

Kapitel 6

Quadratische Zahlkörper

Ein Zahlkörper ist ein Körper K , der den Körper \mathbb{Q} der rationalen Zahlen enthält und als \mathbb{Q} -Vektorraum endlichdimensional ist. Im zweidimensionalen Fall reden wir von quadratischen Zahlkörpern. Die algebraische Zahlentheorie untersucht die (noch zu definierenden) ganzen Zahlen eines solchen Zahlkörpers. In dieser Vorlesung geht es zwar eher um elementare als um algebraische Zahlentheorie, jedoch werden wir im nächsten Kapitel sehen, daß ein Umweg über quadratische Zahlkörper auch bei rein ganzzahligen Problemen gelegentlich hilfreich sein kann.

§1: Grundbegriffe der Ringtheorie

Als erstes wollen wir uns überlegen, in welchen Zahlbereichen außer \mathbb{Z} wir noch sinnvoll von Teilbarkeit und eventuell auch Division mit Rest reden können. Wir brauchen dazu selbstverständlich zumindest eine Addition und eine Multiplikation, d.h. einen der bereits in Kapitel 1, §6 definierten *Ringe*. Wenn wir eindeutige Quotienten wollen, müssen wir aber noch zusätzlich voraussetzen, daß es keine sogenannte *Nullteiler* gibt, d.h. von null verschiedene Elemente r, s , deren Produkt gleich null ist. Ist nämlich $y = qs$, so ist dann auch $y = (q + r)s$, was unserer Vorstellung von Teilbarkeit mit eindeutig bestimmtem Quotienten widerspricht.

Definition: a) Ein Ring heißt *nullteilerfrei* wenn gilt: Ist $x \cdot y = 0$, so muß mindestens einer der beiden Faktoren x, y verschwinden. Ein nullteilerfreier kommutativer Ring heißt *Integritätsbereich* (englisch *domain*).

- b) Wir sagen, ein Element u eines Integritätsbereichs R sei *Teiler* von $x \in R$, in Zeichen $u|x$, wenn es ein $q \in R$ gibt, so daß $x = q \cdot u$.
- c) $u \in R$ heißt *größter gemeinsamer Teiler* von x und y , wenn u Teiler von x und von y ist und wenn für jeden anderen gemeinsamen Teiler v von x und y gilt: $v|u$.
- d) Ein Element $e \in R$ heißt *Einheit*, falls es ein $e' \in R$ gibt mit $e \cdot e' = 1$. Die Menge aller Einheiten von R bezeichnen wir mit R^\times .
- e) Zwei Elemente $x, y \in R$ heißen *assoziiert*, wenn es eine Einheit $e \in R$ gibt, so daß $y = e \cdot x$.

Der Prototyp eines kommutativen Rings ist der Ring \mathbb{Z} der ganzen Zahlen; er ist ein Integritätsbereich mit ± 1 als einzigen Einheiten. Zwei ganze Zahlen sind somit genau dann assoziiert, wenn sie denselben Betrag haben. Man beachte, daß im Sinne der obigen Definition sowohl $+2$ als auch -2 ein größter gemeinsamer Teiler von 4 und 10 ist; der ggT ist also nicht eindeutig bestimmt.

Der Ring \mathbb{Z}/m ist genau dann nullteilerfrei, wenn m prim ist; in diesem Fall ist er sogar ein Körper. Ist aber $m = ab$ eine Zerlegung (in \mathbb{N}) von m in ein Produkt mit $a, b > 1$, so ist in \mathbb{Z}/m zwar $ab = 0$, aber $a, b \neq 0$.

Die Menge aller $n \times n$ -Matrizen über einem Körper ist ein Beispiel für einen der hier ausgeschlossenen nichtkommutativen Ringe. Er ist nicht nullteilerfrei, enthält aber viele Einheiten, die invertierbaren Matrizen.

Auch die Polynome über einem Körper k bilden einen Ring, den Polynomring $k[X]$. Auch er ist ein Integritätsbereich:

Lemma: Ist R ein Integritätsbereich, so auch der Polynomring

$$R[X] = \left\{ \sum_{i=0}^n a_i X^i \mid n \in \mathbb{N}_0, a_i \in R \right\}.$$

Seine Einheiten sind genau die Einheiten von R .

Beweis: Wenn wir Addition und Multiplikation nach den üblichen Regeln definieren, ist klar, daß $R[X]$ alle Ringaxiome erfüllt. Um zu

zeigen, daß $R[X]$ nullteilerfrei ist, betrachten wir zwei Polynome

$$f = \sum_{i=0}^n a_i X^i \quad \text{und} \quad g = \sum_{j=0}^m b_j X^j,$$

die beide von Null verschieden sind. Wir können etwa annehmen, daß n und m so gewählt sind, daß a_n und b_m beide nicht verschwinden. Da R Integritätsbereich ist, kann dann auch das Produkt $a_n b_m$ nicht verschwinden, also ist der führende Term $a_n b_m X^{n+m}$ von fg von Null verschieden und damit auch fg selbst. Tatsächlich beweist dies sogar etwas mehr als die Nullteilerfreiheit, denn wir wissen nun, daß sich bei der Multiplikation zweier Polynome die Grade addieren.

Ist $f \in R[X]$ eine Einheit, so gibt es ein $g \in R[X]$ mit $fg = 1$; da das konstante Polynom 1 den Grad null hat, muß dasselbe auch für f und g gelten, d.h. $f, g \in R$ und damit in R^\times . ■

Für jeden Ring R gilt

Lemma: a) Die Menge R^\times aller Einheiten von R ist eine abelsche Gruppe bezüglich der Multiplikation.

b) Ein kommutativer Ring R ist genau dann ein Integritätsbereich, wenn die folgende *Kürzungsregel* erfüllt ist: Gilt für $x, y, z \in R$ und $z \neq 0$ die Gleichung $xz = yz$, so ist $x = y$.

c) Zwei Elemente x, y eines Integritätsbereich R sind genau dann assoziiert, wenn $x|y$ und $y|x$.

d) Ein größter gemeinsamer Teiler, so er existiert, ist bis auf Assoziiertheit eindeutig bestimmt.

Beweis: a) Sind $e, f \in R$ Einheiten, so gibt es Elemente e', f' mit $ee' = ff' = 1$. Damit ist $(ef)(f'e') = e(ff')e' = ee' = 1$, d.h. auch ef ist eine Einheit. Außerdem ist jede Einheit invertierbar, denn offensichtlich ist e' ein multiplikatives Inverses zu e .

b) Ist R ein Integritätsbereich und $xz = yz$, so ist $(x - y)z = 0$; da $z \neq 0$ vorausgesetzt war, folgt $x - y = 0$, also $x = y$. Folgt umgekehrt aus $xz = yz$ und $z \neq 0$ stets $x = y$, so ist R nullteilerfrei, denn ist $xy = 0$ und $y \neq 0$, so ist $xy = 0y$, also $x = 0$.

c) Ist $y = ex$, so ist x ein Teiler von y . Da Einheiten invertierbar sind, ist auch $x = e^{-1}y$, d.h. $y|x$.

Gilt umgekehrt $x|y$ und $y|x$, so gibt es Elemente q, q' mit $x = qy$ und $y = q'x$. Damit ist $1x = x = (qq')x$, also $qq' = 1$. Somit ist q eine Einheit.

d) Sind u, v zwei größte gemeinsame Teiler von x, y , so ist nach Definition u Teiler von v und v Teiler von u , also sind u und v assoziiert. ■

Manchmal haben wir sogar eine eindeutige Primzerlegung im folgenden Sinn:

Definition: a) Ein Element x eines Integritätsbereichs R heißt *irreduzibel*, falls gilt: x ist keine Einheit, und ist $x = yz$ das Produkt zweier Elemente aus R , so muß y oder z eine Einheit sein.

b) Ein Integritätsbereich R heißt *faktoriell* oder *ZPE-Ring*, wenn gilt: Jedes Element $x \in R$ läßt sich bis auf Reihenfolge und Assoziiertheit eindeutig schreiben als Produkt $x = u \prod_{i=1}^r p_i^{e_i}$ mit einer Einheit $u \in R^\times$, irreduziblen Elementen $p_i \in R$ und natürlichen Zahlen e_i .

(ZPE steht für Zerlegung in Primfaktoren Eindeutig.)

Lemma: In einem faktoriellen Ring gibt es zu je zwei Elementen x, y einen größten gemeinsamen Teiler.

Beweis: Wir wählen zunächst aus jeder Klasse assoziierter irreduzibler Elemente einen Vertreter; für die Zerlegung eines Elements in ein Produkt irreduzibler Elemente reicht es dann, wenn wir nur irreduzible Elemente betrachten, die Vertreter ihrer Klasse sind.

Sind $x = u \prod_{i=1}^r p_i^{e_i}$ und $y = v \prod_{j=1}^s q_j^{f_j}$ mit $u, v \in R^\times$ und p_i, q_j irreduzibel die entsprechenden Zerlegungen von x und y in Primfaktoren, so können wir, indem wir nötigenfalls Exponenten null einführen, o.B.d.A. annehmen, daß $r = s$ ist und $p_i = q_i$ für alle i . Dann ist offenbar $\prod_{i=1}^r p_i^{\min(e_i, f_i)}$ ein ggT von x und y , denn $z = \prod_{i=1}^r p_i^{g_i}$ ist genau dann Teiler von x , wenn $g_i \leq e_i$ für alle i , und Teiler von y , wenn $g_i \leq f_i$. ■

§2: Die Elemente quadratischer Zahlkörper

Ein quadratischer Zahlkörper ist ein Zahlkörper, der als \mathbb{Q} -Vektorraum betrachtet die Dimension zwei hat. Es gibt daher ein von der Eins linear

unabhängiges Element α . Die drei Elemente $1, \alpha, \alpha^2$ müssen aber linear abhängig sein; es gibt also rationale Zahlen p, q, r , so daß $p\alpha^2 + q\alpha + r$ verschwindet. Indem wir mit dem Hauptnenner von p, q, r multiplizieren, erhalten wir eine entsprechende Gleichung mit ganzzahligen Koeffizienten, und wenn wir dann noch durch deren ggT dividieren, erhalten wir teilerfremde ganze Zahlen A, B, C , so daß $A\alpha^2 + B\alpha + C = 0$ ist.

Nach der Lösungsformel für quadratische Gleichungen folgt

$$\alpha = -\frac{B}{2A} \pm \frac{\sqrt{B^2 - 4AC}}{2A}.$$

Den Ausdruck $\Delta = B^2 - 4AC$ unter der Wurzel bezeichnen wir als die *Diskriminante* von α . Für $\alpha = \sqrt{W}$ mit $W \in \mathbb{Z}$ beispielsweise ist $A = 1, B = 0$ und $C = -W$, also $\Delta = 4W$. Für $\alpha = \frac{1}{3} + \frac{1}{5}\sqrt{2}$ haben wir die Gleichung

$$\alpha^2 - \frac{2}{3}\alpha + \frac{1}{9} - \frac{2}{25} = \alpha^2 - \frac{2}{3}\alpha + \frac{7}{225} = 0 \implies 225\alpha^2 - 150\alpha + 7 = 0;$$

hier ist die Diskriminante somit $\Delta = 150^2 - 4 \cdot 225 \cdot 7 = 16200$.

Wegen der Irrationalität von α muß auch $\sqrt{\Delta}$ irrational sein, d.h. Δ ist kein Quadrat. Wegen der Eindeutigkeit der Primzerlegung in \mathbb{Z} können wir ganze Zahlen $Q, D \in \mathbb{Z}$ finden, so daß $\Delta = Q^2 D$ und $\sqrt{\Delta} = Q\sqrt{D}$ ist mit einer quadratfreien Zahl D , d.h. einer Zahl D , die durch keine Quadratzahl ungleich eins teilbar ist. Somit läßt sich α in der Form $r + s\sqrt{D}$ schreiben mit $r, s \in \mathbb{Q}$. Da K als \mathbb{Q} -Vektorraum zweidimensional ist, läßt sich jedes Element von K so schreiben, als Vektorraum ist also $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$.

Umgekehrt ist $\mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$ für jedes Nichtquadrat D ein Körper, denn natürlich liegen Summe und Differenz zweier Elemente wieder in diesem Vektorraum und wegen

$$(r + s\sqrt{D})(u + v\sqrt{D}) = (ru + svD) + (rv + su)\sqrt{D}$$

auch das Produkt. Für den Quotienten können wir wie bei den komplexen Zahlen über die dritte binomische Formel argumentieren:

$$\frac{r + s\sqrt{D}}{u + v\sqrt{D}} = \frac{(r + s\sqrt{D})(u - v\sqrt{D})}{(u + v\sqrt{D})(u - v\sqrt{D})} = \frac{ru - svD}{u^2 - v^2D} + \frac{su - rv}{u^2 - v^2D}.$$

Wir bezeichnen diesen Körper kurz mit $K = \mathbb{Q}[\sqrt{D}]$.

Für $D > 0$ ist $\mathbb{Q}[\sqrt{D}]$ ein Teilkörper von \mathbb{R} ; wir reden in diesem Fall von einem *reellquadratischen* Zahlkörper. Falls $D < 0$, gibt es in $\mathbb{Q}[\sqrt{D}]$ auch imaginäre Elemente; hier reden wir von einem *imaginärquadratischen* Zahlkörper.

§3: Die Hauptordnung eines Zahlkörpers

Jede rationale Zahl ist Lösung einer linearen Gleichung $aX + b = 0$ mit ganzzahligen Koeffizienten a, b , von denen der erste nicht verschwinden darf; sie ist genau dann eine ganze Zahl, wenn man $a = 1$ wählen kann.

Entsprechend ist jedes Element x eines Zahlkörpers K Lösung einer Polynomgleichung

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = 0 \quad \text{mit} \quad a_i \in \mathbb{Z},$$

denn da K nach Definition ein endlichdimensionaler \mathbb{Q} -Vektorraum ist, können die Potenzen von x nicht allesamt linear unabhängig sein. Es gibt also für irgendein n eine lineare Abhängigkeit

$$\lambda_n x^n + \lambda_{n-1} x^{n-1} + \cdots + \lambda_1 x + \lambda_0 = 0 \quad \text{mit} \quad \lambda_i \in \mathbb{Q}.$$

Multiplikation mit dem Hauptnenner der Koeffizienten λ_i macht daraus eine Polynomgleichung mit ganzzahligen Koeffizienten.

Definition: Ein Element x eines Zahlkörpers K heißt *ganz*, wenn es einer Polynomgleichung

$$x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

mit ganzzahligen Koeffizienten $a_i \in \mathbb{Z}$ und höchstem Koeffizienten eins genügt.

Man kann relativ einfach zeigen, daß die ganzen Zahlen in einem Zahlkörper K einen Ring bilden; da wir uns hier aber auf quadratische Zahlkörper beschränken, bei denen wir dies ganz explizit sehen können, sei hier auf einen solche Beweis verzichtet.

Wir betrachten also einen quadratischen Zahlkörper $K = \mathbb{Q}[\sqrt{D}]$. Ein Element $\alpha = r + s\sqrt{D}$ mit $r, s \in \mathbb{Q}$ ist genau dann ganz, wenn es einer Gleichung der Form $x^2 + ax + b = 0$ genügt mit $a, b \in \mathbb{Z}$. Da

$$x^2 = (r + s\sqrt{D})^2 = (r^2 + s^2D) + 2rs\sqrt{D}$$

ist, genügt x der Gleichung

$$x^2 - 2rx + (r^2 - s^2D) = 0.$$

Somit müssen $c = 2r$ und $d = r^2 - s^2D$ ganze Zahlen sein.

Für $r \in \mathbb{Z}$ ist die erste Bedingung trivialerweise erfüllt und die zweite genau dann, wenn auch s eine ganze Zahl ist: Da D keinen Nenner hat, ist der Nenner von $r^2 - s^2D$ in diesem Fall das Quadrat des Nenners von s .

Falls r keine ganze Zahl ist, muß es wegen der ersten Bedingung von der Form $r = c/2$ sein mit einer ungeraden Zahl c . Notwendige Bedingung für die Ganzheit von $r^2 - s^2D$ ist dann, daß auch $s = e/2$ von dieser Form ist. Dann ist

$$r^2 - s^2D = \frac{c^2 - e^2D}{4} \in \mathbb{Z} \implies c^2 - e^2D \equiv 0 \pmod{4}.$$

c und e sind ungerade Zahlen; ihre Quadrate sind also kongruent eins modulo vier. Somit ist $r^2 - s^2D$ genau dann ganz, wenn $D \equiv 1 \pmod{4}$ ist.

In $\mathbb{Q}[\sqrt{D}]$ ist ein Element $r + s\sqrt{D}$ daher für $D \not\equiv 1 \pmod{4}$ genau dann ganz, wenn r und s beide ganz sind; die Menge der ganzen Zahlen ist also $\mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$. Diese Menge ist offensichtlich eine abelsche Gruppe bezüglich der Addition, und da das Quadrat von \sqrt{D} die ganze Zahl D ist, ist sie auch abgeschlossen bezüglich der Multiplikation; die ganzen Zahlen bilden also einen Ring.

Im Fall $D \equiv 1 \pmod{4}$ ist $r + s\sqrt{D}$ auch ganz, wenn r und s beide jeweils die Hälfte einer ungeraden Zahl sind. Insbesondere ist also auch

$$\beta_D = \frac{1 + \sqrt{D}}{2}$$

eine ganze Zahl, und offensichtlich sind die ganzen Zahlen genau die Zahlen, die sich als $u + v\beta_D$ mit $u, v \in \mathbb{Z}$ schreiben lassen. Die Menge der ganzen Zahlen ist also $\mathbb{Z} \oplus \mathbb{Z}\beta_D$. Auch dies ist ein Ring, denn

$$\beta_D^2 = \frac{1 + 2\sqrt{D} + D}{4} = \frac{D-1}{4} + \frac{1 + \sqrt{D}}{2} = \frac{D-1}{4} + \beta_D$$

liegt wieder in dieser Menge, da $(D-1)/4$ im Fall $D \equiv 1 \pmod{4}$ eine ganze Zahl ist.

Die ganzen Zahlen in $\mathbb{Q}[\sqrt{D}]$ bilden also in jedem Fall einen Ring; diesen Ring bezeichnen wir als die *Hauptordnung* $\mathcal{O} = \mathcal{O}_D$ von $\mathbb{Q}[\sqrt{D}]$. Wie wir gerade gesehen haben, ist somit

$$\mathcal{O}_D = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\sqrt{D} & \text{falls } D \not\equiv 1 \pmod{4} \\ \mathbb{Z} \oplus \mathbb{Z}\beta_D \text{ mit } \beta_D = \frac{1}{2}(1 + \sqrt{D}) & \text{falls } D \equiv 1 \pmod{4} \end{cases}.$$

Beim Körper $K = \mathbb{Q}[i]$ der komplexen Zahlen mit rationalem Real- und Imaginärteil ist $D = -1 \equiv 3 \pmod{4}$, also ist die Hauptordnung hier einfach $\mathcal{O}_{-1} = \mathbb{Z} \oplus \mathbb{Z}i$, die sogenannten ganzen GAUSSschen Zahlen. Für $D = -3 \equiv 1 \pmod{4}$ dagegen ist auch $\beta_{-3} = \frac{1}{2}(1 + \sqrt{-3})$ eine ganze Zahl und $\mathcal{O}_{-3} = \mathbb{Z} \oplus \mathbb{Z}\beta_{-3}$.

Dieses Beispiel wirft die Frage auf, ob unsere Definition ganzer Zahlen wirklich so geschickt war: Wir hätten schließlich auch einfach definieren können, daß $r + s\sqrt{D}$ genau dann ganz heißen soll, wenn r und s ganze Zahlen sind.

Einer der Gründe ist sicherlich, daß wir in nichtquadratischen Zahlkörpern keine ausgezeichneten Elemente wie \sqrt{D} haben, und selbst im quadratischen Fall ist \sqrt{D} nicht immer das einzige ausgezeichnete Element. Im Falle $D = -3$ beispielsweise ist $\beta_{-3} = \frac{1}{2}(1 + \sqrt{-3})$ eine primitive sechste Einheitswurzel, und es gibt keinen Grund, diese als „weniger ganz“ oder „weniger ausgezeichnet“ zu betrachten als $\sqrt{-3}$.

Viel wichtiger ist aber, daß wir nur bei dieser Definition der Ganzheit eine Chance auf eindeutige Primzerlegung in der Hauptordnung haben:

Definition: a) Sind $R \leq S$ Integritätsbereiche, so heißt ein Element $x \in S$ ganz über R , wenn es einer Gleichung

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1x + r_0 = 0 \quad \text{mit } r_i \in R$$

genügt.

b) R heißt ganzabgeschlossen oder normal, wenn jedes über R ganze Element des Quotientenkörpers K von R in R liegt.

Satz: Ein faktorieller Ring ist ganzabgeschlossen.

Beweis: Jedes Element x des Quotientenkörpers eines Rings R kann als Quotient $x = p/q$ mit $p, q \in R$ dargestellt werden. Falls R faktoriell ist, können wir dabei annehmen, daß p und q teilerfremd sind. x ist genau dann ganz über R , wenn es ein $n \in \mathbb{N}$ und Elemente $r_0, \dots, r_{n-1} \in R$ gibt derart, daß

$$x^n = -r_{n-1}x^{n-1} - \dots - r_1x - r_0$$

ist. Multiplikation mit q^n macht daraus die Gleichung

$$p^n = -r_{n-1}p^{n-1}q - \dots - r_1pq^{n-1} - r_0q^n.$$

Hier ist die rechte Seite durch q teilbar, also auch die linke. Da p und q als teilerfremd vorausgesetzt war, ist das nur möglich, wenn q eine Einheit ist, d.h. $x = p/q$ liegt in R . ■

§4: Normen und Spuren in quadratischen Zahlkörpern

Beginnen wir mit einem Beispiel: Die Hauptordnung von $K = \mathbb{Q}[\sqrt{-5}]$ ist $\mathcal{O}_{-5} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-5}]$, und dort haben wir die beiden Produktzerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Folgt daraus, daß \mathcal{O}_{-5} nicht faktoriell ist?

Bevor wir diese Frage beantworten können, müssen wir zunächst wissen, ob möglicherweise die Faktoren auf der rechten Seite noch weiter zerlegt werden können. Solche Fragen lassen sich oft entscheiden, indem man die *Normen* der beteiligten Elemente betrachtet.

Definition: a) Für ein Element $\alpha = r + s\sqrt{D}$ von $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$ heißt $\bar{\alpha} = r - s\sqrt{D}$ das zu α konjugierte Element.

b) Die Norm von α ist

$$N(\alpha) = \alpha\bar{\alpha} = (r + s\sqrt{D})(r - s\sqrt{D}) = r^2 - s^2D \in \mathbb{Q}.$$

c) Die Spur von α ist $\text{Sp}(\alpha) = \alpha + \bar{\alpha} = 2r \in \mathbb{Q}.$

- Lemma:** a) Für $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$ ist $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$.
 b) Für $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$ ist $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.
 c) $\alpha \in \mathbb{Q}[\sqrt{D}]$ ist Wurzel der quadratischen Gleichung

$$X^2 - \text{Sp}(\alpha)X + N(\alpha) = 0.$$

- d) $\alpha \in \mathbb{Q}[\sqrt{D}]$ ist genau dann ganz, wenn $N(\alpha)$ und $\text{Sp}(\alpha)$ in \mathbb{Z} liegen.
 e) $\alpha \in \mathcal{O}_D$ ist genau dann eine Einheit, wenn $N(\alpha) = \pm 1$ ist.

Beweis: a) Folgt sofort durch direktes Nachrechnen: Für $\alpha = r + s\sqrt{D}$ und $\beta = u + v\sqrt{D}$ ist

$$\begin{aligned} \overline{\alpha\beta} &= \overline{(ru + svD) + (rv + su)\sqrt{D}} = (ru + svD) - (rv + su)\sqrt{D} \\ &= (r - s\sqrt{D})(u - v\sqrt{D}) = \overline{\alpha}\overline{\beta}. \end{aligned}$$

b) Nach Definition ist

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha} \cdot \beta\overline{\beta} = N(\alpha) \cdot N(\beta).$$

c) Ist offensichtlich, denn α und $\overline{\alpha}$ sind Nullstellen von

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha} = X^2 - \text{Sp}(\alpha)X + N(\alpha).$$

d) folgt sofort aus c) und der Definition der Ganzheit.

e) Ist $\alpha \in \mathcal{O}_D^\times$ eine Einheit, so gibt es ein dazu inverses ganzes Element $\beta \in \mathcal{O}_D$, und wegen $\alpha\beta = 1$ ist $N(\alpha) \cdot N(\beta) = N(\alpha\beta) = N(1) = 1$. Die Norm ist also eine Einheit von \mathbb{Z} , d.h. $N(\alpha) = \pm 1$.

Ist umgekehrt $N(\alpha) = \alpha\overline{\alpha} = \pm 1$, so ist $\alpha \cdot (\pm\overline{\alpha}) = 1$, wir haben also ein ganzes Inverses. ■

Das können wir beispielsweise anwenden auf die eingangs betrachteten Zerlegungen $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. In $\mathbb{Q}[\sqrt{-5}]$ ist

$$N(2) = 2 \cdot 2 = 4, \quad N(3) = 3 \cdot 3 = 9, \quad N(1 \pm \sqrt{-5}) = 1 + 5 = 6.$$

Echte Primteiler einer dieser Zahlen müßten also Norm ± 2 oder ± 3 haben. Wegen

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

müßte für solche Elemente $b = 0$ und $a^2 = 2$ oder 3 sein, was für ein $a \in \mathbb{Q}$ offensichtlich nicht möglich ist. Somit sind die Elemente $2, 3$

und $1 \pm \sqrt{-5}$ allesamt irreduzibel, und die Zahl sechs läßt sich auf zwei verschiedene Weisen als Produkt irreduzibler Elemente schreiben. (Es ist klar, daß 2 und 3 nicht zu $1 \pm \sqrt{-5}$ assoziiert sein können, denn die Normen assoziierter Elemente unterscheiden sich höchstens im Vorzeichen.)

Damit haben wir gezeigt, daß die Hauptordnung von $\mathbb{Q}[\sqrt{-5}]$ nicht faktoriell ist.

§5: Euklidische Ringe

In Kapitel I bewiesen wir die eindeutige Primzerlegung in \mathbb{Z} mit Hilfe des EUKLIDISCHEN Algorithmus. Wenn wir Beispiele für faktorielle Ringe \mathcal{O}_D suchen, liegt es daher nahe, nach Ringen zu suchen, in denen es einen EUKLIDISCHEN Algorithmus gibt. Solche Ringe heißen EUKLIDISCHE Ringe.

Wie wir gesehen haben, ist die Division mit Rest das wichtigste Werkzeug beim EUKLIDISCHEN Algorithmus, und wie sich in diesem Abschnitt herausstellen wird, brauchen wir kein weiteres. Wir definieren daher

Definition: Ein EUKLIDISCHER Ring ist ein Integritätsbereich R zusammen mit einer Abbildung $\nu: R \setminus \{0\} \rightarrow \mathbb{N}_0$, so daß gilt: Ist $x|y$, so ist $\nu(x) \leq \nu(y)$, und zu je zwei Elementen $x, y \in R$ gibt es Elemente $q, r \in R$ mit

$$x = qy + r \quad \text{und} \quad r = 0 \quad \text{oder} \quad \nu(r) < \nu(y).$$

Wir schreiben auch $x : y = q$ Rest r und bezeichnen r als Divisionsrest bei der Division von x durch y .

Das Standardbeispiel ist natürlich der Ring \mathbb{Z} der ganzen Zahlen mit $\nu(x) = |x|$. Ein anderes Beispiel ist der Polynomring $k[X]$ über einem Körper k : Hier können wir $\nu(f)$ für ein Polynom $f \neq 0$ als den Grad von f definieren; dann erfüllt auch die Polynomdivision mit Rest die Forderung an einen EUKLIDISCHEN Ring.

Man beachte, daß weder der Quotient noch der Divisionsrest eindeutig bestimmt sein muß: Beispielsweise ist schon in \mathbb{Z} einerseits

$15 : 4 = 3$ Rest 3 , andererseits aber auch 4 Rest -1 , wobei letzteres im EUKLIDischen Algorithmus möglicherweise sogar schneller ans Ziel führt.

Lemma: In einem EUKLIDischen Ring R gibt es zu je zwei Elementen $x, y \in R$ einen ggT. Dieser kann nach dem EUKLIDischen Algorithmus berechnet werden und läßt sich als Linearkombination von x und y mit Koeffizienten aus R darstellen.

Beweis: In jedem Integritätsbereich folgt aus der Gleichung $x = qy + r$ mit $x, y, q, r \in R$, daß die gemeinsamen Teiler von x und y gleich denen von y und r sind. Speziell in einem EUKLIDischen Ring können wir dabei r als Divisionsrest wählen und, wie beim klassischen EUKLIDischen Algorithmus, danach y durch r dividieren usw., wobei wir eine Folge von Divisionsresten r_i erhalten mit der Eigenschaft, daß in jedem Schritt die gemeinsamen Teiler von x und y gleich denen von r_{i-1} und r_i sind. Außerdem ist stets entweder $r_i = 0$ oder $\nu(r_i) < \nu(r_{i-1})$, so daß die Folge nach endlich vielen Schritten mit einem $r_n = 0$ abbrechen muß. Auch hier sind die gemeinsamen Teiler von r_{n-1} und $r_n = 0$ genau die gemeinsamen Teiler von x und y . Da jede Zahl Teiler der Null ist, sind die gemeinsamen Teiler von r_{n-1} und Null aber genau die Teiler von r_{n-1} , und unter diesen gibt es natürlich einen größten, nämlich r_{n-1} selbst. Somit haben auch x und y einen größten gemeinsamen Teiler, nämlich den nach dem EUKLIDischen Algorithmus berechneten letzten von Null verschiedenen Divisionsrest r_{n-1} .

Auch die lineare Kombinierbarkeit folgt wie im klassischen Fall: Bei jeder Division mit Rest ist der Divisionsrest als Linearkombination von Dividend und Divisor darstellbar; beim EUKLIDischen Algorithmus beginnen wir mit Dividend x und Divisor y , die natürlich beide als Linearkombinationen von x und y darstellbar sind, und induktiv folgt, daß auch alle folgenden Dividenden und Divisoren sind als Reste einer vorangegangenen Division Linearkombinationen von x und y sind, also ist es auch ihr Divisionsrest. Insbesondere ist auch der ggT als letzter nichtverschwindender Divisionsrest Linearkombination von x und y , und die Koeffizienten können wie in Kapitel I mit dem erweiterten EUKLIDischen Algorithmus berechnet werden. ■

Lemma: a) In einem EUKLIDischen Ring R ist jedes Element $x \neq 0$ mit $\nu(x) = 0$ eine Einheit.

b) Ist $x = yz \neq 0$, wobei y, z keine Einheiten sind, so ist $\nu(y) < \nu(x)$ und $\nu(z) < \nu(x)$.

Beweis: a) Wir dividieren eins durch x mit Rest: $1 : x = q$ Rest r . Dann ist entweder $r = 0$ oder aber $\nu(r) < \nu(x) = 0$. Letzteres ist nicht möglich, also ist $qx = 1$ und x eine Einheit.

b) Da y und z Teiler von x sind, sind $\nu(y), \nu(z) \leq \nu(x)$. Um zu zeigen, daß $\nu(y)$ echt kleiner als $\nu(x)$ ist, dividieren wir y mit Rest durch x ; das Ergebnis sei q Rest r , d.h. $y = qx + r$ mit $r = 0$ oder $\nu(r) < \nu(x)$. Wäre $r = 0$, wäre y ein Vielfaches von x , es gäbe also ein $u \in R$ mit $y = ux = u(yz) = (uz)y$. Damit wäre $uz = 1$, also z eine Einheit, im Widerspruch zur Annahme. Somit ist $\nu(r) < \nu(x)$.

Als Teiler von x ist y auch Teiler von $r = y - qx = y(1 - qz)$, also muß $\nu(y) \leq \nu(r) < \nu(x)$ sein. Genauso folgt, daß auch $\nu(z) < \nu(x)$ ist. ■

Satz: Jeder EUKLIDische Ring ist faktoriell.

Beweis: Wir müssen zeigen, daß jedes Element $x \neq 0$ aus R bis auf Reihenfolge und Assoziiertheit eindeutig als Produkt aus einer Einheit und geeigneten Potenzen irreduzibler Elemente geschrieben werden kann. Wir beginnen damit, daß sich x überhaupt in dieser Weise darstellen läßt.

Dazu benutzen wir die Betragsfunktion $\nu: R \setminus \{0\} \rightarrow \mathbb{N}_0$ des EUKLIDischen Rings R und beweisen induktiv, daß für $n \in \mathbb{N}_0$ alle $x \neq 0$ mit $\nu(x) \leq n$ in der gewünschten Weise darstellbar sind.

Ist $\nu(x) = 0$, so ist x nach obigem Lemma eine Einheit. Diese kann als sich selbst mal dem leeren Produkt von Potenzen irreduzibler Elemente geschrieben werden.

Für $n > 1$ unterscheiden wir zwei Fälle: Ist x irreduzibel, so ist $x = x$ eine Darstellung der gewünschten Form, und wir sind fertig.

Andernfalls läßt sich $x = yz$ als Produkt zweier Elemente schreiben, die beide keine Einheiten sind. Somit sind nach obigem Lemma $\nu(y) < \nu(x)$

und $\nu(z) < \nu(x)$, beide lassen sich also nach Induktionsvoraussetzung als Produkte von Einheiten und Potenzen irreduzibler Elemente schreiben. Damit läßt sich auch $x = yz$ so darstellen.

Als nächstes müssen wir uns überlegen, daß diese Darstellung bis auf Reihenfolge und Einheiten eindeutig ist. Das wesentliche Hilfsmittel hierzu ist die folgende Zwischenbehauptung:

Falls ein irreduzibles Element p ein Produkt xy teilt, teilt es mindestens einen der beiden Faktoren.

Zum *Beweis* betrachten wir den ggT von x und p . Dieser ist insbesondere ein Teiler von p , also bis auf Assoziiertheit entweder p oder 1. Im ersten Fall ist p Teiler von x und wir sind fertig; andernfalls können wir

$$1 = \alpha p + \beta x$$

als Linearkombination von p und x schreiben. Multiplikation mit y macht daraus $y = \alpha p x + \beta x y$, und hier sind beide Summanden auf der rechten Seite durch p teilbar: Bei $\alpha p x$ ist das klar, und bei $\beta x y$ folgt es daraus, daß nach Voraussetzung p ein Teiler von xy ist. Also ist p Teiler von y , und die Zwischenbehauptung ist bewiesen.

Induktiv folgt sofort:

Falls ein irreduzibles Element p ein Produkt $\prod_{i=1}^r x_i$ teilt, teilt es mindestens einen der Faktoren x_i .

Um den Beweis des Satzes zu beenden, zeigen wir induktiv, daß für jedes $n \in \mathbb{N}_0$ alle Elemente mit $\nu(x) \leq n$ eine bis auf Reihenfolge und Einheiten eindeutige Primfaktorzerlegung haben.

Für $n = 0$ ist x eine Einheit; hier ist die Zerlegung $x = x$ eindeutig.

Seien nun

$$x = u \prod_{i=1}^r p_i^{e_i} = v \prod_{j=1}^s q_j^{f_j}$$

zwei Zerlegungen eines Elements $x \in R$, wobei wir annehmen können, daß alle $e_i, f_j \geq 1$ sind. Dann ist p_1 trivialerweise Teiler des ersten Produkts, also auch des zweiten. Wegen der Zwischenbehauptung teilt p_1 also mindestens eines der Elemente q_j , d.h. $p_1 = w q_j$ ist bis auf eine

Einheit w gleich q_j . Da p_1 keine Einheit ist, ist $\nu(x/p_1) < \nu(x)$; nach Induktionsannahme hat also $x/p_1 = x/(wq_j)$ eine bis auf Reihenfolge und Einheiten eindeutige Zerlegung in irreduzible Elemente. Damit hat auch x diese Eigenschaft. ■

Bemerkung: Die Umkehrung dieses Satzes gilt nicht: Beispielsweise sind nach einem Satz von GAUSS auch $\mathbb{Z}[X]$ sowie Polynomringe in mehr als einer Veränderlichen über \mathbb{Z} oder einem Körper faktoriell, aber keiner dieser Ringe ist EUKLIDISCH, da sich weder der ggT eins von 2 und X in $\mathbb{Z}[X]$ noch der ggT eins von X und Y in $k[X, Y]$ als Linearkombination der Ausgangselemente schreiben läßt.

Wir interessieren uns in diesem Kapitel vor allem für quadratische Zahlkörper; daher wollen wir uns fragen, wann die Hauptordnung eines solchen Körpers EUKLIDISCH ist.

Dazu brauchen wir zunächst eine Abbildung ν nach \mathbb{N}_0 . Für \mathbb{Z} konnten wir einfach den Betrag nehmen; für die Hauptordnung eines quadratischen Zahlkörpers können wir unser Glück versuchen mit dem Betrag der Norm.

Falls die Hauptordnung \mathcal{O}_D von $\mathbb{Q}[\sqrt{D}]$ zusammen mit dieser Abbildung ein EUKLIDISCHER Ring ist, muß es zu je zwei Elementen $r, s \in \mathcal{O}_D$ mit $s \neq 0$ ein Element $q \in \mathcal{O}_D$ geben, so daß $|\mathbf{N}(r - sq)| < |\mathbf{N}(s)|$ ist. Division durch s macht daraus die Ungleichung

$$\left| \mathbf{N}\left(\frac{r}{s} - q\right) \right| < |\mathbf{N}(1)| = 1.$$

Da sich jedes Element von $\mathbb{Q}[\sqrt{D}]$ als so ein Quotient r/s darstellen läßt, muß es also zu jedem $x \in \mathbb{Q}[\sqrt{D}]$ ein $q \in \mathcal{O}_D$ geben, so daß $|\mathbf{N}(x - q)| < 1$ ist. Dies zeigt auch, wie man im EUKLIDISCHEN Fall die Division mit Rest durchführt: Man berechnet den Quotienten x/y zunächst im Körper $\mathbb{Q}[\sqrt{D}]$ und nimmt dann das bezüglich der Norm nächstgelegene Element von \mathcal{O}_D .

Betrachten wir als Beispiel die Division von $23 + 9i$ durch $2 - 3i$ im Ring $\mathbb{Z}[i]$ der GAUSSschen Zahlen. In $\mathbb{Q}[i]$ ist

$$\frac{23 + 9i}{2 - 3i} = \frac{(23 + 9i)(2 + 3i)}{13} = \frac{19}{13} + \frac{87}{13}i.$$

Da $19 : 13 = 1$ Rest 6 und $87 : 13 = 6$ Rest 9 ist, liegt das Element $1 + 7i$ aus $\mathbb{Z}[i]$ am nächsten bei dieser Zahl. Die Norm von

$$\frac{19}{13} + \frac{87}{13}i - (1 + 7i) = \frac{6}{13} - \frac{4}{13}i$$

ist $(6^2 + 4^2)/13^2 = 52/169$ und damit deutlich kleiner als eins. Somit ist

$$(23 + 9i) : (2 - 3i) = (1 + 7i) \text{ Rest } -2i$$

ein mögliches Ergebnis der Division mit Rest. Ein anderes wäre

$$(23 + 9i) : (2 - 3i) = (1 + 6i) \text{ Rest } 3,$$

denn auch die Norm von 3 ist kleiner als die von $2 + 3i$. (Der Rest wurde jeweils als Dividend minus Divisor mal Quotient berechnet.)

Um zu sehen, in welchen der Ringe \mathcal{O}_D eine solche Division mit Rest stets möglich ist, betrachten wir die Situation geometrisch. Wir beschränken uns dabei zunächst auf den imaginärquadratischen Fall.

Um besser zu sehen, welche Terme in den folgenden Rechnungen positiv und welche negativ sind, schreiben wir den Körper als $\mathbb{Q}[\sqrt{-D}]$ mit $D > 0$; seine Elemente lassen sich dann in der Form $x + iy\sqrt{D}$ darstellen, wobei $i = \sqrt{-1}$ die imaginäre Einheit bezeichnet.

Wir betrachten $\mathbb{Q}[\sqrt{-D}]$ als Teilmenge der komplexen Zahlenebene \mathbb{C} ; dann ist

$$N(r + is\sqrt{D}) = (r + is\sqrt{D})(r - is\sqrt{D}) = r^2 + s^2D = \left| r + is\sqrt{D} \right|^2$$

einfach das Quadrat des üblichen komplexen Betrags. \mathcal{O}_{-D} ist also genau dann ein EUKLIDISCHER Ring mit der Norm als Betragsfunktion, wenn es zu jedem Element $x \in \mathbb{Q}[\sqrt{-D}]$ ein $q \in \mathcal{O}_{-D}$ gibt, so daß $|x - q| < 1$ ist. Da $\mathbb{Q}[\sqrt{-D}]$ dicht in \mathbb{C} liegt, müssen dazu die Kreisscheiben mit Radius eins um die Punkte aus \mathcal{O}_{-D} die ganze komplexe Zahlenebene überdecken. Bei den Punkten, die nur auf Rändern solcher Kreisscheiben liegen, muß zudem überprüft werden, daß sie nicht in $\mathbb{Q}[\sqrt{-D}]$ liegen: Andernfalls sind das Körperelemente, für die obige Ungleichung nicht erfüllt ist.

Die Punkte aus \mathcal{O}_D bilden ein Gitter in \mathbb{C} ; für jeden der Gitterpunkte $q \in \mathcal{O}_D$ definieren wir dessen *Wirkungsbereich* oder VORONOI-Bereich

als den Abschluß der Menge aller $z \in \mathbb{C}$, die näher bei q liegen als bei jedem der anderen Gitterpunkte:

$$W(q) = \{z \in \mathbb{C} \mid \forall q' \in \mathcal{O}_{-D} : |z - q| \leq |z - q'|\}$$

Offensichtlich liegt jedes $z \in \mathbb{C}$ in mindestens einem dieser Wirkungsbereiche, und falls $W(q) \subseteq \{z \in \mathbb{C} \mid |z - q| < 1\}$, folgt insbesondere, daß jedes Element von $\mathbb{Q}[\sqrt{-D}]$ im Innern einer Kreisscheibe mit Radius eins um einen Gitterpunkt liegt: Dann ist der Ring \mathcal{O}_{-D} EUKLIDISCH.

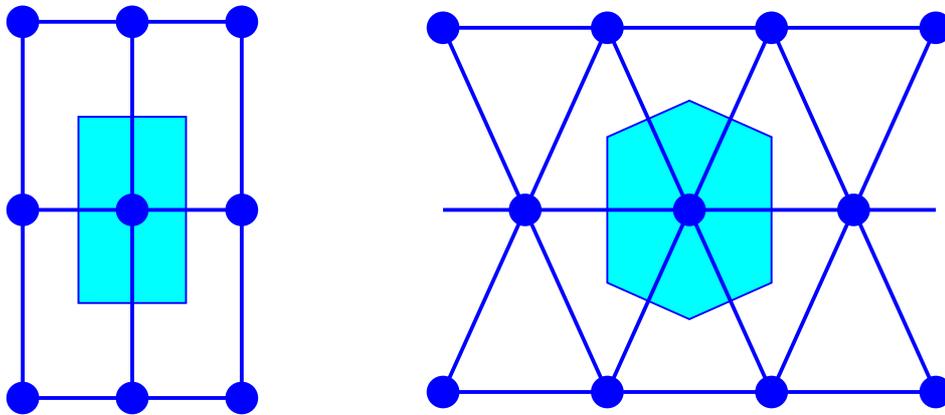
Der Wirkungsbereich eines Gitterpunkts z unterscheidet sich von dem des Nullpunkts nur durch eine Verschiebung um z ; entsprechendes gilt auch für die Kreise mit Radius eins um die beiden Punkte. Daher reicht es, zu untersuchen, wann der Wirkungsbereich des Nullpunkts ganz im Innern des Einheitskreises liegt.

Die Struktur des Wirkungsbereichs hängt ab von $D \bmod 4$: Falls $D \not\equiv -1 \pmod{4}$, d.h. $D \not\equiv 3 \pmod{4}$, ist $\mathcal{O}_{-D} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-D}]$. In der komplexen Zahlenebene bilden diese Punkte ein Rechteckgitter mit den Gitterpunkten $q = r + is\sqrt{D}$ zu $r, s \in \mathbb{Z}$. Der Wirkungsbereich des Nullpunkts ist daher das Rechteck mit Ecken $\pm\frac{1}{2} \pm \frac{i}{2}\sqrt{D}$, und die am weitesten von der Null entfernte Punkte sind die Ecken mit Abstand

$$\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{D}}{2}\right)^2} = \frac{\sqrt{1+D}}{2}.$$

Dies ist genau dann echt kleiner als eins, wenn $D \leq 2$ ist, d.h. $D = 1$ oder $D = 2$.

Für $D = 3$ überdecken zwar die abgeschlossenen Kreisscheiben mit Radius eins um die Gitterpunkte ganz \mathbb{C} , aber die gerade betrachteten Eckpunkte sind Elemente des Körpers $\mathbb{Q}[\sqrt{-3}]$, die in keiner offenen Kreisscheibe um einen Gitterpunkt liegen. Das ist allerdings hier kein Problem, denn in $\mathbb{Q}[\sqrt{-3}]$ sind diese Eckpunkte ja selbst Gitterpunkte: Für $D \equiv 3 \pmod{4}$ gibt es schließlich mehr ganze Zahlen in $\mathbb{Q}[\sqrt{-D}]$.



Hier wird das Gitter \mathcal{O}_{-D} erzeugt von der Eins und von $\frac{1}{2}(1 + i\sqrt{D})$. Der Nullpunkt hat somit sechs nächste Nachbarn, nämlich ± 1 und $\pm \frac{1}{2} \pm \frac{i}{2}\sqrt{D}$. Die Wirkungsbereiche der Null und von ± 1 werden getrennt durch die Geraden $x = \pm \frac{1}{2}$, und auch für die vier anderen Punkte müssen wir die Mittelsenkrechte zur Verbindungsstrecke betrachten. Diese geht durch den Streckenmittelpunkt, also durch $\pm \frac{1}{4} \pm \frac{i}{4}\sqrt{D}$, und sie steht senkrecht auf dieser Strecke.

Eine Drehung um 90° kann in der komplexen Zahlenebene realisiert werden durch Multiplikation mit i ; wir haben also die vier Geraden

$$\left\{ \left(\pm \frac{1}{2} \pm \frac{i}{2}\sqrt{D} \right) + \left(\mp \frac{\sqrt{D}}{2} \pm \frac{i}{2} \right) t \mid t \in \mathbb{R} \right\}.$$

Zwei der Ecken des Wirkungsbereichs liegen (aus Symmetriegründen) auf der imaginären Achse; Einsetzen in die Geradengleichungen ergibt, daß deren Imaginärteile gleich $\pm \frac{1}{4}(\sqrt{D} + 1/\sqrt{D})$ sind. Die restlichen vier Ecken liegen auf den Geraden $x = \pm \frac{1}{2}$, haben also Realteil $\pm \frac{1}{2}$; hier führt die Rechnung auf die Imaginärteile $\pm \frac{1}{4}(\sqrt{D} - 1/\sqrt{D})$.

Der Abstand dieser Punkte vom Nullpunkt ist

$$\sqrt{\left(\frac{1}{2}\right)^2 + \frac{(\sqrt{D} - 1/\sqrt{D})^2}{16}} = \frac{1}{4}\sqrt{4 + D - 2 + \frac{1}{D}} = \frac{1}{4}\sqrt{2 + D + \frac{1}{D}};$$

dies ist genau dann kleiner als eins, wenn gilt

$$2 + D + \frac{1}{D} < 4^2 = 16 \quad \text{oder} \quad D + \frac{1}{D} < 14.$$

Die einzigen $D \equiv 3 \pmod{4}$, die dies erfüllen, sind $D = 3, D = 7$ und $D = 11$. Für diese ist auch $\frac{1}{4}(\sqrt{D} + 1/\sqrt{D}) < 1$, so daß dann und nur dann der gesamte Wirkungsbereich der Null im Einheitskreis liegt.

Die einzigen imaginärquadratischen Zahlkörper $\mathbb{Q}[\sqrt{D}]$, deren Hauptordnung bezüglich der Norm EUKLIDisch ist, sind somit die mit

$$D \in \{-1, -2, -3, -7, -11\};$$

von diesen wissen wir damit auch, daß ihre Hauptordnung faktoriell ist.

Es ist nicht bekannt, ob es andere $D < 0$ gibt, für die die Hauptordnung bezüglich einer anderen Funktion $\nu: \mathcal{O}_D \setminus \{0\} \rightarrow \mathbb{N}_0$ EUKLIDisch ist. Bekannt ist aber, daß die einzigen weiteren faktoriellen Hauptordnungen \mathcal{O}_D die sind mit $D \in \{-19, -43, -67, -163\}$: siehe H. STARK: A complete determination of the complex fields of class-number one, *Michigan J. of Math.* **14** (1967), 1–27. Die Methoden seines Beweises liegen deutlich über dem Niveau dieser Vorlesung.

Im reellquadratischen Fall wird die Ungleichung $|\mathbf{N}(z - q)| - 1$ für $z = x + y\sqrt{D}$ und $q = r + s\sqrt{D}$ zu

$$|(x - r)^2 - (y - v)^2 D| < 1.$$

Betrachten wir für festes $q = r + s\sqrt{D} \in \mathcal{O}_D$ die Menge Z_q aller $(x, y) \in \mathbb{R}^2$, für die $z = x + y\sqrt{D}$ diese Ungleichung erfüllt, erhalten wir also einen Bereich, der durch Hyperbeln begrenzt wird, und wir müssen zeigen, daß die Vereinigung aller Z_q für $q \in \mathcal{O}_D$ ganz \mathbb{R}^2 ist. Durch mühsames Abhaken vieler Einzelfälle folgt aus einer ganzen Reihe von Arbeiten, daß dies genau dann der Fall ist, wenn

$$D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Die letzten offenen Fälle wurden 1950 untersucht in H. CHATLAND, H. DAVENPORT: Euclid's algorithm in real quadratic fields, *Canadian J. Math.* **2** (1950), 289–296; dort sind auch die weiteren Arbeiten zitiert, aus denen zusammen schließlich das obige Ergebnis folgt.

Genau für diese D ist also \mathcal{O}_D EUKLIDisch bezüglich der Norm. Es gibt zahlreiche weitere positive D , für die \mathcal{O}_D faktoriell ist; vermutungsweise sind es sogar unendlich viele. Ob einige dieser Ringe möglicherweise

bezüglich einer anderen Abbildung $\nu: R \setminus \{0\} \rightarrow \mathbb{N}_0$ EUKLIDISCH sind, ist nicht bekannt, und die Nichtexistenz einer solchen Abbildung ist natürlich nur schwer zu beweisen.

§6: Einheiten in quadratischen Zahlkörpern

Ist $x + y\sqrt{D}$ eine Einheit in \mathcal{O}_D (man spricht auch kurz, aber schlampig, von einer Einheit des Zahlkörpers $\mathbb{Q}[\sqrt{D}]$), so muß die Norm $x^2 - Dy^2$ eine Einheit in \mathbb{Z} sein, also gleich ± 1 .

Im imaginärquadratischen Fall ist $x^2 - Dy^2$ die Summe zweier positiver Terme; hier kommt also nur der Wert $+1$ in Frage. Die einzigen ganzzahligen Lösungen sind offensichtlich $(x, y) = (\pm 1, 0)$, sowie im Fall $D = -1$ der GAUSSSchen Zahlen $(x, y) = (0, \pm 1)$. Für $D \equiv 1 \pmod{4}$ sind auch echt halbzahlige Werte für sowohl x als auch y zugelassen; dies führt offensichtlich nur für $D = -3$ zu weiteren Lösungen, nämlich $x = \pm \frac{1}{2}$ und $y = \pm \frac{1}{2}$. Damit haben wir gezeigt:

Lemma: In einem imaginärquadratischen Zahlkörper $\mathbb{Q}[\sqrt{D}]$ gibt es für $D \neq -1$ und $D \neq -3$ nur die Einheiten ± 1 . In $\mathbb{Q}[i]$ gibt es zusätzlich noch die Einheiten $\pm i$, und in $\mathbb{Q}[\sqrt{-3}]$ sind die Einheiten genau die sechsten Einheitswurzeln ± 1 und $\pm \frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$. ■

In reellquadratischen Körpern führt die Bedingung $N(x) = \pm 1$ auf die Gleichung $x^2 - Dy^2 = \pm 1$ mit einem positiven D ; hier können wir nicht ausschließen, daß es unendlich viele Lösungen gibt.

Betrachten wir zunächst den Fall, daß $x^2 - Dy^2 = 1$ ist. Diese Gleichung bezeichnet man als die PELLsche Gleichung.

JOHN PELL (1611–1685) wurde im englischen Sussex geboren und ging auch dort zur Schule. Bereits 1624 begann er sein Studium an der Universität Cambridge; 1628 erhielt er seinen Bachelor und 1630 seinen Master. Danach arbeitete er meist als Lehrer. Von 1654–1658 war er als Diplomat im Auftrag CROMWELLS in Zürich. In einem dort von JOHANN HEINRICH RAHN (1622–1676) verfaßten Buch, an dem PELL wesentlich mitwirkte, ist ein Beispiel der obigen Gleichung zu finden, weshalb sie EULER (1707–1783) nach PELL benannte. Tatsächlich wurde sie wohl erstmalig von dem indischen Mathematiker und Astronom BRAHMAGUPTA (598–670) untersucht; die vollständige Theorie dazu geht

zurück auf LAGRANGE (1736–1813), der die Gleichung als ein Problem bezeichnet, das FERMAT den englischen Mathematikern stellte. Nach seiner Rückkehr aus Zürich wurde PELL Priester. 1663 wählte ihn die Royal Society zum Mitglied, 1675 wurde er deren Vizepräsident.

Mit der PELLschen Gleichung werden wir uns im nächsten Kapitel genauer beschäftigen, und wir werden sehen, daß sie stets unendlich viele Lösungen hat. Als Vorbereitung dazu wollen wir uns hier etwas genauer mit der Struktur der Einheitengruppe beschäftigen. Dazu betrachten wir die Abbildung

$$\lambda: \begin{cases} \mathcal{O}_D^\times \rightarrow \mathbb{R}^2 \\ \alpha \mapsto (\log |\alpha|, \log |\bar{\alpha}|) \end{cases}$$

Da eine Einheit Norm ± 1 hat, ist $|\alpha| \cdot |\bar{\alpha}| = 1$, das Bild von λ liegt also auf der zweiten Winkelhalbierenden $y = -x$ von \mathbb{R}^2 . Außerdem sind α und $\bar{\alpha}$ reell, so daß α genau dann im Kern von λ liegt, wenn $\alpha = \pm 1$ ist.

Das Bild von λ ist diskret, denn hat $\lambda(\alpha)$ höchstens den Abstand M vom Nullpunkt, so ist $\log |\alpha| \leq M$ und $\log |\bar{\alpha}| \leq M$. Ist $\log R = M$, so ist also $|\alpha| \leq R$ und $|\bar{\alpha}| \leq R$. Damit ist $|\text{Sp}(\alpha)| \leq 2R$ und $|\text{N}(\alpha)| \leq R^2$. Da Norm und Spur ganzzahlig sind, gibt es also für beide nur endlich viele Möglichkeiten, und da für ein ganzes Element Norm und Spur zusammen mit dem führenden Koeffizienten eins die Koeffizienten der quadratischen Gleichung sind, gibt es auch nur endlich viele quadratische Gleichungen und damit nur endlich viele Möglichkeiten für α .

Somit gibt es im Bild von λ ein Element $\lambda(\alpha) = (r, -r)$ mit *minimalem* $r > 0$. Wir wollen uns überlegen, daß das jeder andere Punkt im Bild ein ganzzahliges Vielfaches davon ist. Da mit $(s, -s)$ auch $(-s, s)$ im Bild liegt, können wir uns dabei auf Punkte $(s, -s)$ mit $s \geq 0$ beschränken.

Für einen solchen Punkt $\lambda(\beta) = (s, -s)$ gibt es jedenfalls ein größtes $n \in \mathbb{N}_0$, so daß $nr \leq s$ ist. Dann ist

$$\lambda(\beta\alpha^{-n}) = \lambda(\beta) - n\lambda(\alpha) = (s, -s) - n(r, -r) = (s - nr, nr - s),$$

so daß auch dieser Punkt im Bild liegt. Nach Wahl von n ist aber $0 \leq s - nr < r$; wegen der Minimalität von r ist also $s - nr = 0$, d.h. $s = nr$ und $\beta = \alpha^n$.

Damit haben wir bewiesen

Satz: Falls es im reellquadratischen Zahlkörper $K = \mathbb{Q}[\sqrt{D}]$ ein Element aus \mathcal{O}_D^\times gibt, dessen Norm größer als eins ist, gibt es auch ein entsprechendes Element α mit kleinster Norm, und die Einheiten von \mathcal{O}_D sind genau die Elemente $\pm\alpha^n$ mit $n \in \mathbb{Z}$. Insbesondere ist dann die Einheitengruppe unendlich. ■

Im nächsten Kapitel werden wir sehen, daß jeder reellquadratische Zahlkörper eine solche „Grundeinheit“ α hat; die Einheitengruppe eines reellquadratischen Zahlkörpers besteht also stets genau aus den Elementen der Form $\pm\alpha^n$ mit $n \in \mathbb{Z}$ und $\alpha \in \mathcal{O}_D^\times$.

Bevor wir das im einzelnen untersuchen, wollen wir zum Abschluß dieses Kapitels und zur Vorbereitung auf das nächste noch ein Beispiel einer nichtkommutativen Variante eines Zahlkörpers betrachten.

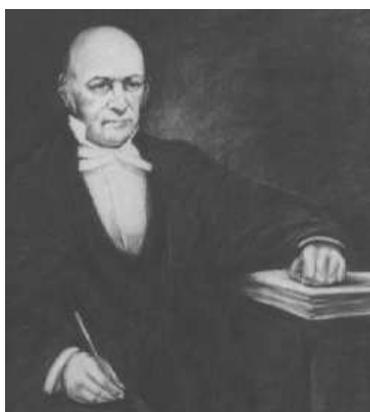
§7: Quaternionen

Nachdem durch die komplexen Zahlen \mathbb{R}^2 mit der Struktur eines Körpers versehen war, versuchten viele Mathematiker ähnliches auch für \mathbb{R}^3 zu erreichen. Natürlich kann weder \mathbb{R}^3 noch sonst ein \mathbb{R}^n mit $n > 2$ zu einem Körper gemacht werden, denn ein solcher Körper wäre eine algebraische Erweiterung von \mathbb{R} ; da aber der algebraische Abschluß von \mathbb{R} gleich \mathbb{C} ist, muß dann $n = 1$ oder $n = 2$ sein.

Die damaligen Mathematiker waren jedoch bescheidener: Ihnen genügte es, einfach irgendeine Art von Multiplikation zu finden, die nicht unbedingt allen Körperaxiomen genügte – von Körpern sprach damals ohnehin noch niemand.

Erst 1940 konnte HEINZ HOPF (1894–1971) (auf dem Umweg über Vektorfelder auf Sphären) zeigen, daß das nicht möglich ist: Selbst eine bilineare Abbildung $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ kann nur dann existieren, wenn n eine Zweierpotenz ist, und 1958 zeigten dann unabhängig voneinander und mit verschiedenen Methoden JOHN MILNOR und MICHEL KERVAIRE, daß auch noch $n \leq 8$ sein muß, so daß nur die vier Möglichkeiten $n = 1, 2, 4$ und 8 in Frage kommen. Genau in diesen Fällen waren auch bereits entsprechende Produkte bekannt: Für $n = 1$ und 2 haben wir

natürlich die reelle bzw. komplexe Multiplikation. Den Fall $n = 4$ löste HAMILTON 1843: Er fand eine Multiplikation auf \mathbb{R}^4 , die zwar nicht kommutativ ist, ansonsten aber alle Körperaxiome erfüllt. Man spricht in so einem Fall von einem *Schiefkörper* oder, in der neueren Literatur, einer *Divisionsalgebra*. HAMILTON bezeichnete seine vierdimensionalen Zahlen als *Quaternionen*. Kurz danach konstruierte ARTHUR CAYLEY (1821–1895) ein nicht-assoziatives Produkt auf \mathbb{R}^8 ; die so erhaltenen „Zahlen“ nannte er *Oktaven*.



WILLIAM ROWEN HAMILTON (1805–1865) wurde in Dublin geboren; bereits mit fünf Jahren sprach er Latein, Griechisch und Hebräisch. Mit dreizehn begann er, mathematische Literatur zu lesen, mit 21 wurde er, noch als Student, Professor der Astronomie am Trinity College in Dublin. Er verlor allerdings schon bald sein Interesse an der Astronomie und beschäftigte sich stattdessen mit mathematischen und physikalischen Problemen. Am bekanntesten ist er für seine Entdeckung der Quaternionen, vorher publizierte er aber auch bedeutende Arbeiten über Optik, Dynamik und Algebra.

HAMILTON wählte eine Basis von $\mathbb{H} = \mathbb{R}^4$, die aus der Eins sowie drei „imaginären Einheiten“ $\mathbf{i}, \mathbf{j}, \mathbf{k}$ besteht, d.h. $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$. Außerdem postulierte er, daß $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ sein sollte; daraus lassen sich dann über das Assoziativgesetz auch die anderen Produkte imaginärer Einheiten berechnen.

Damit ist, wenn man die Gültigkeit des Distributivgesetzes postuliert, eine Multiplikation auf \mathbb{R}^4 definiert; der Beweis, daß hierbei alle Körperaxiome außer der Kommutativität der Multiplikation erfüllt sind, enthält wie üblich nur einen etwas schwierigeren Punkt, die Existenz von Inversen; der Rest ist mühsame Abhakerei.

Zum Glück fand CAYLEY 1858 einen einfacheren Weg: Die vier komplexen 2×2 -Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{und} \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

erfüllen dieselben Relationen

$$I^2 = J^2 = K^2 = -E \quad \text{und} \quad IJ = -JI = K;$$

wir können also die Quaternion $a + bi + cj + dk$ identifizieren mit der Matrix

$$aE + bI + cJ + dK = \begin{pmatrix} a + di & b + ci \\ -b + ci & a - di \end{pmatrix} \in \mathbb{C}^{2 \times 2}.$$

Da für Matrizen das Assoziativgesetz wie auch das Distributivgesetz gelten, ist klar, daß das Produkt zweier solcher Matrizen wieder von derselben Form ist und daß auch die Quaternionenmultiplikation Assoziativ- und Distributivgesetz erfüllt.

Die Quaternionen entsprechen somit genau den komplexen 2×2 -Matrizen der Form

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \quad \text{mit} \quad \alpha = a + di, \beta = b + ci.$$

Die Determinante dieser Matrix ist $\alpha\bar{\alpha} + \beta\bar{\beta} = a^2 + b^2 + c^2 + d^2$.

Definieren wir in Analogie zum Fall der quadratischen Zahlkörper wieder das konjugierte Element zu $\gamma = a + bi + cj + dk$ als die Quaternion $\bar{\gamma} = a - bi - cj - dk$, so entspricht $\bar{\gamma}$ der Matrix

$$\begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} = (\alpha\bar{\alpha} + \beta\bar{\beta})E.$$

Damit folgt insbesondere, daß $\gamma\bar{\gamma}$ eine reelle Zahl ist, die genau dann verschwindet, wenn $\gamma = 0$ ist. Wir bezeichnen diese Zahl wieder als die *Norm* $N(\gamma)$ der Quaternion γ , und wieder ist $\bar{\gamma}/N(\gamma)$ das multiplikative Inverse zu γ – sowohl für die Links- als auch die Rechtsmultiplikation.

$N(\gamma)$ ist gleichzeitig die Determinante der γ zugeordneten Matrix; aus dem Multiplikationssatz für Determinanten folgt daher sofort die Formel

$$N(\gamma\delta) = N(\gamma)N(\delta).$$