Richard Lindner und Nicole Nowak

Quadratische Zahlenkörper und ihre Klassenzahl

28. Juni 2004

Algebra SS2003

Inhaltsverzeichnis

1

Einleitung

Die folgenden Ausarbeitung ist auf eine Algebravorlesung im Hauptstudium aufbauend entstanden.
Als Grundlage dieser Ausarbeitung dienten uns Abschnitte aus dem Buch *Algebra* von M.Artin. Wir haben uns weitgehend an der Struktur des Buches orientiert und haben versucht, den Inhalt verständlich und etwas ausführlicher wiederzugeben.

1.1 Ganze algebraische Zahlen

In diesem Teil möchten wir zunächst einige Grundbegriffe klären, die für das Verständnis unabdingbar sind. Es ist einsichtig, dass zunächst geklärt werden muss, was genau ein quadratischer Zahlenkörper ist und unter welchen Aspekten wir diesen Körper betrachten wollen. Da wir später in den quadratischen Zahlenkörpern die Ringe der *ganzen algebraischen Zahlen* betrachten möchte, sollen hier zunächst grundlegende Eigenschaften jener erwähnt werden.

Definition 1.1.1. Eine komplexe Zahl α wird *ganze algebraische Zahl* genannt, wenn sie Nullstelle eines *normierten* Polynoms $f(X) \neq 0$ mit ganzzahligen Koeffizienten ist. Also eines Polynoms der Form $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$.

Die Menge aller Polynome in $\mathbb{Q}[X]$, die eine ganze algebraische Zahl α als Nullstelle haben, bilden ein Hauptideal, da diese Menge der Kern des Einsetzungshomomorphismus $\phi : \mathbb{Q}[X] \to \mathbb{C} : f(X) \to f(\alpha)$ ist. Dieses Hauptideal wird von einem irreduziblen Polynom $f(X)$ erzeugt. Dieses Polynom wird *irreduzibles Polynom von α über $\mathbb{Q}$* genannt. Weiterhin unterscheiden wir das *Minimalpolynom* von α, das normierte irreduzible Polynom von α, und das *primitive* Polynom für α in $\mathbb{Z}[X]$. Man kann das irreduzible Polynom für α auch als primitives Polynom in $\mathbb{Z}[X]$ wählen, da das Minimalpolynom mit dem Hauptnenner der Koeffizienten durchmultipliziert werden kann, ohne, dass die neuen Koeffizienten einen weiteren Faktor gemeinsam haben. Existierte dieser Faktor, so könnte das Minimalpolynom nicht normiert gewesen sein.

Satz 1.1.2. *Der Kern des Homomorphismus $\phi : \mathbb{Z}[X] \to \mathbb{C} : f(x) \to f(\alpha)$, der x auf α abbildet, ist das Hauptideal von $\mathbb{Z}[X]$, das von dem primitiven irreduziblen Polynom von α erzeugt wird.*

Beweis. Sei $f(x)$ das primitive irreduzible Polynom von α. Jedes andere Polynom $g(x)$ in $\mathbb{Z}[x]$, welches α als Nullstelle hat, enthält $f(x)$ als Faktor, wird also von $f(x)$ geteilt. Also ist g ein Element des von f erzeugten Hauptideals. □

Nun lässt sich etwas darüber sagen, wann eine algebraische Zahl α eine ganze algebraischen Zahl ist.

Satz 1.1.3. *Sei α eine algebraische Zahl. Dann sind die folgenden Aussagen äquivalent:*
(1) α ist eine ganze algebraische Zahl.
(2) Das primitive irreduzible Polynom von α ist normiert. Anders gesagt: α ganze algebraische Zahl $\Leftrightarrow$ das Minimalpolynom von α in $\mathbb{Q}[X]$ hat ganzzahlige Koeffizienten.

Beweis. (2) $\Rightarrow$ (1): Da für das primitive irreduzible Polynom von α gilt, dass α eine Nullstelle ist, folgt sofort, dass α eine ganze algebraische Zahl ist.
(1) $\Rightarrow$ (2): Hier zeigen wir $\neg(2) \Rightarrow \neg(1)$ Sei das primitive irreduzible Polynom $f(x)$ von α nicht normiert. Wir wissen jedoch, dass der Leitkoeffizient von f den Leitkoeffizienten jedes Vielfachen von f teilt. Ist also $f(x)$ nicht normiert, so kann α auch nicht Nullstelle eines normierten ganzzahligen Polynoms sein. α ist also keine ganze algebraische Zahl. □

2

Ganze algebraische Zahlen in quadratischen Zahlkörpern

2.1 Einführung in quadratische Zahlkörper

Ein quadratischer Zahlkörper ist eine Erweiterung der rationalen Zahlen durch eine echte Quadratwurzel einer ganzen Zahl. Sie haben also die Form $K = \mathbb{Q}[\sqrt{d}]$ für bestimmte $d \in \mathbb{Z}$. Wir nennen dieses d den *Erzeuger* von K. Wir unterscheiden zunächst zwischen negativ und positiv erzeugten Zahlkörpern. Da alle negativ erzeugten durch die Wurzel einer negativen Zahl entstehen und somit die komplexe Zahl $i\sqrt{|d|}$ enthalten nennen wir diese *imaginär-quadratische Zahlkörper* $K \leq \mathbb{C}$. Die von positiven d erzeugten Körper heißen *reell-quadratische Zahlkörper* $K \leq \mathbb{R}$.

Damit wir durch $\sqrt{d}$ eine echte Erweiterung von $\mathbb{Q}$ bekommen müssen wir natürlich fordern, dass d kein Quadrat einer ganzen Zahl ist, also fallen diese alle weg. Wir möchten aber auch, dass d quadratfrei ist, also keinen Primfaktor mehrmals besitzt. Wenn d nämlich einen quadratischen Teiler in $\mathbb{Z}$ hat, so kann man diesen rauskürzen und d/p^2 erzeugt immer noch denselben Körper.

2.2 Ganze algebraische Zahlen

Wir werden die ganzen algebraischen Zahlen für einen beliebigen quadratischen Zahlkörper nun charakterisieren und wir beginnen mit einem Lemma.

Lemma 2.2.1. *$z = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ ist eine ganze algebraische Zahl genau dann, wenn $2a, a^2 - b^2 d \in \mathbb{Z}$ sind.*

Beweis. Sei $K := \mathbb{Q}[\sqrt{d}]$ und $z = a + b\sqrt{d} \in K$ aber $z \notin \mathbb{Q}$. Dann ist $b \neq 0$ und $\hat{z} := a - b\sqrt{d}$ ist auch ein Element in K. Somit ist z Nullstelle des Polynoms $p(x) = (x - z)(x - \hat{z})$. Dieses Polynom ist mit zwei Nullstellen irreduzibel über $\mathbb{Q}$. Es ist sogar das Minimalpolynom von z, da z als nicht rationale Zahl nicht Nullstelle eines linearen Polynoms aus $\mathbb{Q}[X]$ sein kann! Wir Formen nun p etwas um und betrachten die Koeffizienten.
$(x - z)(x - \hat{z})$
$= x^2 - (z + \hat{z})x + z\hat{z}$
$= x^2 - (a + b\sqrt{d} + a - b\sqrt{d})x + (a)^2 - (b\sqrt{d})^2$
$= x^2 + (-2a)x + (a^2 - b^2 d)$
Wir wissen, dass z eine ganze algebraische Zahl ist genau dann, wenn die Koeffizienten des Minimalpolynoms p Elemente in $\mathbb{Z}$ sind. Da $-2a \in \mathbb{Z} \Leftrightarrow 2a \in \mathbb{Z}$ folgt hieraus das Lemma. □

Mit Hilfe dieses Lemmas kommen wir jetzt direkt zu dem wichtigen Satz, der die ganzen algebraischen Zahlen für quadratische Zahlkörper allgemein klassifiziert.

Satz 2.2.2. *Sei $K = \mathbb{Q}[\sqrt{d}]$ für ein quadratfreies d mit*
(I) $d \equiv_4 2$ oder 3, dann gilt:
$z = a + b\sqrt{d}$ ist ganze algebraische Zahl in $K \Leftrightarrow a, b \in \mathbb{Z}$
(II) $d \equiv_4 1$ dann gilt:
$z = a + b\sqrt{d}$ ist ganze algebraische Zahl in $K \Leftrightarrow a, b \in \mathbb{Z}$ oder $a, b \in \mathbb{Z} + \frac{1}{2}$

Der Fall $d \equiv_4 0$ taucht nicht auf, denn wenn d durch 4 teilbar ist, war es nicht quadratfrei und somit hätte man es vorher vereinfachen müssen.

Beweis. Wir beweisen zuerst die $\Leftarrow$ Implikation.
Gilt $a, b \in \mathbb{Z}$ so sind wir mit Hilfe des zuvor gezeigten Lemmas fertig. Es bleibt also nur der Fall aus (II), wo $a, b \in \mathbb{Z} + \frac{1}{2}$ sind. $2a \in \mathbb{Z}$ gilt hier noch. Es fehlt also nur $a^2 - b^2 d \in \mathbb{Z}$. Wir schreiben nun a, b in der Form $a = \frac{1}{2}m$ und $b = \frac{1}{2}n$ mit $m, n \in 2\mathbb{Z} + 1$ also ungerade. Was wir zeigen wollen ist jetzt $\frac{1}{4}(m^2 - n^2 d) \in \mathbb{Z}$. Durch Umformen sieht man:
$m^2 - n^2 d$
$\equiv_4 (\pm 1)^2 - (\pm 1)^2 * 1$
$\equiv_4 1 - 1 * 1 \equiv_4 0$
Das beendet die eine Implikation. Nun die Andere $\Rightarrow$.
Sei also $z = a + b\sqrt{d}$ eine ganze algebraische Zahl in K. Dann gilt nach dem vorigen Lemma auf jeden Fall, dass $(\bullet)$ $2a \in \mathbb{Z}$ und $(\star)$ $a^2 - b^2 d \in \mathbb{Z}$ ist. Wir unterscheiden zwei Fälle:
(1) $a \in \mathbb{Z}$. Dann folgt aus $(\star)$, dass $b^2 d \in \mathbb{Z}$ ist. Da b ursprünglich aus $\mathbb{Q}$ kommt können wir es als $b = \frac{p}{q}$ schreiben. Diese p, q sind teilerfremd in $\mathbb{Z}$ und es gilt $q > 0$. Aus $b^2 d \in \mathbb{Z}$ wird $\frac{p^2 d}{q^2} \in \mathbb{Z}$. Da p und q teilerfremd waren, sind auch p^2 und q^2 teilerfremd. Weil d quadratfrei ist kann auch hier q^2 kein Teiler sein. Da das Produkt $\frac{p^2 d}{q^2}$ in $\mathbb{Z}$ liegt ergibt sich, dass $q = 1$ sein muss! Daraus folgt dann $b = \frac{p}{1}$ also ist $b \in \mathbb{Z}$.
(2) $a \in \mathbb{Z} + \frac{1}{2}$. Es gilt also wieder $a = \frac{1}{2}m$ für ein ungerades $m \in \mathbb{Z}$. Daraus folgt sicher $4a^2 = m^2 \in \mathbb{Z}$ und damit folgern wir aus $(\star)$, dass $4b^2 d \in \mathbb{Z}$ ist. Wir überlegen uns, dass $b^2 d \in \mathbb{Z}$ nicht gelten darf, denn sonst würde aus $(\star)$ folgen, dass $a^2 = \frac{1}{4}m^2 \in \mathbb{Z}$ liegt und daraus folgt, weil ja m ungerade war: $4 = 1$. Dies ist ein Widerspruch! Wir schreiben $b = \frac{p}{q}$ wie vorher mit teilerfremden p und $q > 0$. Nun wissen wir ja, dass $4b^2 d = 4(\frac{p}{q})^2 d \in \mathbb{Z}$ ist. Also muss q^2 ein Teiler von 4 sein. Aber der Fall $q = 1$ fällt weg, weil $b^2 d = (\frac{p}{q})^2 d \notin \mathbb{Z}$ gilt. Also muss $q = 2$ sein. Daraus folgt nun, dass auch $b = \frac{1}{2}p \in \mathbb{Z} + \frac{1}{2}$ ist. Wir setzten $n := p$ und schreiben es wie vorher als $b = \frac{1}{2}n$. Nach $(\star)$ wissen wir, dass folgendes gilt:
$4a^2 - 4b^2 d \equiv_4 0$
$\equiv_4 m^2 - n^2 d$
$\equiv_4 (\pm 1) - (\pm 1) * d \equiv_4 0$
Damit wissen wir dann, dass $d \equiv_4 1$ gelten muss. Also sind wir fertig! □

2.3 Ring der ganzen algebraischen Zahlen

Nun wird gezeigt, dass die ganzen algebraischen Zahlen in einem quadratischen Zahlkörper immer einen Ring R bilden und welche Form dieser hat.

Satz 2.3.1. *Die ganzen algebraischen Zahlen in einem quadratischen Zahlkörper* $K = \mathbb{Q}[\sqrt{d}]$ *bilden einen Ring R.*

Von nun an möchten wir eine vereinfachende Notation verwenden:

$$\delta := \sqrt{d} \text{ und } \eta := \frac{1}{2}(1+\delta).$$

Beweis. Man zeigt, dass R Unterring von $\mathbb{C}$ ist. 0 und 1 sind offensichtlich Elemente in R, da sie Nullstellen der ganzzahligen, normierten Polynome X und X-1 sind.

Zeigen wir zuerst, dass R abgeschlossen ist unter Addition.
Seien α und β ganze algebraische Zahlen in R, dann haben diese Zahlen nach dem vorhergehenden Satz folgende Darstellungen $\alpha = a + b\delta$ und $\beta = x + y\delta$ für $d \equiv_4 2$ oder 3 bzw. $\alpha = a + b\eta, \beta = x + y\eta$ im Fall $d \equiv_4 1$, mit a,b,x,y $\in \mathbb{Z}$.
$\alpha + \beta = (a+x) + (b+y)\delta$ bzw. $(a+x) + (b+y)\eta$. $\alpha + \beta$ ist also offensichtlich wieder Element in R. Nun Abgeschlossenheit unter Multiplikation.
$\alpha\beta = ax + ay\delta + bx\delta + byd = (ax + byd) + (ay + bx)\delta \in R$ Jetzt der Fall $d \equiv_4 1$:
$\alpha\beta = ax + ay\eta + bx\eta + by\eta^2 = ax + (ay + bx)\eta + by\eta^2$ Es ist bereits zu sehen, dass $ax + (ay + bx)\eta$ Element von R ist, jetzt gilt noch zu zeigen, dass auch $by\eta^2 \in R$. Denn dann folgt, dass $\alpha\beta \in R$. Da by offensichtlich eine ganze Zahl ist, genügt es sogar zu zeigen, dass η^2 in R liegt.
$\eta^2 = \frac{1}{4}(1 + 2\delta + d) = \frac{1+d}{4} + \frac{1}{2}\delta$
Da $d \equiv_4 1$ ist $(d+1) \equiv_4 2$, hier folgt $\frac{d+1}{2}$ ist eine ungerade ganze Zahl.
$2k + 1 := \frac{d+1}{2}$ Jetzt lässt sich η^2 schreiben als $\frac{2k+1}{2} + \frac{1}{2} = k + \frac{1}{2}(1+\delta) = k + \eta$ also ist gezeigt, dass $\eta^2 \in R$ und somit ist die multiplikative Abgeschlossenheit von R gezeigt. □

Satz 2.3.2. *Sei* $d \equiv_4 1$. *Dann sind die ganzen algebraischen Zahlen in* $K = \mathbb{Q}[\delta]$ *von der Form* $a + b\eta$ *mit* $a, b \in \mathbb{Z}$. *Sie bilden also den Ring* $\mathbb{Z}[\eta]$. *Falls* $d \equiv_4 2$ *oder* 3 *so bilden die ganzen algebraischen Zahlen den Ring* $\mathbb{Z}[\delta]$.

Beweis. Wie bereits zuvor gezeigt, hat eine ganze algebraische Zahl α im Fall $d \equiv_4 1$ genau die Form $a + b\delta$ mit $a, b \in \mathbb{Z}$ oder $a, b \in \mathbb{Z} + \frac{1}{2}$.
Sagen wir zunächst der erste Fall trete ein, also $a, b \in \mathbb{Z}$. Dann lässt sich α auch schreiben als $\frac{2a}{2} + \frac{2b}{2}\delta = \frac{2a-2b}{2} + \frac{2b}{2} + \frac{2b}{2}\delta = a - b + b\frac{1}{2}(1+\delta) = a - b + b\eta$. Hier ist also gezeigt, dass sich α in diesem Fall genau so schreiben lässt, wie wir im Satz behaupten.
Betrachten wir nun den zweiten Fall, $a, b \in \mathbb{Z} + \frac{1}{2}$:
Also lässt sich α schreiben als $\frac{m}{2} + \frac{n}{2}\delta$, mit m, n ungerade. Nun formen wir wieder um: $\frac{m}{2} + \frac{n}{2}\delta = \frac{m-n}{2} + \frac{n}{2} + \frac{n}{2}\delta = \frac{m-n}{2} + n\frac{1}{2}(1+\delta)$. Da m-n gerade ist, also $\frac{m-n}{2} \in \mathbb{Z}$ und α wieder in die gewünschte Form gebracht.
Der zweite Teil des Satzes folgt direkt aus Satz 2.2.2. □

2.4 Der Ring als Gitter

Eine interessante und vor allem nützliche Beobachtung ist, dass sich für imaginärquadratische Zahlkörper der Ring der ganzen algebraischen Zahlen immer als erstaunlich einfaches *Gitter* in der komplexen Zahlenebene darstellen lässt.

Behandeln wir zuerst den Fall $d \equiv_4 1$: Dann wissen wir der Ring der ganzen algebraischen Zahlen ist $\mathbb{Z}[\eta]$. Also haben alle Elemente des Rings die Form $a + b\eta$ mit $a, b \in \mathbb{Z}$. Wir wollen nun diese Elemente als Punkte in die komplexe Zahlenebene eintragen. Also fangen wir bei Null an und machen erstmal auf der reellen Achse

alle ganzen Zahlen zu Punkten. Dann können wir von Null um η nach rechts oben gehen und auf dieser Höhe wieder alle ganzen Zahlen einzeichnen.

Dasselbe können wir auch für alle ganzzahligen Vielfachen von η machen. Damit bekommen wir in $\mathbb{C}$ ein schönes Gitter mit der Gitterbasis $(1, \eta)$. Da die reelle Komponente von η genau ein halb ist, bilden $0, 1, \eta$ ein Dreieck. Durch Verschieben kann man dieses Dreieck an jede Zahl in dem Ring hängen. Das Gitter ist also so aufgebaut, dass an jedem Punkt ein solches Dreieck existiert.

Nun der andere Fall $d \equiv_4 2$ **oder** 3: Alles verläuft analog nur das alle η zu δ werden. Die Gitterbasis hier ist also $(1, \delta)$. Der große Unterschied ist, dass δ keinen Realteil mehr hat! Dadurch entstehen in diesem Gitter keine Dreiecke sondern Vierecke. Ein Viereck bilden zum Beispiel $0, 1, \delta, 1 + \delta$. Auch hier ist alles so aufgebaut, dass dieses selbe Viereck an jeden Punkt des Rings gelegt werden kann.

2.5 Die Diskriminante eines quadratischen Zahlkörpers

Definition 2.5.1. *Für die Diskriminante D eines quadratischen Zahlkörpers der Form $K = \mathbb{Q}[\sqrt{d}]$ unterscheiden wir zwei Fälle:*

(I) $d \equiv_4 1$. Dann bezeichnen wir die Diskriminante des Polynoms $x^2 - x + \frac{1}{4}(1-d)$ als Diskriminante von K.

(II) $d \equiv_4 2$ oder 3. Dann bezeichnen wir die Diskriminante des Polynoms $x^2 - d$ als Diskriminante von K.

Explizit bedeutet das: $D := d$, falls $d \equiv_4 1$ und $D := 4d$, falls $d \equiv_4 2$ oder 3.

3

Faktorzerlegung in imaginär-quadratischen Zahlkörpern

Nachdem wir nun wissen, dass die ganzen algebraischen Zahlen in quadratischen Zahlkörpern einen Ring bilden, wollen wir diesen Ring genauer betrachten. Fragen, die hier interessant sind, sind die Fragen nach den Einheiten in diesem Ring und nach Faktorzerlegungen in dem Ring.
Sei R der Ring der ganzen algebraischen Zahlen in einem imaginär-quadratischen Zahlkörper $\mathbb{Q}[\delta]$.

3.1 Die Norm einer ganzen algebraischen Zahl

Falls $\alpha = a + b\delta \in R$, so ist auch ihr komplex konjugiertes $\bar{\alpha} = a - b\delta \in R$.

Definition 3.1.1. *Unter der Norm von einer ganzen algebraischen Zahl α in einem quadratischen Zahlkörper verstehen wir*

$$N(\alpha) = \alpha\bar{\alpha}$$

Die Norm ist also das Betragsquadrat von α, also immer positiv, sofern $\alpha \neq 0$. Die Norm einer ganzen algebraischen Zahl ist so immer eine ganze Zahl.
Die folgende Proposition ist durch die Multiplikativität der Norm auf $\mathbb{C}$ gegeben.

Proposition 3.1.2. *Die Norm ist multiplikativ. Es gilt also:*

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

□

Da wir nun Zerlegungen und Einheiten in R betrachten wollen, soll hier noch gesagt sein, dass als Teiler einer ganzen algebraischen Zahl α nur solche Zahlen in Frage kommen, welche die Norm von α teilen.

3.2 Einheiten und Faktorzerlegungen in R

Bevor wir uns Zerlegungen einer ganzen algebraischen Zahl betrachten können. müssen wir zuerst klären, welche Elemente in R Einheiten sind.

Satz 3.2.1. *Ein Element α von R ist genau dann eine Einheit, wenn $N(\alpha) = 1$ ist.*

Beweis. $\Rightarrow$: Sei α eine Einheit in R, dann gilt $N(\alpha)N(\alpha^{-1}) = N(1) = 1$ aufgrund der Multiplikativität der Norm. Da $N(\alpha)$ und $N(\alpha^{-1})$ natürliche Zahlen sind, sind beide gleich 1.
$\Leftarrow$: Ist $N(\alpha) = \alpha\bar{\alpha} = 1$, dann ist $\bar{\alpha} = \alpha^{-1}$. Also ist $\alpha^{-1} \in R$ und α daher eine Einheit.

Eine ganze algebraische Zahl ist also genau dann eine Einheit, wenn sie auf dem Einheitskreis der komplexen Ebene liegt.
Jetzt, da wir wissen, welches die Einheiten in R sind, können wir betrachten wie ein Element $\alpha \in R$ in irreduzible Faktoren zerlegbar ist.

Satz 3.2.2. *In R existieren Zerlegungen in irreduzible Faktoren.*

Beweis. Falls in R gilt $\alpha = \beta\gamma$ und β und γ keine Einheiten sind, so gilt $N(\alpha) = N(\beta)N(\gamma)$. Da wir uns hier nun im Ring der ganzen Zahlen befinden und wir wissen, dass β und γ keine Einheiten sind, liegt hier eine echte Zerlegung im Ring der ganzen Zahlen vor. Da auf $\mathbb{Z}$ eine Primfaktorzerlegung existiert, folgt hier die Existenz einer Zerlegungin irreduzible Faktoren auf R. □

Es ist jedoch zu bemerken, dass die Zerlegung in irreduzible Faktoren in den meisten Fällen nicht eindeutig ist. Nun stellt sich natürlich die Frage in welchen Ringen R eine eindeutige Zerlegung in irreduzible Faktoren existiert, also welche der Ringe R faktoriell sind.

Satz 3.2.3. *Der einzige Ring R mit $d \equiv_4 3$ der faktoriell ist, ist der Ring der ganzen Gaußschen Zahlen.*

Beweis. Wir setzen als bekannt voraus, dass der Ring der ganzen Gaußschen Zahlen faktoriell ist. Wir wollen also nur zeigen, dass alle anderen Ringe nicht faktoriell sind. Sei $d \equiv_4 3$, jedoch $d \neq -1$. Dann gibt es zwei unterschiedliche Zerlegungen von 1-d in R.
$1 - d = 2 \cdot (\frac{1-d}{2})$ und $1 - d = (1 - \delta)(1 + \delta)$.
2 ist ein irreduzibles Element in R, da $N(2) = 4$ der kleinste Wert< 1 ist, den die Norm auf R annimmt. Es gibt also kein Element, dass 2 teilt. Wenn man nun die beiden Zerlegungen von (1-d) miteinander vereinbaren wollte, also zeigen wollte, dass sie nicht der Eindeutigkeit der Zerlegung widersprechen, so müsste 2 entweder $(1 + \delta)$ oder $(1 - \delta)$ teilen. Wäre dies der Fall, dann könnte die rechte Zerlegung so umgeformt werden, dass sie mit der linken übereinstimmt. (Natürlich wäre das dann auch genau umgekehrt möglich.) Dieser Versuch scheitert jedoch daran, dass $\frac{1}{2} \pm \frac{1}{2}\delta \notin R$, falls $d \equiv_4 3$. Also belegen die beiden unterschiedlichen Zerlegungen von $1 - d$ die Nichteindeutigkeit der Faktorzerlegung in R. □

3.3 Idealklassen in imaginär-quadratischen Zahlkörpern

Wir betrachten weiterhin R, den Ring der ganzen algebraischen Zahlen eines imaginär-quadratischen Zahlkörpers. Wie wir bereits wissen, ist die Zerlegung von Elementen aus R in irreduzible Faktoren nicht eindeutig. Nun wollen wir versuchen zu beschreiben in welchem Ausmaß die Eindeutigkeit dieser Zerlegung verletzt ist. Dazu führen wir eine Äquivalenzrelation auf der Menge der Ideale von R ein. Diese Ideale sind Untergitter von R, die auch eine genau 2 elementige Gitterbasis haben. Zunächst müssen wir hierfür jedoch eine Operation auf den Idealen einführen.

Definition 3.3.1. *Seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale eines Ringes R. Dann ist das Produktideal die Menge aller endlichen Summen von Produkten der Form $\sum_i \alpha_i\beta_i$ mit $\alpha_i \in \mathfrak{a}$ und $\beta_i \in \mathfrak{b}$.*

Es wäre nicht ausreichend gewesen alle Produkte in die Menge aufzunehmen, da diese Menge im allgemeinen kein Ideal bildet. Weiterhin sei noch gesagt, dass die Multiplikation von Idealen kommutativ und assoziativ ist, sowie, dass der ganze Ring R ein neutrales Element für diese Multiplikation bildet.

Lemma 3.3.2. *Sei R der Ring der ganzen algebraischen Zahlen in einem imaginär quadratischen Zahlkörper. Das Produkt eines Ideals* $\mathfrak{a} \neq (0)$ *und des dazugehörigen konjugierten Ideals* $\bar{\mathfrak{a}}$ *ist ein Hauptideal von R, das von einer gewöhnlichen ganzen Zahl erzeugt wird:*

$$\mathfrak{a}\bar{\mathfrak{a}} = (n) \text{ für ein } n \in \mathbb{Z}.$$

Beweis. Seien α und β die Erzeugenden des Gitters des Ideals $\mathfrak{a}$. Es ist klar, dass diese Elemente $\mathfrak{a}$ auch als Ideal erzeugen, denn schließlich h repräsentiert das Gitter das Ideal von $\mathfrak{a}$. Weiterhin erzeugen $\bar{\alpha}$ und $\bar{\beta}$ das konjugierte Ideal $\bar{\mathfrak{a}}$. Betrachten wir nun das Ideal $\mathfrak{a}\bar{\mathfrak{a}}$, dann wissen wir dass dieses Ideal von den vier Produkten $\alpha\bar{\alpha}, \alpha\bar{\beta}, \bar{\alpha}\beta$ und $\beta\bar{\beta}$ erzeugt wird. Dies ist aus der Definition von Produktideal ersichtlich, denn wir wissen, dass wir die endlichen Summen der Produkte, je auf Linearkombinationen der Erzeugenden der miteinander multiplizierten Ideale zurückführen können.
Die drei Elemente $\alpha\bar{\alpha}, \beta\bar{\beta}$ und $\alpha\bar{\beta}+\bar{\alpha}\beta$ sind gleich mir ihren Konjugierten und daher rationale Zahlen.(Bei der Summe ist dies durch nachrechnen schnell klar.) Sie sind sogar gewöhnliche ganze Zahlen, da sie ganze algebraische Zahlen sind. Sei n ihr größter gemeinsamer Teiler in $\mathbb{Z}$. Dann ist n eine Linearkombination von $\alpha\bar{\alpha}, \beta\bar{\beta}$ und $\alpha\bar{\beta} + \bar{\alpha}\beta$ mit ganzzahligen Koeffizienten. Damit ist klar, dass n auch im Produktideal $\mathfrak{a}\bar{\mathfrak{a}}$ liegt und so $(n) \subset \mathfrak{a}\bar{\mathfrak{a}}$.
Die umgekehrte Inklusion ist gegeben, sobald gezeigt ist, dass n jedes der vier erzeugenden Elemente des Produktideals teilt.
n teilt $\alpha\bar{\alpha}$ und $\beta\bar{\beta}$ nach Konstruktion in $\mathbb{Z}$ und damit auch in R. Um zu zeigen, dass n auch die beiden anderen erzeugenden in R teilt, müssen wir zeigen, dass $\frac{\alpha\bar{\beta}}{n}$ und $\frac{\bar{\alpha}\beta}{n}$ ganze algebraische Zahlen sind. Dies ist jedoch schnell ersichtlich, da sie Nullstellen des Polynoms $x^2 - rx + s$ sind, mit $r = \frac{\alpha\bar{\beta}+\bar{\alpha}\beta}{n}$ und $s = \frac{\alpha\bar{\alpha}}{n}\frac{\beta\bar{\beta}}{n}$. Das r und s ganze Zahlen sind, liefert die Konstruktion von n, also sind $\frac{\alpha\bar{\beta}}{n}$ und $\frac{\bar{\alpha}\beta}{n}$ ganze algebraische Zahlen. Dadurch ist die zweite Inklusion $\mathfrak{a}\bar{\mathfrak{a}} \subset (n)$ gezeigt. Es folgt die Aussage des Lemmas: $\mathfrak{a}\bar{\mathfrak{a}} = (n)$. □

Lemma 3.3.3. *Seien* $\mathfrak{a} \subset \mathfrak{b}$ *Gitter in* $\mathbb{R}^2$*. Dann gibt es nur endlich viele Gitter* Γ *zwischen* $\mathfrak{a}$ *und* $\mathfrak{b}$*, das heißt, so dass* $\mathfrak{a} \subset \Gamma \subset \mathfrak{b}$ *gilt.*

Beweis. Sei P das Parallelogramm, das von einer Gitterbasis von $\mathfrak{a}$ aufgespannt wird. In diesem Parallelogramm gibt es nur endlich viele Punkte aus $\mathfrak{b}$. Falls Γ ein Gitter zwischen $\mathfrak{a}$ und $\mathfrak{b}$ ist, dann gibt es nur endlich viele Möglichkeiten für die Menge $M = \Gamma \cap P$. Dies liefert die Endlichkeit der Anzahl der Zwischengitter. Γ ist nämlich bestimmt durch seine Gitterbasis, die in N liegt.

Kommen wir jetzt zur Äquivalenzrelation auf den Idealen.

Definition 3.3.4. *Wir nennen zwei Ideale ähnlich und schreiben* $\mathfrak{a} \sim \mathfrak{b}$*, falls es Elemente* $\sigma, \tau \in R \setminus \{0\}$ *gibt, so dass*

$$\sigma\mathfrak{b} = \tau\mathfrak{a}$$

ist.
Dies ist eine Äquivalenzrelation und die Äquivalenzklassen dieser Relation werden Idealklassen genannt. Die Idealklasse eines Ideals $\mathfrak{a}$ *wird mit* $\langle\mathfrak{a}\rangle$ *bezeichnet.*

Da wir uns in einem quadratischen Zahlkörper$K = \mathbb{Q}[\delta]$ befinden, können wir die Definition auch folgendermassen umformulieren:

$$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow (\exists \lambda \in \mathbb{Q}[\delta])\mathfrak{b} = \lambda\mathfrak{a}$$

Als nächstes wollen wir diese Äquivalenzrelation unter geometrischen Aspekten betrachten.
Zwei Ideale sind ähnlich, wenn ihre Gitter in der komplexen Ebene ähnliche geometrische Figuren sind. Dies ist leicht zu erkennen, da das λ in der äquivalenten Definition eine komplexe Zahl ist und Multiplikation mit einer komplexen Zahl immer eine Drehstreckung beschreibt. Drehstreckungen sind orientierungserhaltende Abbildungen und bilden so ähnliche geometrische Figuren aufeinander ab.
Mit Hilfe dieser geometrischen Anschauung erhält man den folgenden Satz:

Satz 3.3.5. *Die Idealklasse $\langle R\rangle$ besteht aus den Hauptidealen.*

Beweis. Ein Ideal $\mathfrak{b}$ ist genau dann dem Einsideal R ähnlich, wenn es ein $\lambda \in K$ gibt, so dass $\mathfrak{b} = \lambda R$. Dann ist $\mathfrak{b}$ das Hauptideal (λ). □

Satz 3.3.6. *Die Idealklassen bilden eine abelsche Gruppe $\mathcal{K}$, wobei die Verknüpfung von der Idealmultiplikation induziert wird:*

$$\langle\mathfrak{a}\rangle\langle\mathfrak{b}\rangle = \textit{Klasse von } \mathfrak{ab} = \langle\mathfrak{ab}\rangle.$$

Beweis. Seien $\mathfrak{a} \sim \mathfrak{a}'$ und $\mathfrak{b} \sim \mathfrak{b}'$, so gibt es $\lambda, \mu \in \mathbb{Q}[\delta]$ mit $\mathfrak{a}' = \lambda\mathfrak{a}$ und $\mathfrak{b}' = \mu\mathfrak{b}$. Dann ist $\mathfrak{a}'\mathfrak{b}' = \lambda\mu\mathfrak{ab}$. Hier ist gezeigt $\langle\mathfrak{ab}\rangle = \langle\mathfrak{a}'\mathfrak{b}'\rangle$, also ist die Verknüpfung von Idealklassen wohldefiniert. Über die Idealmulitplikation ist die Kommutativität und die Assoziativität gegeben. Ebenso ist durch die Idealmultiplikation gegeben, dass die Idealklasse von R das neutrale Element bildet. Nun bleibt noch die Frage nach den Inversen. Wir wissen jdoch bereits, dass $\mathfrak{a}\bar{\mathfrak{a}} = (n)$ ein Hauptideal ist, jedoch damit in der Klasse von R, also im neutralen Element von $\mathcal{K}$, liegen.
Es gilt also $\langle\mathfrak{a}\rangle\langle\bar{\mathfrak{a}}\rangle = \langle R\rangle$, das heisst $\langle\bar{\mathfrak{a}}\rangle = \langle\mathfrak{a}\rangle^{-1}$. □

Korollar 3.3.7. *Sei R der Ring der ganzen algebraischen Zahlen eines Imaginärquadratischen Zahlkörpers.Folgende Aussagen sind dann äquivalent:*
(a) R ist ein Hauptidealring.
(b) R ist faktoriell.
(c) die Idealklassengruppe $\mathcal{K}$ ist die triviale Gruppe.

Beweis. Die Äquivalenz von (a) und (b) setzen wir als bewiesen voraus. (a)⇔(c): Ist R ein Hauptidealring, so ist jedes Ideal dem Einsideal ähnlich, also enthält die Idealklassengruppe $\mathcal{K}$ genau die Identität, nämlich $\langle R\rangle$.
Ist die Idealklassengruppe trivial, dann sind alle Ideale von R dem Einsideal ähnlich, folglich Hauptideale. □

Jetzt wird es interessant zu fragen, wieviele Idealklassen es gibt, um so ein Mass für die Nichteindeutigkeit der Faktorzerlegung von Elementen von R zu erhalten. Man nennt diese Anzahl der Idealklassen *Klassenzahl* von $K = \mathbb{Q}[\delta]$.
Es ist von Interesse sicher zu wissen, dass die Klassenzahl immer endlich ist, das bedeutet das die Idealklassengruppe $\mathcal{K}$ immer endliche Ordnung hat. Bis wir endgültig zu diesem Beweis gelangen ist noch einiges an Vorarbeit zu leisten. Eine der wichtigsten Grundlagen ist der *Minkowskische Gitterpunktsatz.*

Definition 3.3.8. *Eine beschränkte Teilmenge A der Ebene $\mathbb{R}^2$ heisst* konvex *und* zentralsymmetrisch*, wenn sie folgende Eigenschaften hat:*
(a) Konvexität*: Zu je zwei Punkten $p, q \in A$ enthält A auch die Verbindungsstrecke dieser Punkte.*
(b) Zentralsymmetrie*: Ist $p \in A$ so ist auch $-p \in A$.*

Es ist klar, dass aus diesen Bedingungen folgt, dass $0 \in A$, wenn A nicht leer ist.

Satz 3.3.9. Minkowskischer Gitterpunktsatz*: Sei Γ ein Gitter in $\mathbb{R}^2$ und A eine konvexe und zentralsymmertische Teilmenge von $\mathbb{R}^2$. Dann bezeichnet $\Delta(\Gamma)$ den Flächeninhalt des Parallelogramms, das von einer Gitterbasis von Γ aufgespannt wird, und $F(A)$ den Flächeninhalt von A. Falls $F(A) > 4\Delta(\Gamma)$ so enthält A ausser dem Nullpunkt noch einen weiteren Gitterpunkt*

Beweis. Zunächst 'schrumpfen' wir die Menge A um die Hälfte zu einer neuen konvexen und zetralsymmetrischen Teilmenge U von $\mathbb{R}^2$. Dies tun wir auf folgende Weise: $p \in U \Leftrightarrow 2p \in A$. Durch diese 'Schrumpfung' ergibt sich für den Flächeninhalt $F(U) = \frac{1}{4}F(A)$. So kann man die Voraussetzung des Satzes umformulieren:
$F(U) > \Delta(\Gamma)$.
Auf dem Weg zum Beweis des Satzes hilft es unterwegs ein Lemma zu beweisen.

Lemma 3.3.10. *Es gibt ein Element $\alpha \in \Gamma$, so dass $U \cap (U + \alpha) \neq \emptyset$.*

Beweis. Sei P das Parallelogramm, welches von einer Gitterbasis von Γ aufgespannt wird. Die verschobenen Parallelogramme $P + \alpha$, mit $\alpha \in \Gamma$ bilden eine Überdeckung der Ebene. Die einzelnen Parallelogramme schneiden sich höchstens entlang ihrer Kanten. Ordenen wir nun jedem $P + \alpha$ ein $U + \alpha$ zu. Da der Flächeninhalt von U grösser ist als der von P, müssen sich die $U + \alpha$ überschneiden. Jetzt kann man beobachten, dass die Menge U nur endlich viele $P + \alpha$ trifft. Diese bezeichnen wir mit $P + \alpha_1, ..., P + \alpha_k$.
Seien $U_i := U \cap (P + \alpha_i)$. Dann ist jetzt U in Teilmengen $U_1, ..., U_k$ zerlegt. Es ist klar, dass nun gilt $F(U) = \sum F(U_i)$. Diese U_i verschieben wir jetzt zurück nach P indem wir einfach den Translationssummanden α_i wieder abziehen. Wir definieren neue $V_i := U_i - \alpha_i = P \cap (U - \alpha_i)$. Die V_i sind also Teilmengen von P, die P überdecken, und es gilt $F(U_i) = F(V_i)$. Jetzt folgt
$\sum F(V_i) = \sum F(U_i) = F(U)\ \Delta(\Gamma) = F(P)$. Da jetzt also die Summe der Flächeninhalte der V_i grösser als der von P, was bedeutet, dass sich zwei der V_i schneiden müssen. Es gibt also $i \neq j$, so dass $(U - \alpha_i) \cap (U - \alpha_j) \neq \emptyset$ ist. Jetzt muss nur noch α_i auf beiden Seiten dieser Mengenungleichung addiert werden und wir erhalten. $U \cap (U + \alpha_i - \alpha_j) \neq \emptyset$. Wir haben also unser gesuchtes $\alpha \in \Gamma$ gefunden, nämlich $\alpha = \alpha_i - \alpha_j$.

Jetzt wollen wir den Beweis des Satzes mit Hilfe des Lemmas zu Ende bringen. Wir wählen uns also unser α genau wie im Lemma zuvor. Es ist also gegeben, dass wir einen Punkt p in $U \cap (U + \alpha)$ finden. Da $p \in U + \alpha$ wissen wir $p - \alpha \in U$. Nun benutzen wir, dass U zentralsymmetrisch ist. Hier folgt, dass auch $q := \alpha - p \in U$. Der Mittelpunkt zwischen p und q liegt wegen der Konvexität auch in U. Deshalb liegt $\alpha \in K$.
Jetzt ist der Beweis vollendet, da wir einen Punkt des Gitters gefunden haben, nämlich α, der in K liegt. □

Um später unseren angestrebten Beweisdurchführen zu können, ist es an dieser Stelle nötig noch ein Korollar zu zeigen.

Korollar 3.3.11. *Jedes Gitter Γ in $\mathbb{R}^2$ einthält einen Vektor $\alpha \neq 0$ mit*

$$|\alpha|^2 \leq \frac{4\Delta(\Gamma)}{\pi}.$$

Beweis. Wir wollen den zuvor gezeigten Minkowskischen Gitterpunktsatz (MGS) verwenden. Als konvexe, zentralsymmetrische Teilmenge von $\mathbb{R}^2$ verwenden wir einen Kreisscheibe K mit Radius r. Falls gilt, dass $\pi r^2 > 4\Delta(\Gamma)$, bzw.$r^2 < \frac{4\Delta(\Gamma)}{\pi}$, dann liegt nach MGS in K ein weiterer Gitterpunkt $\alpha \neq 0$. Für jedes $\epsilon > 0$ gibt es

also ein $\alpha \in \Gamma$, so dass $|\alpha|^2 < \frac{4\Delta(\Gamma)}{\pi+\epsilon}$. Da wir uns in K jedoch in einem beschränkten Gebiet befinden, liegen innerhalb von K nur endlich viele Gitterpunkte. Weiterhin dürfen wir ϵ so klein wählen wie wir wollen und deshalb gibt es auch einen Gitterpunkt mit $|\alpha|^2 \leq \frac{4\Delta(\Gamma)}{\pi}$, wie es das Korollar behauptet.

Weiter auf dem Weg zum Beweis, dass die Idealklassengruppe endlich ist kehren wir nun zu dem Ring des ganzen algebraischen Zahlen in einem imaginär-quadratischen Zahlkörper und seinen Idealen zurück.
Wir wollen versuchen die Grösse eines Ideals zu beschreiben. Dafür gibt es zwei Ansätze: Des Index des Ideals in R, $[R : \mathfrak{a}]$ = Anzahl der additiven Nebenklassen von von $\mathfrak{a}$ in R, das zweite ist die Norm des Ideals.

Definition 3.3.12. *Wir nennen n die Norm des Ideals $\mathfrak{a}$, falls gilt $\mathfrak{a}\bar{\mathfrak{a}} = (n)$. Wir schreiben dann $N(\mathfrak{a}) = n$.*

Natürlich überträgt sich auch hier die Multiplikativität der Norm. Es ist weiterhin zu bemerken, dass für Hauptideale gilt $N((\alpha)) = \alpha\bar{\alpha} = N(\alpha)$.
Ein Ergebnis, das hier nicht bewiesen wird, ist die Übereinstimmung der beiden Ansätze, die hier in einem Lemma formuliert ist.

Lemma 3.3.13. *Für jedes Ideal $\mathfrak{a} \neq (0)$ von R gilt $[R : \mathfrak{a}] = N(\mathfrak{a})$.*

Der folgende Satz ist ebenfalls für unseren letzten Beweis nötig ist. Auch hier ist der Beweis zu umfangreich und benutzt zu viel Vorwissen, als dass wir ihn hier aufführen wollte.

Satz 3.3.14. *Sei $\mu = 2\frac{\sqrt{|D|}}{\pi}$. Jede Idealklasse enthält ein Ideal $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq \mu$.*

Jetzt endlich können wir die Endlichkeit der Klassenzahl folgern:

Satz 3.3.15. *Die Idealklassengruppe $\mathcal{K}$ ist endlich.*

Beweis. Mit dem vorausgegangenen Lemma und dem Satz zuvor ist alles was noch zu zeigen ist, dass es endlich viele Ideale gibt, deren Index nicht grösser ist als μ. Dies ist der Fall, da wir ja wissen, dass in jeder Idealklasse eines der Ideal, dessen Norm kleiner oder gleich μ ist, enthalten ist. Wenn es also nur endlich viele Ideale mit dieser Eigenschaft gibt, dann wird klar, dass es auch nur endlich viele Idealklassen geben kann. Also folgt hier die Endlichkeit der Idealklassengruppe.
Da die Ideale in R aber immer Untergitter sind, reicht es also sicher zu zeigen, dass es nur endlich viele Untergitter $\Gamma \subset R$ gibt, mit $[R : \Gamma] \leq \mu$ gibt.Um dies zu zeigen, wählen wir eine natürliche Zahl $n \leq \mu$ und nehmen an, Γ sei ein Untergitter für welches gilt $[R : \Gamma] = n$. Betrachtet man nun den Quotientenraum R/Γ, so befinden wir uns in einer abelschen Gruppe der Ordnung n. Also ist die Multiplikation mit n auf diesem Raum die Nullabbildung. Es gilt also für alle Nebenklassen $a + \Gamma$ mit $a \in R$, dass $na + \Gamma = \Gamma$. Daraus ergibt sich f"ur R, dass $nR \subset \Gamma$. Jetzt wissen wir also, dass jedes Untergitter vom Index n auf jeden Fall nR enthält.
Nach einem Lemma über Zwischengitter, gibt es nur endlich viele solcher Gitter die nR enthalten und selbst in R enthalten sind. Da auch die Wahl für n endlich war, ist nund gezeigt, dass es nur endlich viele Untergitter mit Index kleiner oder gleich μ gibt. Damit ist der Beweis, dass die Idealklassengruppe endlich ist fertig! □

4

Reell quadratische Zahlkörper

Nun befassen wir uns also mit den positiv erzeugten Körpern $K = \mathbb{Q}[\sqrt{d}]$ mit $d > 0$. Natürlich betrachten wir auch hier wieder den Ring der ganzen algebraischen Zahlen in K.
Zuerst überlegen wir uns, dass $\mathbb{Q}[\sqrt{d}]$ ein Unterkörper von $\mathbb{R}$ ist. Es lassen sich also Teilmenge dieses Körpers, wie die ganzen algebraischen Zahlen, nicht mehr als Gitter in $\mathbb{C}$ einbetten.
Wir möchten uns ab hier auf den Fall $d \equiv_4 2$ oder 3 beschränken, da alles weitere für den Fall $d \equiv_4 1$ analog geht. Man muss dafür nur konsequent alle δ durch η ersetzen.

4.1 Die (u, v)-Ebene

Es erweist sich als nützlich nicht einfach $\mathbb{Q}[\sqrt{d}]$ als zwei-dimensionalen Vektorraum über $\mathbb{Q}$ aufzufassen und sein Gitter $\mathbb{Z}[\delta]$ dorthin zu legen. Wir brauchen auch einen Art Konjugation in unserem quadratischen Zahlkörper um die Analogie zu den Sätzen für imaginär quadratischen Zahlkörpern herzustellen.

Definition 4.1.1. *In einem reell-quadratischen Zahlkörper $\mathbb{Q}[\delta]$ ist das Konjugierte einer Zahl $z = a + b\delta$ folgendes: $\bar{z} := a - b\delta$.*

Wir betrachten nun die (u, v)-Ebene:$= (\mathbb{Q}[\delta])^2$ und bilden eine ganze algebraische Zahl z auf $(z, \bar{z})$ ab. So entsteht aus dem Ring $\mathbb{Z}[\delta]$ wieder ein Gitter. Als Norm benutzen wir wie im imaginär quadratischen Fall die Abbildung
$N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Z} : z \mapsto z\bar{z}$. Allerdings wird hier die von uns neu definierte Konjugation benutzt. Eine kleine Beobachtung liefert das Lemma.

Lemma 4.1.2. *Die Norm einer ganzen algebraischen Zahl ist eine ganze Zahl.*

Beweis. Sei z eine ganze algebraische Zahl.
Ist $d \equiv_4 2$ oder 3, so hat z die Form $a + b\delta$. Wir erkennen durch umformen:
$N(z) = z\bar{z} = (a + b\delta)(a - b\delta) = a^2 - b^2 d$
Da a, b, d in $\mathbb{Z}$ liegen sind wir in diesem Fall schon fertig.
Ist $d \equiv_4 1$, so hat z die Form $\frac{m}{2} + \frac{n}{2}\delta$ für ungerade m und n. Wir formen wieder etwas um:
$N(z) = z\bar{z} = (\frac{m}{2} + \frac{n}{2}\delta)(\frac{m}{2} - \frac{n}{2}\delta) = (\frac{m}{2})^2 - (\frac{n}{2})^2 d = \frac{m^2 - n^2 d}{4}$
Wir wissen aber noch dass: $m^2 - n^2 * d \equiv_4 (\pm 1)^2 - (\pm 1)^2 * 1 \equiv_4 0$
Daraus folgt die Behauptung. □

Mit den so getroffenen Definitionen lassen sich viele Sätze für imaginär quadratische Körper einfach eins-zu-eins auf reell quadratische übertragen...

4.2 Der geometrische Unterschied

Der erste Unterschied zwischen den reell und imaginär quadratischen Zahlkörpern ist, dass die geometrische Interpretationsmöglichkeit über die Ähnlichkeit von Gittern wegfällt. Im imaginären Fall konnten wir sagen, dass alle Gitter aus einer Klasse durch die Multiplikation mit einem $\lambda \in \mathbb{Q}[\delta]$ ineinander überführbar sind. Dies entsprach einer bestimmten Drehstreckung.
Im reellen Fall müssen wir hier feststellen, dass sich die Ähnlichkeit der Gitter einer Klasse nicht mehr geometrisch sondern nur noch rechnerisch erkennen lässt. Die Multiplikation mit dem $\lambda = a + b\delta$ ist jetzt nicht mehr eine Drehstreckung in der komplexen Ebene, sondern sie Streckt die u-Koordinate um $a + b\delta$ und die v-Koordinate um $a - b\delta$. Die Ähnlichkeit dieser Form kann man im allgemein nicht mehr an den Bildern der Gitter erkennen.

4.3 Der Einheiten-Unterschied

Der zweite Unterschied ist etwas positiver und dafür schwer zu glauben. Wir werden zeigen, dass in einem reell quadratischen Zahlkörper $K := \mathbb{Q}[\delta]$ der Ring der ganzen Zahlen $R := \mathbb{Z}[\delta]$ unendlich viele Einheiten hat!
Wir überlegen uns zuerst, wie man die Einheiten in der (u, v)-Ebene schnell erkennen kann. Ein Punkt ist genau dann eine Einheit, wenn er Norm eins hat. Sei $z = a + b\delta$ eine Einheit in R. $N(z) = z\bar{z} = \pm 1$. Betrachten wir z als Punkt der (u, v) Ebene bedeutet dies: $z\bar{z} = u(z)v(z) = \pm 1$. Wir betrachten also in der Ebene die beiden Hyperbeln $uv = 1$ und $uv = -1$. Also ist jeder Punkt des Gitters, der eine davon schneidet ist eine Einheit und jede Einheit sitzt auf den Hyperbeln.
Wir arbeiten uns jetzt langsam dahin vor, dass es da unendlich viele Einheiten in R gibt. Wir beginnen mit einem Lemma.

Lemma 4.3.1. *Es sei Δ der Flächeninhalt des Parallelogramms, das von einer Gitterbasis von R in der (u, v)-Ebene E aufgespannt wird. Dann gibt es unendlich viele Elemente $z \in R$ deren Norm beschränkt ist.* $(\exists B > \Delta)\ |N(z)| \leq B$

Beweis. Als B nehmen wir irgendeine reelle Zahl, die größer als Δ ist. Um nun in der Ebene die Punkte zu finde, deren Norm betraglich kleiner als B ist formen wir folgende Ungleichung etwas um:
$|N(z)| \leq B$
$-B \leq N(z) \leq B$
$-B \leq u(z)v(z) \leq B$
Also suchen wir genau die Punkte z der Ebene, die zwischen den Hyperbeln $u(z)v(z) = B$ und $u(z)v(z) = -B$ liegen.
Um den Minkowskischen Gitterpunktsatz zu verwenden basteln wir uns jetzt ein Rechteck zwischen den Hyperbeln. Sei $r \in \mathbb{R}^+$ eine beliebige positive reelle Zahl. Dann sind folgende vier Punkte die Ecken eines Rechtecks, dass zwischen und auf den Hyperbeln liegt:
$(r, B/r)$; $(r, -B/r)$; $(-r, B/r)$; $(-r, -B/r)$
Da das Produkt der u und v Koordinate für jeden Punkt $\pm B$ ergibt, liegen die Punkte auf jeden Fall auf den Hyperbeln. Anhand der Koordinaten kann man auch schnell erkennen, dass sie Eckpunkte eines Rechtecks sind. Der Flächeninhalt dieses Rechtecks sei F. Er berechnet sich leicht:
F = u-Achsen Seitenlänge * v-Achsen Seitenlänge
$= 2r * 2B/r = 4B$
Da $B > \Delta$ gewählt wurde ist auch $F = 4B > 4\Delta$. Das Rechteck ist eine konvexe zentralsymmetrische Teilmenge des $\mathbb{R}^2$. Damit sind alle Bedingungen für den

Minkowskis Gitterpunktsatz erfüllt und wir wissen, das es innerhalb des Rechtecks einen Punkt $z \neq 0$ aus R gibt.
Wir stellen fest, dass dieser Punkt nicht auf einer der Achsen liegen kann, da alle Achsenpunkte eine Nullkoordinate und somit auch die Norm Null haben. Der einzige Punkt aus R mit Norm Null ist aber schon die Null selber. Also kann der Punkt $z \in R \setminus \{0\}$ aus Minkowskis Satz nicht auf den Achsen liegen.
Wenn man sich nun vorstellt wie die Rechtecke sich verändern, wenn wir r gegen unendlich gehen lassen, so erkennt man wie sie immer flacher und breiter werden und sich an die v-Achse schmiegen. Wir fangen also mit irgendeinem $r_1 > 0$ an und lassen uns in seinem Rechteck A_1 ein z_1 finden. Dann nehmen wir $r_2 > r_1$ so groß, dass $z_1 \notin A_2$ ist. Das geht, weil die Rechtecke beliebig flach werden. Nun lassen wir uns z_2 darin finden. So kann man das beliebig fortsetzen, da die reellen Zahlen, wo die r_i herkommen ja nicht nach oben beschränkt sind.
Es gibt also unendlich viele Punkte $z \in R \setminus \{0\}$ innerhalb dieser Rechtecke. Da alle Rechtecke immernoch zwischen den Hyperbeln liegen sind die Punkte in der Norm immer durch B und $-B$ beschränkt. Hieraus folgt das Lemma. □

Das aus diesem Lemma folgende Korollar ist zwar klein und leicht zu zeigen aber auch sehr wichtig.

Korollar 4.3.2. *Es existiert eine Zahl $n \in \mathbb{Z}$, so dass es in R unendlich viele Elemente mit Norm n gibt.*

Beweis. Nach dem Lemma wissen wir es gibt ein B, so dass für unendlich viele z aus R gilt: $-B \leq N(z) \leq B$. Für alle $z \in R$ wissen wir, dass $N(z)$ eine ganze Zahl ist. In dem Intervall $[-B, B]$ gibt es aber nur endlich viele ganze Zahlen, also muss mindestens eine davon die Norm von unendlich vielen Elementen aus R sein. □

Nach einem weiteren kleinen Lemma über die Einheiten von R können wir dann alles in einem schönen Satz zusammenfassen.

Lemma 4.3.3. *Es seien x, y zwei Elemente in R, die beide Norm n haben. Weiterhin sei $x \equiv_n y :\Leftrightarrow \frac{x-y}{n} \in R$. Dann ist $\frac{x}{y}$ eine Einheit in R.*

Beweis. Es genügt zu zeigen, dass $\frac{x}{y}$ überhaupt in R liegt, da damit analog gezeigt ist, dass sein Inverses $\frac{y}{x}$ auch in R liegt.
Da für jedes Ringelement das sein Konjugiertes auch im Ring ist gilt:
$\frac{x-y}{n} \in R \Rightarrow \overline{(\frac{x-y}{n})} = \frac{\bar{x}-\bar{y}}{\bar{n}} = \frac{\bar{x}-\bar{y}}{n} \in R \Rightarrow \bar{x} \equiv_n \bar{y}$
Wir Formen $\frac{x}{y}$ nun ein wenig um:
$\frac{x}{y} = \frac{x\bar{y}}{y\bar{y}} = \frac{x\bar{y}}{n}$.
Ein letztes umformen ergibt nun:
$x\bar{y} \equiv_n x\bar{x} \equiv_n n \equiv_n 0 \Rightarrow \frac{x\bar{y}}{n} = \frac{x}{y} \in R$ □

Jetzt fehlt nur noch der Satz bei dem alle Lemmas benutzt werden und hier ist er!

Satz 4.3.4. *Der Ring R der ganzen algebraischen Zahlen in einem reell-quadratischen Zahlkörper enthält unendlich viele Einheiten.*

Beweis. Nach dem letzten Korollar wissen wir: Es existiert eine ganze Zahl n, so dass es in R unendlich viele Elemente mit Norm n gibt. Wir betrachten nun all diese Elemente und tun sie in eine neue Menge M.
Diese Menge unterteilen wir jetzt in Kongruenzklassen modulo a. Wir verfahren wie in Lemma 4.3.3: $x \equiv_n y :\Leftrightarrow \frac{x-y}{n} \in R$. Das bedeutet für zwei Elemente $x, y \in M$:
$x \equiv_n y \Leftrightarrow \frac{x-y}{n} = \frac{(a+b\delta)-(c+d\delta)}{n} = \frac{a-c}{n} + \frac{b-d}{n}\delta \Leftrightarrow a \equiv_n c$ und $b \equiv_n d$.
Da a, b, c, d ganze Zahlen sind. Ist der letzte Ausdruck ein normaler Modulo in $\mathbb{Z}_n$!

Wenn wir also M in Kongruenzklassen einteilen. So ist das gleichbedeutend damit zweimal $\mathbb{Z}$ in Kongruenzklassen modulo n einzuteilen. Wir brauchen für den Beweis allerdings nur die Information, dass wir auf M endlich viele Kongruenzklassen haben. Dies ist aber klar, weil man auf $\mathbb{Z}$ nur endlich viele hat. Da wir in M unendlich viele Elemente haben, muss es eine Kongruenzklasse mit unendlich vielen Elementen geben. Nach Lemma 4.3.3 sind alle Quotienten von Elementen dieser Klasse Einheiten in R. Da es unendlich viele Elemente gibt, gibt's auch unendlich viele Quotienten. Das beendet den Beweis. □