha^\sigma < 0$, dann ist $\frac{\alpha}{\sqrt{d}} \gg 0$, also $[\mathfrak{a}]^+ = \left[(\sqrt{d}) \right]^+$. In beiden Fällen erhalten wir $[\mathfrak{a}]^+ \in Bild(\kappa)$. □

Dieses wichtige Ergebnis, bildet in Dedekinds Auslegungen das Gegenstück zur Endlichkeit der echten Äquivalenzklassen, was wir in Kürze sehen werden.

Aus dem obigen Homomorphismus folgt $h_{\mathbb{Q}(\sqrt{d})} \leq h^+_{\mathbb{Q}(\sqrt{d})} \leq 2h_{\mathbb{Q}(\sqrt{d})}$. Genauere Auskunft über den Zusammenhang zwischen der gewöhnlichen Klassenzahl und der Klassenzahl im engeren Sinne gibt das folgende

Korollar 4.2.3. *Für* $d < 0$ *gilt* $h^+_{\mathbb{Q}(\sqrt{d})} = 2h_{\mathbb{Q}(\sqrt{d})}$. *In Fall* $d > 0$ *sei* ε *eine Grundeinheit. Dann gilt*

$$h^+_{\mathbb{Q}(\sqrt{d})} := \begin{cases} h_{\mathbb{Q}(\sqrt{d})} & , \quad falls \quad N(\varepsilon) = -1 \\ 2h_{\mathbb{Q}(\sqrt{d})} & , \quad falls \quad N(\varepsilon) = +1 \end{cases}$$

Beweis: Wir wissen, dass im imaginärquadratischen Fall jedes Element eine positive Norm hat. Wohingegen es im reellquadratischen Fall immer Elemente mit negativer Norm gibt. Nach Proposition 4.2.2 erhalten wir, dass $h^+_{\mathbb{Q}(\sqrt{d})} = h_{\mathbb{Q}(\sqrt{d})}$ genau dann gilt, wenn die Idealklasse $\left[(\sqrt{d}) \right]^+$ trivial ist. Nun ist $(\sqrt{d})$ ein Hauptideal im engeren Sinne genau dann, wenn es eine Einheit $\upsilon \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$ gibt, sodass $\upsilon\sqrt{d} \gg 0$. Ist $d < 0$, dann können wir $\upsilon = 1$ wählen. Ist hingegen $d > 0$ und $\upsilon\sqrt{d} \gg 0$, dann zeigt $N(\sqrt{d}) < 0$, dass $N(\upsilon) < 0$ sein muss, also $N(\upsilon) = -1$. Es gilt daher $\left[(\sqrt{d}) \right]^+ = 1$ genau dann, wenn, es eine Einheit υ mit Norm -1 gibt. Eine solche existiert genau dann, wenn die Grundeinheit ε die Norm -1 hat. □

4.3 Geschlechter

In den Art.228-265 entwickelte Gauss die Geschlechtertheorie als die Theorie der Geschlechter quadratischer Formen. Eine der größten Errungenschaften, die Gauss zu

Geschlechtertheorie leistete, ist ohne zweifel die Berechnung der Anzahl der Geschlechter von Formen mit gegebener Diskriminante D. Er konnte schließlich zeigen, dass ihre Anzahl gleich 2^{r-1} ist, wobei r die Anzahl der in D enthaltenen Primfaktoren bezeichnet. Darüber hinaus wies er nach, dass 2^{r-1} stets ein Teiler der (echten) Äquivalenzklassen von primitiv, positiv definiten Formen mit Diskriminante D ist. Ist die Einteilung in Idealklassen im engeren Sinne feiner als die im gewöhnlichen, dann ist die Einteilung in Geschlechter sehr grob. Wir werden die Geschlechtertheorie mit Idealklassen anstatt wie Gauss mit Formen behandeln. Alle Überlegungen werden für reell- bzw. imaginärquadratische Zahlkörper mit Diskriminante D durchgeführt. Hauptziel wird es sein, die Korrespondenz zwischen Idealen und Formen zu beweisen. Man nennt zwei von (0) verschiedene Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *ähnlich* (im Zeichen $\mathfrak{a} \overset{+}{\approx} \mathfrak{b}$), wenn $N(\mathfrak{a}) = N(\lambda)N(\mathfrak{b})$ für ein von 0 verschiedenes $\lambda \in \mathbb{Q}(\sqrt{d})^{\times}$ mit $\lambda \gg 0$ gilt. Die zugehörigen Äquivalenzklassen nennt man *Geschlechter.* Insbesondere bildet die Menge aller Geschlechter eine abelsche Gruppe, die so genannte *Geschlechterklassengruppe* $Cl^{+}_{gen}(\mathbb{Q}(\sqrt{d}))$. Das Einselement von $Cl^{+}_{gen}(\mathbb{Q}(\sqrt{d}))$ nennt man das *Hauptgeschlecht.* Es ist dasjenige, welches die Hauptideale im engeren Sinne enthält. Ideale, welche im engeren Sinne äquivalent sind, gehören offenbar zu demselben Geschlecht, wenn sie zu d prim sind. In Anlehnung an [Za,§12,Satz1] sind Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ genau dann ähnlich, wenn sie zum selben Geschlecht gehören, wenn sich also ihre Idealklassen im engeren Sinne um ein Quadrat unterscheiden, d.h., es gilt

$$\mathfrak{a} \overset{+}{\approx} \mathfrak{b} \quad \Leftrightarrow \quad \mathfrak{a} \overset{+}{\sim} \mathfrak{b}\mathfrak{c}^2$$

für ein Ideal $\mathfrak{c} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Wir sehen also, dass die Geschlechterklassengruppe $Cl^{+}_{gen}(\mathbb{Q}(\sqrt{d}))$ isomorph ist zu C_+/C_+^2, d.h. $Cl^{+}_{gen}(\mathbb{Q}(\sqrt{d})) \simeq C_+/C_+^2$, wobei $C_+ := Cl^{+}_{\mathbb{Q}(\sqrt{d})}$ die Idealklassengruppe im engeren Sinne bezeichnet.

Bemerkung 4.3.2. Man kann zeigen, dass die Gruppe C_+/C_+^2 wiederum isomorph zu $(\mathbb{Z}/2\mathbb{Z})^{r-1}$ ist, wobei r die Anzahl der verschiedenen Primteiler von D bezeichne. Insbesondere ist die Klassenzahl $h(D)$ teilbar durch die Anzahl $\mathfrak{A}(D)$ der Geschlechter. Wir halten daher fest,

Theorem 4.3.3. *In einem quadratischen Zahlkörper mit Diskriminante D ist die Anzahl der Geschlechter gleich 2^{r-1} und die Anzahl der Klassen in jedem Geschlecht ist $\mathfrak{K}(D) = \frac{h(D)}{2^{r-1}}$. Wobei r die Anzahl der verschiedenen Primteiler von D bezeichne.*

Der Beweis dieser wichtigen Eigenschaft ist ziemlich kompliziert. Wir verweisen auf [Za,§12, Seite112] oder [He,§48,Satz145].

Wir wollen nun auf den Zusammenhang von echten Äquivalenzklassen primitiver Formen und den Äquivalenzklassen von Idealen im engeren Sinne eingehen, d.h. auf die Korres-

pondenz zwischen Idealen und Formen. Beim Beweis des nachfolgenden Satzes halte ich mit im Wesentlichen an das Buch [Za,Seite 92 pp].

Theorem 4.3.4. *Sei $D \equiv 0,1 \mod 4$ (D kein Quadrat) eine Fundamentaldiskriminante. Dann gibt es eine bijektive Korrespondenz zwischen den echten Äquivalenzklassen bijektiv quadratischer Formen mit Diskriminante D und den Äquivalenzklassen im engeren Sinne von Idealen von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Insbesondere ist die Anzahl $h^+_{\mathbb{Q}(\sqrt{d})}$ der Äquivalenzklassen von Idealen im engeren Sinne gleich der Klassenzahl $h(D)$.*

Beweis: Sei $\mathfrak{a}$ ein von (0) verschiedenes Ideal von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, so ist $\lambda \in \mathfrak{a}$ und wegen $(\lambda) \subseteq \mathfrak{a}$ folgt nach Korollar 2.1.4, dass $\mathfrak{a}|(\lambda)$, also auch $N(\mathfrak{a})|N(\lambda)$. Damit nimmt die Abbildung

$$\phi : \mathfrak{a} \to \mathbb{Q}\,, \qquad \phi(\mathfrak{a}) = \tfrac{N(\lambda)}{N(\mathfrak{a})}$$

Werte in $\mathbb{Z}$ an. Nach Bemerkung 2.1.2 besitzt $\mathfrak{a}$ eine Basis $\{\alpha, \beta\}$. Damit ist $\mathfrak{a} = \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \simeq \mathbb{Z}^2$ und es lässt sich ϕ als Funktion f auf $\mathbb{Z}^2$ auffassen:

$$f(x,y) = \phi(x\alpha + y\beta) = \tfrac{(x\alpha+y\beta)(x\alpha'+y\beta')}{N(\mathfrak{a})} = \tfrac{N(\alpha)}{N(\mathfrak{a})}x^2 + \tfrac{\alpha\beta'+\alpha'\beta}{N(\mathfrak{a})}xy + \tfrac{N(\beta)}{N(\mathfrak{a})}y^2$$

Wir erhalten also eine binäre quadratische Form:

$$f(x,y) = ax^2 + bxy + cy^2 \;\text{ wobei }\; a := \frac{N(\alpha)}{N(\mathfrak{a})},\; b := \frac{\alpha\beta' + \alpha'\beta}{N(\mathfrak{a})},\; c := \frac{N(\beta)}{N(\mathfrak{a})} \tag{2}$$

Für die Diskriminante findet man leicht

$$b^2 - 4ac = \frac{(\alpha\beta' + \alpha'\beta)^2 - 4N(\alpha)N(\beta)}{N(\mathfrak{a})^2} = \frac{(\alpha\beta' - \alpha'\beta)^2}{N(\mathfrak{a})^2} = \frac{D(\mathfrak{a})}{N(\mathfrak{a})^2} = D, \tag{3}$$

wobei die Diskriminante $D(\mathfrak{a})$ definiert ist als das Quadrat der Determinante von $\begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}$.
Nun sind sowohl $a = \frac{N(\alpha)}{N(\mathfrak{a})}$,$c = \frac{N(\beta)}{N(\mathfrak{a})} \in \mathbb{Z}$, also auch $D = b^2 - 4ac \in \mathbb{Z}$ und damit auch $b \in \mathbb{Z}$. Somit besitzt die Form f ganzzahlige Koeffizienten und Diskriminante D. Ist nun $\{\alpha_1, \beta_1\}$ eine weitere Basis von $\mathfrak{a}$, dann hängen $\{\alpha, \beta\}$ und $\{\alpha_1, \beta_1\}$ durch die Matrix $T = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ mit Determinante $ps - qr = \pm 1$ zusammen. Aus der obigen Abbildung ϕ erhalten wir die zur Basis $\{\alpha_1, \beta_1\}$ gehörende Form f_1, indem wir (x, y) durch $(px+qy, rx+sy)$ transformieren. Wir haben im Abschnitt 3.1 nur echte Äquivalenzen von Formen definiert, d.h. nur solche, die durch unimodulare Transformationen auseinander hervorgehen. Um diese wünschenswerte Eigenschaft auch für die obigen Basen zu erreichen, stellen wir an diese eine zusätzliche Forderung, um nur solche Matrizen beim Basiswechsel zu erhalten. Eine Basis $\{\alpha, \beta\}$ von $\mathfrak{a}$ heißt *positiv orientiert*, wenn für die rationale Zahl $\frac{\alpha'\beta - \alpha\beta'}{\sqrt{D}} > 0$ gilt. Diese Betrachtung ist zweckmäßig, da $\left(\frac{\alpha'\beta-\alpha\beta'}{\sqrt{D}}\right)^2 = \frac{D(\mathfrak{a})}{D} = N(\mathfrak{a})^2$ sowohl positiv als auch reell ist. Damit hat die Matrix eines Basiswechsels zwischen positiv orientierten Basen immer die Determinante +1. Lässt man also nur positiv orientierte

Basen zu, dann hängt die von oben definierte Form $f(x,y) = ax^2+bxy+cy^2$ bis auf echter Äquivalenz nur vom Ideal $\mathfrak{a}$ und nicht von der Basiswahl ab. Ersetzen wir nun das Ideal $\mathfrak{a}$ durch $(\tau)\mathfrak{a}$ mit $\tau \in \mathbb{Q}(\sqrt{d})$ und $N(\tau) > 0$, dann ist $(\tau\alpha, \tau\beta)$ eine positiv orientierte Basis für $(\tau)\mathfrak{a}$ und $N((\tau)\mathfrak{a}) = |N(\tau)|\, N(\mathfrak{a}) = N(\tau)N(\mathfrak{a})$. Damit stimmt die zum Ideal $(\tau)\mathfrak{a}$ gehörende Form

$$(x,y) \mapsto \tfrac{N(x\tau\alpha+y\tau\beta)}{N((\tau)\mathfrak{a})} = \tfrac{N(\tau)N(x\alpha+y\beta)}{N(\tau)N(\mathfrak{a})} = \tfrac{N(x\alpha+y\beta)}{N(\mathfrak{a})}$$

mit der Form f überein. Es kann also in eindeutiger Weise jeder Idealklasse im engeren Sinne eine echte Äquivalenzklasse von binär quadratischen Formen mit Diskriminante D zugeordnet werden. Können wir zeigen, dass die Zuordnung bijektiv ist, dann sind wir fertig. Sei also

$$f(x,y) = ax^2 + bxy + cy^2, \quad a,b,c, \in \mathbb{Z}\ , \ \ b^2 - 4ac = D$$

eine quadratische Form mit Diskriminante D. Nun ist D eine Fundamentaldiskriminante, also ist $\mathrm{ggT}(a,b,c) = 1$ und damit f eine primitive Form. Sei zunächst $a > 0$. Dann erhalten wir als Lösung der quadratischen Gleichung $az^2 - bz + c = 0$ die Nullstellen $z_1 = \frac{b+\sqrt{D}}{2a}$, $z_2 = \frac{b-\sqrt{D}}{2a}$.

Nun ist $\mathfrak{a} = \mathbb{Z} \oplus \mathbb{Z}z$. Wir zeigen, dass $\mathfrak{a}$ ein ganzes Ideal ist. Ist nun $\tau = \frac{u+v\sqrt{d}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ mit $u, v \in \mathbb{Z}$, $u \equiv vD \bmod 2$ und $\alpha = x + yz \in \mathfrak{a}$ dann ist

$$\begin{aligned}
\tau\alpha &= \left(\tfrac{u+v\sqrt{d}}{2}\right)\left(x + \tfrac{yb+y\sqrt{d}}{2a}\right) \\
&= \tfrac{xu}{2} + \tfrac{ybu}{4a} + \tfrac{yvD}{4a} + \left(\tfrac{xv}{2} + \tfrac{ybv}{4a} + \tfrac{uy}{4a}\right)\sqrt{D} \\
&= \tfrac{xu}{2} + \tfrac{ybu}{4a} + \tfrac{yv(b^2-4ac)}{4a} + \left(\tfrac{xv}{2} + \tfrac{ybv}{4a} + \tfrac{uy}{4a}\right)(2az - b) \\
&= \left(x\tfrac{u-vb}{2} - yvc\right) + \left(xva + y\tfrac{u+vb}{2}\right)z,
\end{aligned}$$

und damit $\mathbb{Z} \oplus \mathbb{Z}z$. Zudem gilt: $b^2 \equiv D \mod 4a \ \Rightarrow\ b \equiv D \bmod 2 \ \Rightarrow\ u \equiv vD \equiv vb \bmod 2$. Aus $\frac{z_1-z_2}{2a} > 0$ erhalten wir, dass die Basis $\{1, z\}$ positiv orientiert ist. Das Ideal $\mathfrak{a}$ hat die Diskriminante

$$D(\mathfrak{a}) = \det\begin{pmatrix} 1 & z_1 \\ 1 & z_2 \end{pmatrix}^2 = (z_1 - z_2)^2 = \tfrac{D}{a^2},$$

und da wie in (3) gesehen $\frac{D(\mathfrak{a})}{N(\mathfrak{a})^2} = D$ gilt, folgt $N(\mathfrak{a}) = \frac{1}{a}$. Wir erhalten also für die zum Ideal $\mathfrak{a}$ zugehörige Form

$$(x,y) \mapsto \tfrac{N(x+yz)}{N(\mathfrak{a})} = \tfrac{x^2+\frac{b}{a}xy+\frac{c}{a}y^2}{\frac{1}{a}} = f(x,y).$$

Ist hingegen $\mathfrak{a}$ ein Ideal mit positiv orientierter Basis $\{\alpha, \beta\}$ mit $N(\alpha) > 0$, dann erhalten wir mit den Substitutionen für a, b, c wie in (2)

$$\begin{aligned}
\tfrac{b+\sqrt{D}}{2a} &= \tfrac{\alpha\beta'+\alpha'\beta+N(\mathfrak{a})\sqrt{D}}{2N(\alpha)} \\
&= \tfrac{\alpha\beta'+\alpha'\beta+(\alpha'\beta-\alpha\beta')}{2N(\alpha)} = \tfrac{\beta}{\alpha}\ .
\end{aligned}$$

Damit ist also $\mathbb{Z} \oplus \mathbb{Z}\frac{b+\sqrt{D}}{2a} = \mathbb{Z} \oplus \mathbb{Z}\frac{\beta}{\alpha} = (\alpha^{-1})\mathfrak{a}$ zum Ideal $\mathfrak{a}$ Äquivalent im engeren Sinne. Sei nun $a < 0$, also $D > 0$. Ist nun $\mathbb{Z}\tau \oplus \mathbb{Z}\tau z$ ein Ideal mit $\tau \in \mathbb{Q}(\sqrt{D})$ und $N(\lambda) < 0$. Dann ist $\{\lambda, \lambda z\}$ eine positiv orientierte Basis. Die zum Ideal $\mathfrak{a}$ gehörende Form ist also wiederum f. Insbesondere liefert jedes Ideal $\mathfrak{a}$ mit positiv orientierter Basis $\{\alpha, \beta\}$ und $N(\alpha) < 0$ eine primitive Form f mit $a < 0$, für die das Ideal $\mathbb{Z}\tau \oplus \mathbb{Z}\tau z$ im engeren Sinne Äquivalent zum Ideal $\mathfrak{a}$ ist. Insbesondere folgt $h^+_{\mathbb{Q}(\sqrt{d})} = h(D)$. Also ist die Korrespondenz zwischen den echten Äquivalenzklassen von Formen und den Idealklassen im engeren Sinne bijektiv und das Theorem damit bewiesen. □

Bemerkung 4.3.5. Im Allgemeinen besteht es kein Isomorphismus zwischen den Mengen der gewöhnliche Äquivalenz von primitiv, positiv definiter Formen und den Idealklassen im gewöhnlichen Sinne. Betrachten wir beispielsweise die Determinante $D = -303$, dann ist $h(-303) = 10$ und $h_{\mathbb{Q}(\sqrt{-303})} = 6$. Im Gegensatz dazu $h^+_{\mathbb{Q}(\sqrt{-303})} = h(-303) = 10$.

4.4 Einteilung in Geschlechterklassen

Wir wollen nun die Einteilung von Formen in Geschlechterklassen untersuchen. Da dies in den meisten Lehrbüchern oft zu wenig behandelt wird, jedoch für das Verständnis der Geschlechtertheorie unabdingbar ist, werden wir systematisch beschreiben, wie die Verteilung von Formen in Geschlechter gelingt. Sei $f = \langle a, b, c\rangle$ eine quadratische Form mit Diskriminante D und z, w zwei beliebige durch die Form f dargestellte Zahlen (dabei ist es egal, ob die Zahlen Primzahlen sind oder nicht), dann kann das Produkt zw immer in die Form $x^2 - dy^2$, $x, y \in \mathbb{Z}$ gebracht werden. Denn sind beispielsweise

$$z = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \quad , \quad w = \mathrm{a}\beta^2 + 2b\beta\delta + c\delta^2 \text{ wobei } \alpha, \beta, \gamma, \delta \in \mathbb{Z}$$

dann können wir die Form $\langle a, b, c\rangle$ durch die in 3.1 beschriebene unimodulare Transformation mit

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathbb{Z}^{2\times 2} \text{ und } \alpha\delta - \gamma\beta = 1$$

in die Form $\langle z, x, w\rangle$ überführen. Dann ist deren Diskriminante $x^2 - zw$ von der Form dy^2, also das Produkt zw von der Form $x^2 - dy^2$. Es lassen sich nun wichtige Folgerungen ziehen[13].

1. Seien $p_1, \ldots, p_t$ für $t \geq 0$ ungerade in D aufgehende Primzahlen, dann hat für jede natürliche Zahl m, welche sich durch die Form f darstellen lässt und für die p_i , $1 \leq i \leq t$ kein Teiler von m ist, das Legendre Symbol

$$\chi_i(m) = \left(\tfrac{m}{p_i}\right)$$

[13] Man vergleich die Disquisitiones Arithmeticae Art.229-231

ein und denselben Wert. Denn sind m_1, m_2 zwei beliebige zu p teilerfremde Zahlen, welche sich durch f darstellen lassen, dann folgt dass

$m_1 m_2 \equiv x^2 \mod p$ und damit $(m_1 m_2/p) = +1$, als $(m_1/p) = (m_2/p)$. Man nennt χ_i einen *Dirichletschen Charakter* modulo p.

2. Sei $D \equiv 3 \mod 4$. Dann hat für alle durch diese Form dargestellten ungeraden Zahlen m der Ausdruck

$$\varsigma(m) = (-1)^{\frac{m-1}{2}}$$

ein und denselben Wert. Denn sind m_1, m_2 zwei beliebige ungerade Zahlen, dann ist $m_1 m_2 = x^2 - dy^2 \equiv x^2 + y^2 \mod 4$, und da das Produkt $m_1 m_2$ ungerade ist, muss eine der beiden Zahlen x, y gerade, die andere ungerade sein. Das impliziert $m_1 m_2 \equiv 1 \mod 4$, also auch $m_1 \equiv m_2 \mod 4$ und damit $(-1)^{\frac{m_1-1}{2}} = (-1)^{\frac{m_2-1}{2}}$.

3. Sei $D \equiv 2 \mod 8$. Dann hat für alle durch diese Form dargestellten ungeraden Zahlen m der Ausdruck

$$\varepsilon(m) = (-1)^{\frac{m^2-1}{8}}$$

ein und denselben Wert. Denn aus $m_1 m_2 = x^2 - dy^2 \equiv x^2 - 2y^2 \mod 8$ erhalten wir, da x ungerade ist, dass $m_1 m_2 \equiv \pm 1 \mod 8$ ist. Damit folgt die Behauptung aus $m_1 \equiv \pm m_2 \mod 8$. Analoge Überlegungen ergeben sich nun für die nächsten zwei Schritte.

4. Ist $D \equiv 6 \mod 8$, dann hat für alle, durch diese Form dargestellten, ungeraden Zahlen m der Ausdruck

$$\varsigma(m) \cdot \varepsilon(m) = (-1)^{\frac{m-1}{2} + \frac{m^2-1}{8}}$$

ein und denselben Wert.

5. Sei $D \equiv 4 \mod 8$. Dann hat für alle durch diese Form dargestellten ungeraden Zahlen m den Ausdruck

$$\varsigma(m) = (-1)^{\frac{m-1}{2}}$$

ein und denselben Wert.

6. Sei $D \equiv 0 \mod 8$. Dann hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen m jeder der beiden Ausdrücke

$$\varsigma(m) = (-1)^{\frac{m-1}{2}} \text{ und } \varepsilon(m) = (-1)^{\frac{m^2-1}{8}}$$

einen für sich unveränderlichen Wert. Denn aus $m_1 m_2 = x^2 - dy^2 \equiv x^2 \equiv 1 \mod 8$ folgt $m_1 \equiv m_2 \mod 8$.

Damit haben wir alle Einteilungen binär quadratischer Formen mit gegebener Diskriminante D in Geschlechter gefunden. Wir halten dies in der folgenden Tabelle fest:

Diskriminante	Zugehörige Charaktere
$D \equiv 1 \mod 4$	$\chi_1, \ldots, \chi_t$
$D = 4D',\ D' \equiv 1 \mod 4$	$\chi_1, \ldots, \chi_t$
$D = 4D',\ D' \equiv 3 \mod 4$	$\chi_1, \ldots, \chi_t, \varsigma$
$D = 4D',\ D' \equiv 2 \mod 8$	$\chi_1, \ldots, \chi_t, \varepsilon$
$D = 4D',\ D' \equiv 6 \mod 8$	$\chi_1, \ldots, \chi_t, \varsigma\varepsilon$
$D = 4D',\ D' \equiv 4 \mod 8$	$\chi_1, \ldots, \chi_t, \varsigma$
$D = 4D',\ D' \equiv 0 \mod 8$	$\chi_1, \ldots, \chi_t, \varsigma, \varepsilon$

Tabelle 2: Diskriminante, Charaktere

Es ist sinnvoll, die Menge aller zugehörigen Charaktere jeweils mit Θ und ihre Anzahl mit r zu bezeichnen. Wir wissen nach Theorem 4.3.3, dass r gleich die Anzahl der in D aufgehenden verschiedenen Primzahlen ist. Die Menge der bestimmten Werte ± 1, die diesen r Charakteren Θ für eine bestimmte Form $\langle a, b, c\rangle$ zukommen, heißt der *Totalcharakter*[14] der Form. Je nachdem, wie das Ergebnis des Totalcharakters ausfällt, teilen sich sämtliche Formen mit gleicher Diskriminante und gleicher Art in Geschlechter ein. D.h. je zwei Formen gehören in dasselbe Geschlecht oder in zwei verschiedene Geschlechter, je nachdem ob der Totalcharakter der einen Form mit dem andren übereinstimmt oder nicht. Damit ist ein Geschlecht der Inbegriff aller ursprünglichen Formen von gleicher Diskriminante und gleicher Art, für die jeder der r Charaktere Θ für sich genommen den gleichen Wert besitzt. Da alle Zahlen, welche durch eine bestimmte Form darstellbar sind, auch durch ihre (echt) äquivalenten Formen dargestellt werden, gehören all diese Formen derselben Klasse auch in dasselbe Geschlecht. Wir bemerken noch, dass die einzelnen Charaktere einer gegeben primitiven Form $\langle a, b, c\rangle$ sich immer aus einen der Koeffizienten a, c erkennen lassen. Denn so oft p ein Primteiler von D ist, so wird sicher einer der Zahlen durch p nicht teilbar sein, denn wären beide durch p teilbar, dann würde p auch in $b^2 = D + ac$ und damit auch in b aufgehen. Damit wäre die Form aber nicht primitiv.

Beispiel 4.4.1. Betrachten wir die Diskriminante $D = -35$. Dann findet man leicht die folgenden acht primitiven, nicht äquivalenten reduzierten Formen:

$$\langle 1, 0, -35\rangle, \langle 5, 0, 7\rangle, \langle 3, \pm 1, 12\rangle, \langle 4, \pm 1, 9\rangle, \langle 2, 1, 8\rangle, \langle 6, 1, 6\rangle,$$

[14] Gauss verwendet den Begriff des Totalcharakters zum ersten Mal in Art.231, bei seiner Untersuchung „Teilung der Ordnung in Geschlechter“ und sagt „hierauf gründen wir die Einteilung der ganzen Ordnung der eigentlich primitiven [...] Klassen mit gegebener Determinante in mehrere verschiedene Geschlechter [...].“

welche die vollständig zu untersuchende Menge bilden. Die Diskriminante $D = -35 = (-1)\cdot 7\cdot 5$ zerfällt in die zwei verschieden Primzahlen 7 und 5. Nach Theorem 4.3.3 existieren daher genau $\mathfrak{A}(-35) = 2$ Geschlechterklassen. Zudem ist die Anzahl der Klassen in jedem Geschlecht genau $\mathfrak{K}(-35) = {}^{8}\!/_{2} = 4$. Nun ist $D = -35 \equiv 1 \bmod 4$, d.h., für die Einteilung der Formen müssen wir nun die beiden Charaktere betrachten:

$$\chi_1(m) = (m/7)\,,\ \chi_2(m) = (m/5)$$

Die Auswertung dieser liefert nun das folgende Resultat.

Für die Formen $\langle 1,0,-35\rangle, \langle 4,\pm 1,9\rangle, \langle 2,1,8\rangle$ erhalten wir für die Charaktere $(m/7) = (m/5) = +1$ und für die Formen $\langle 5,0,7\rangle, \langle 3,\pm 1,12\rangle, \langle 6,1,6\rangle$ erhalten wir $(m/7) = (m/5) = -1$. Damit bildet die Menge $\{\langle 1,0,-35\rangle, \langle 4,\pm 1,9\rangle, \langle 2,1,8\rangle\}$ das Hauptgeschlecht, dessen Totalcharakter $(m/7) = (m/5) = +1$ ist. Die anderen Menge bildet hingegen $\{\langle 5,0,7\rangle, \langle 3,\pm 1,12\rangle, \langle 6,1,6\rangle\}$ das Nichthauptgeschlecht mit dem Totalcharakter $(m/7) = (m/5) = -1$.

4.5 Primzahlen der Form $x^2 + ny^2$

Die Diskussion der Geschlechtertheorie hat uns von dem eigentlichen gestellten Problem, nämlich der Vermutung Eulers, abgelenkt. Wir erinnern daran, dass Euler behauptete, eine Primzahl p wird durch die Form $x^2 + 5y^2$ genau dann dargestellt, wenn $p = 5$ oder $p \equiv 1, 9 \bmod 20$ ist. Im anderen Fall, wird eine Primzahl p durch die Form $2x^2+2xy+3y^2$ genau dann dargestellt, wenn $p \equiv 3, 7 \bmod 20$ gilt. Die Geschlechtertheorie übernimmt nun einen ernsthaften Versuch solche Primzahlen zu charakterisieren, die sich durch eine Form mit Fundamentaldiskriminante darstellen lassen. D.h. sie gestattet es zu entscheiden, ob eine Primzahl durch eine binär quadratische Form dargestellt wird oder nicht. Sie macht jedoch im Allgemeinen keine Aussagen über die Darstellung allgemeiner Formen. Die Geschlechtertheorie beweist, wie wir nun sehen werden, die Vermutung Eulers.

Für $D = -20$ erhalten wir die beidem primitiven nicht äquivalenten reduzierten Formen $f_1 := \langle 1,0,5\rangle$ und $f_2 := \langle 2,2,3\rangle$. Die Determinante lässt sich zerlegen: $D = -20 = -2^2\cdot 5$. Aus Theorem 4.3.3 folgt daher $\mathfrak{A}(-20) = 2$. Also liegen genau zwei Geschlechter vor und in jedem der Geschlechter liegt genau eine der Formen. Nun ist $-20 \equiv 4 \bmod 8$. Wir betrachten daher die beiden Charaktere:

$$\delta(p) = (-1)^{\frac{p-1}{2}} \text{ und } \chi(p) = (p/5).$$

Nun stellt man leicht fest, dass der Totalcharakter von f_1 den Wert $(-1)^{\frac{p-1}{2}} = (p/5) = +1$ besitzt. Also ist die Menge $\{f_1\}$ das Hauptgeschlecht. Und da f_2 den Totalcharakter $(-1)^{\frac{p-1}{2}} = (p/5) = -1$ hat, ist $\{f_2\}$ das Nichthauptgeschlecht. Ist nun $p \neq 5$ eine ungerade Primzahl, dann wird p genau dann durch f_1 dargestellt, wenn

$$(-1)^{\frac{p-1}{2}} = +1 \text{ und } (p/5) = +1.$$

Dies ist genau dann der Fall, wenn $p \equiv 1, 9 \mod 20$ ist. Analog dazu erhalten wir, dass p genau dann durch f_2 dargestellt wird, wenn

$$(-1)^{\frac{p-1}{2}} = -1 \text{ und } (p/5) = -1.$$

Also wenn $p \equiv 3, 7 \mod 20$ ist. Damit haben wir nun die Darstellung der Primzahlen durch die Formen f_1 und f_2 eindeutig charakterisiert und die Vermutung Eulers bestätigt.

Die Anwendung der Geschlechtertheorie ist im Falle, dass in einem Geschlecht mehr als eine Form liegt nicht mehr so aufschlussreich.

4.6 Die Formen $x^2 + 14y^2, x^2 + 27y^2, x^2 + 64y^2$

In der von Euler 1744 publizierten Arbeit behandelt er unter anderem die Form x^2+14y^2. Zunächst stellt man fest, dass die quadratische Kongruenz $x^2+14y^2 \equiv 0 \mod p$ für genau die Primzahlen nicht trivial lösbar ist, für die -14 ein Quadrat im Restklassenkörper $\mathbb{F}_p$ ist. Aus dem quadratischen Reziprozitätsgesetz folgt dann, dass das außer für $p = 2$ oder $p = 7$ nur für die Primzahlen $p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \mod 56$ gilt. Aus Tabelle 1 entnehmen wir zur Diskriminante $D = -56$ die vier reduzierten, primitiven Formen:

$$f_1 = \langle 1, 0, 14\rangle\,, \quad f_2 = \langle 3, 2, 5\rangle\,, \quad f_3 = \langle 2, 0, 7\rangle\,, \quad f_4 = \langle 3, -2, 5\rangle\,.$$

Wir zerlegen die Diskriminante $D = -56 = -2^3 \cdot 7$ in die zwei verschiedenen Primteiler 2 und 7. Also gibt es genau 2 verschiedene Geschlechter. Zudem folgt aus $h(-56) = 4$, dass die Anzahl der Klassen in jedem Geschlecht genau $\mathfrak{K}(-56) = \frac{4}{2} = 2$ beträgt. Nun ist $D = -56 \equiv 0 \mod 8$. Also sind die folgenden drei Charaktere zu betrachten:

$$\varsigma(p) = (-1)^{\frac{p-1}{2}}\,,\ \varepsilon(p) = (-1)^{\frac{p^2-1}{8}}\,,\ \chi(p) = (p/7)$$

Das Hauptgeschlecht besteht aus den Formen $\{f_1, f_3\}$. Diese haben den Totalcharakter $\{+1, +1\}$. Das Nichthauptgeschlecht aus den Formen $\{f_2, f_4\}$ mit den Totalcharakter $\{-1, -1\}$. Daraus folgt nun, dass eine Primzahl $p \neq 2, 7$ durch f_1 oder f_2 genau dann dargestellt wird, wenn

$$(-1)^{\frac{p^2-1}{8}} = +1, (p/7) = +1$$

gilt. Durch einfache Berechnung erhält man, dass dies genau dann der Fall ist, wenn $p \equiv 1, 9, 15, 23, 25, 39 \mod 56$. Es kann jedoch keine Aussage darüber getroffen werden, ob p durch f_1 bzw. f_3 dargestellt wird. Analog stellt man leicht fest, dass eine Primzahl $p \neq 2, 7$ genau dann durch f_1 oder f_2 dargestellt wird, wenn $p \equiv 3, 5, 13, 19, 27, 45 \mod 56$ ist. Wieder lässt sich keine Bedingung abgeleitet, ob p durch f_1 bzw. f_2 dargestellt wird.

Wir sehen also, dass die Geschlechtertheorie in ihre Grenzen stößt und nicht alle Fragen, bezüglich der Darstellung von Primzahlen durch binär quadratische Formen, befriedigend beantworten kann. Eine noch wesentlich komplexere Situation liegt für die Formen $x^2 + 27y^2$, $x^2 + 64y^2$ vor. Euler behauptet 1749 in seinem unvollständigen Werk Tractatus de nomerorum doctrina

- *Eine Primzahl p hat genau dann die Gestalt $p = x^2 + 27y^2$, wenn $p \equiv 1 \mod 3$ und 2 eine dritte Potenz in $\mathbb{F}_p$ ist.*
- *Eine Primzahl p hat genau dann die Gestalt $p = x^2 + 64y^2$, wenn $p \equiv 1 \mod 4$ und 2 eine vierte Potenz in $\mathbb{F}_p$ ist.*

Beispielsweise liegen die quadratischen Formen $f_1(x, y) = x^2 + 27y^2$ und $f_2(x, y) = 4x^2 + 2xy + 7y^2$ mit Diskriminante $D = -108$ in einem Geschlecht, obwohl sie nicht äquivalent sind, denn offensichtlich wird die Zahl 13 durch die Form f_2 mit $(x, y) = (1, 1)$, jedoch nicht durch die Form f_1, dargestellt. Beide Formen stellen aber dieselben primitiven Restklassen modulo 108 dar, nämlich

$$p = 1, 7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 91, 97, 103.$$

Die Darstellbarkeit einer Primzahl p durch die Form f_1 kann also in diesem Fall nicht mehr durch eine einfache Kongruenzberechnung bewältigt werden. Nun lässt sich nach Euler eine Primzahl p genau dann durch die Form $x^2 + 27y^2$ darstellen, wenn $p \equiv 1 \mod 3$ gilt und 2 ein kubischer Rest modulo p ist, d.h. die Kongruenz $x^3 \equiv 2 \mod p$ ist lösbar.

Gauss stieß im Jahre 1805 auf die Vermutungen Eulers und bewies sie mit Hilfe der kubischen bzw. biquadratischen Reziprozität, wir verweisen auf [Cox,Th. 4.15 und Th. 4.23ii)]. Fragestellungen und Probleme solcher Art gehören heute in die im 20.Jh. aus den höheren Reziprozitätsgesetzen entwickelte Klassenkörpertheorie.

Zusammenfassung

Im letzten Kapitel haben wir die Kompositionen von Formen behandelt und gesehen, dass sich zwei primitiv, positiv definite Formen zu einer dritten Komponieren lassen und dass die Menge dieser Formenklassen eine endlich abelsche Gruppe bildet. Damit die Verbindung zwischen Formen und Idealen in quadratischen Zahlkörpern hergestellt werden konnte haben wir die Idealklassen im engeren Sinne eingeführt und gezeigt, dass diese eine endlich abelsche Gruppe bilden. Wir haben die Geschlechter eingeführt und gesehen, dass zwei Ideale $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, zum selben Geschlecht gehören, wenn sich also ihre Idealklassen im engeren Sinne um ein Quadrat unterscheiden. Wir haben die Korrespondenz zwischen den echten Äquivalenzklassen primitiver Formen und den Äquivalenzklassen im engeren Sinne von Idealen bewiesen. Zudem ist die Anzahl der Geschlechter genau 2^{t-1} und die Anzahl der Klassen in jedem Geschlecht gleich $\frac{h(D)}{2^{t-1}}$. Mit Hilfe der Geschlechtertheorie konnten wir schließlich die von Euler aufgestellte Vermutung, über die Darstellung von Primzahlen durch binär quadratische Formen, beweisen. Sahen aber auch am Beispiel der Formen $x^2 + 14y^2, x^2 + 27y^2, x^2 + 65y^2$, dass die Geschlechtertheorie für den Fall,

dass mehr als eine Form in jedem Geschlecht existiert, nicht mehr so aufschlussreich ist bzw. keine genaue Aussage mehr getroffen werden kann und in solchen Fällen auf höhere Reziprozitätsgesetze zurückgegriffen werden muss.

Literaturverzeichnis

Lehrbücher

[We1] A.Weil‘, Introduction to ’Collected Papers by E.E.Kummer’ OEuvres Scientifiques, vol.III Springer 1979

[We2] A. Weil‘, La cyclotomie jadis et nagu‘ere, OEuvres Scientifiques, vol.III Springer 1979

[Di] Peter Gustav Lejeune Dirichlet, Vorlesungen über Zahlentheorie, Herausgegrben von R.Dedekind, 1863. Edition Classic, VDM Verlag.

[DA] Carl Friedrich Gauss, Disquisitiones Arithmeticae: Untersuchungen über höhere Arithmetik, Kessel, Norbert; Auflage:1 deut. Aufl. 1889 (30. April 2009)(Taschenbuch).

[Lang] Serge Lang, Algebra, Graduate Texts in Mathematics, Springer; 3rd edition (June 21, 2005).

[Fi] Gerd Fischer, Lineare Algebra: Eine Einführung für Studienanfänger, Vieweg + Teubner Auflage:16., überarb. u. erw. (28. August 2008).

[Wuß] Hans Wussing, 6000 Jahre Mathematik. Band 2:Eine kulturgeschichtliche Zeitreise-Von Euler bis zur Gegenwart, Springer, Berlin; Auflage:1 (Dezember 2008)

[KaMe] Christian Karpfinger, Kurt Meyberg, Algebra: Gruppen-Ringe-Körper, Spektrum Akademischer Verlag; Auflage:1 (Oktober 2008).

[Schmidt] Alexander Schmidt, Einführung in die algebraische Zahlentheorie, Springer, Berlin; Auflage:1 (Juni 2009).

[Wol] Jürgen Wolfart, Einführung in die Zahlentheorie und Algebra, Vieweg Verlagsgesellschaft Nr.86; Auflage:1 (1. September 1996).

[StPi] Stefan Müller-Stach und Jens Piontkowski, Elementare und algebraische Zahlentheorie:Ein moderner Zugang zu klassischen Themen, Vieweg+Teubner; Auflage: 1 (16. Januar 2007).

[Art] Michael Artin und Annette A.Campo, Algebra, Birkhäuser Verlag; Auflage:1 (19. Mai 1998).

[Neu] Jürgen Neukirch, Algebraische Zahlentheorie, Springer, Berlin; Auflage: Nachdruck d.1.A.(4. Dezember 2007).

[Ri] Paulo Ribenboim, Die Welt der Primzahlen:Geheimnisse und Rekorde, Springer, Berlin; Auflage:1 (5. September 2006).

[SchFr] Haralt Scheid, Andreas Frommer, Zahlentheorie, Spektrum Akademischer Verlag; Auflage:4. A. (19. Oktober 2006)
[La] Edmund Georg Hermann Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante, Math. Annalen 56 pp 671-676 (1903).

[He] Erich Hecke, Vorlesungen über die theorie der algebraischen Zahlen, American Mathematical Society (15. März 2000).

[Cox] David A. Cox, Primes of the form $x^2 + ny^2$:Fermat,Class Field Theory, and Complex Multiplication, Wiley-Interscience (May 8, 1997).

[Za] D.A.Zagier, Zetafunktionen und quadratische Körper:Eine Einführung in die höhere Zahlentheorie, Springer, Berlin; Auflage:1 (September 1981).

Wissenschaftliche Artikel und Skripte

[Be] Ch.Bessenrodt, Skript zur 2 St. Vorlesung:Algebra I
http://www.blu7.com/Skripte/Algebra I WS0304 Skript.pdf

[Sa] J.Sander, Skript zur 2 St. Vorlesung:Einführung in die Zahlentheorie,
http://www.blu7.com/Skripte/Zahlentheorie WS0607 Skript.pdf

[Ma] B.H.Matzat, Skript zur 2 St. Vorlesung: Elementare Zahlentheorie
http://www.hl=deq=matzart+vorlesung+zalentheoriemeta=fp=30df391052660486

[Schaff] Karl Schaffstein, Tafel der Klassenzahlen der reellen quadratischen Zahlkörper mit Primzahldiskriminante unter 12000 und zwischen 100000–101000 und 1000000–1001000,
Mathematische Annalen: Volume98 Number1/März 1928, Springer Berlin/Heidelberg.

[Canad.J.Math.2] H. Chatland, H. Davenport, Euclids algorithm in real quadratic fields, Canad. J. Math.2 (1950), 289-296.

[Michigan Math.J.14] Harold Mead Stark, A complete determination of the complex quadratic fields of class numberone, Michigan Math.J.14 (1967), 1-27.

Skript von Prof. Dr. Annette Huber-Klawitter zur algebraischen Zahlentheorie. http://home.mathematik.uni-freiburg.de/arithmetische-geometrie/lehre/ss08/azt.pdf

Franz Lemmermeyer: Quadratische Zahlkörper. Ein Schnupperkurs. http://www.ub.uni-heidelberg.de/archiv/16

Plagiatserklärung

Hiermit versichere ich, dass ich die Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, sind als solche kenntlich gemacht. Die Arbeit ist in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen worden.

Hannover, den 30. September 2009 _____