Kapitel 4
Quadratische Zahlkörper

Ein Zahlkörper ist ein Körper K, der den Körper $\mathbb{Q}$ der rationalen Zahlen enthält und als $\mathbb{Q}$-Vektorraum betrachtet endlichdimensional ist. Im zweidimensionalen Fall reden wir von quadratischen Zahlkörpern. Die algebraische Zahlentheorie untersucht die (noch zu definierenden) ganzen Zahlen eines solchen Zahlkörpers.

§ 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 im ersten Kapitel definierten *Ringe*. Wenn wir eindeutige Quotienten wollen, müssen wir aber noch zusätzlich voraussetzen, daß es keine sogenannten *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. Zur Bequemlichkeit des Lesers sei hier auch die Definition von Ringen noch einmal wiederholt:

Definition: *a)* Ein Ring ist eine Menge R zusammen mit zwei Rechenoperationen „+“ und „·“, so daß gilt:

1.) R bildet bezüglich „+“ eine abelsche Gruppe.

2.) Die Verknüpfung „·“: $R \times R \to R$ erfüllt das Assoziativgesetz $x(yz) = (xy)z$, und es gibt ein Element $1 \in R$, so daß $1x = x1 = x$.

3.) „+“ und „·“ erfüllen die Distributivgesetze $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

b) Ein Ring heißt *kommutativ*, falls zusätzlich noch das Kommutativgesetz $xy = yx$ der Multiplikation erfüllt ist.

c) Ein Ring heißt *nullteilerfrei* wenn gilt: Falls ein Produkt xy verschwindet, muß mindestens einer der beiden Faktoren x, y verschwinden. Ein nullteilerfreier kommutativer Ring heißt *Integritätsbereich*.

d) 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 $x = qu$.

e) $u \in R$ 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: $v|u$.

f) Ein Element $e \in R$ heißt *Einheit*, falls es ein $e' \in R$ gibt mit $ee' = 1$. Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$.

g) Zwei Elemente $x, y \in R$ heißen assoziiert, wenn es eine Einheit $e \in R$ gibt, so daß $y = ex$.

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.

Der Ring $\mathbb{Z}/m$ ist genau dann nullteilerfrei, wenn m eine Primzahl 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 $a, b \neq 0$.

Der Menge aller $n \times n$-Matrizen über einem Körper ist ein Beispiel eines nichtkommutativen Rings. Er ist nicht nullteilerfrei, enthält aber viele invertierbare Elemente.

Auch die Polynome über einem Körper k bilden einen Ring, den Polynomring $k[X]$. Allgemeiner gilt sogar:

Lemma: Ist R ein Integritätsbereich, so auch der Polynomring

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

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 $R^\times$. ∎

Allgemein 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 gilt: Ist $xz = yz$ für ein Element $z \neq 0$ und zwei beliebige Elemente x, y, so ist $x = y$.
c) Zwei Elemente x, y eines Integritätsbereich R sind genau dann assoziert, 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, r mit $x = qy$ und $y = rx$. Damit ist $1x = x = (qr)x$, also $qr = 1$. 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. ∎

In Integritätsbereichen können wir somit einen Teilbarkeitsbegriff einführen, der den üblichen, von $\mathbb{Z}$ her gewohnten Regeln genügt. Manchmal können wir auch, wie in $\mathbb{Z}$, von einer eindeutigen Primzerlegung reden:

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 *Z*erlegung in *P*rimfaktoren *E*indeutig.)

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 $g_i \le e_i$ für alle i, und Teiler von y, wenn $g_i \le f_i$. ∎

§2: Die Elemente quadratische 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 A, B, C, so daß $A\alpha^2 + B\alpha + C = 0$ verschwindet. Nach der Lösungsformel für quadratische Gleichungen folgt

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

Wegen der Irrationalität von α muß auch $\sqrt{B^2 - 4AC}$ irrational sein, d.h. $B^2 - 4AC$ ist kein Quadrat einer rationalen Zahl. Wegen der Eindeutigkeit der Primzerlegung in $\mathbb{Z}$ können wir aber ganze Zahlen p, q und D finden, so daß

$$B^2 - 4AC = \frac{p^2 D}{q^2} \quad \text{und} \quad \sqrt{B^2 - 4AC} = \frac{p}{q}\sqrt{D}$$

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 quadratfreie 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:

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

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.

Jede Zahl aus $\alpha = r + s\sqrt{D} \in K$ genügt einer quadratischen Gleichung, zum Beispiel der Gleichung $(\alpha - r)^2 = s^2 D$. Durch Multiplikation mit dem Hauptnenner der Koeffizienten und gegebenenfalls noch Kürzen mit dem ggT erhalten wir eine Gleichung

$$A\alpha^2 + B\alpha + C = 0 \quad \text{mit} \quad A, B, C \in \mathbb{Z} \quad \text{und} \quad \text{ggT}(A, B, C) = 1 .$$

Nach der Lösungsformel für quadratische Gleichungen ist

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

Die Zahl $\Delta = B^2 - 4AC$ bezeichnen wir als die *Diskriminante* von α.

Für $\alpha = \sqrt{D}$ beispielsweise haben wir die quadratische Gleichung $\alpha^2 - D = 0$ mit ganzzahligen, teilerfremden Koeffizienten; somit ist die Diskriminante von $\sqrt{D}$ gleich $4D$. Für $\alpha = \frac{1}{3} + \frac{1}{5}\sqrt{2}$ haben wir die Gleichung

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

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

§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: Eine 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.

Als (in dieser Vorlesung einziges) Beispiel betrachten wir den quadratischen Zahlkörper $K = \mathbb{Q}[\sqrt{D}]$. Ein Element $\alpha = r + s\sqrt{D}$ mit $r, s \in \mathbb{Z}$ ist genau dann ganz, wenn es einer Gleichung der Form $x^2 + ax + b$ mit $a, b \in \mathbb{Z}$ genügt. Da

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

ist, genügt x der Gleichung

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

Somit müssen $c = 2r$ und $d = r^2 - s^2 D$ 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 $r^2 - s^2 D$ 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 r. Notwendige Bedingung für die Ganzheit von $r^2 - s^2 D$ ist dann, daß auch $s = e/2$ von dieser Form ist. Dann ist

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

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

In $\mathbb{Q}[\sqrt{D}]$ ist ein Element $r + s\sqrt{D}$ daher für $D \not\equiv 1 \bmod 4$ 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 $D \equiv 1 \bmod 4$ ist $r + s\sqrt{D}$ auch noch dann ganz, wenn r und s beide 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 $u + \beta_D$ 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 $D \equiv 1 \bmod 4$ 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 also

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

Beim Körper $K = \mathbb{Q}[i]$ der komplexen Zahlen mit rationalem Real- und Imaginärteil ist $D = -1 \equiv 3 \bmod 4$, also ist die Hauptordnung hier einfach $\mathcal{O}_{-1} = \mathbb{Z} \oplus \mathbb{Z}i$, die sogenannten ganzen GAUSSschen Zahlen. Für $D = -3 \equiv 1 \bmod 4$ 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 unserere 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

$$x^n + r_{n-1}x^{n-1} + \ldots + r_1 x + r_0 = 0 \quad \text{mit} \quad r_i \in R$$

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 $r_0, \ldots, r_{n-1} \in R$ gibt derart, daß

$$x^n = -r_{n-1}x^{n-1} - \ldots - r_1 x - r_0$$

ist. Multiplikation mit q^n macht daraus die Gleichung

$$p^n = -r_{n-1}p^{n-1}q - \ldots - r_1 pq^{n-1} - r_o q^n \,.$$

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 Elements $\alpha = r + s\sqrt{D}$ von $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$ heißt $\overline{\alpha} = r - s\sqrt{D}$ das zu α konjugierte Element.
b) Die Norm von α ist

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

c) Die Spur von α ist $\quad \mathrm{Sp}(\alpha) = \alpha + \overline{\alpha} = 2r \,.$

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 $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$.
c) $\alpha \in \mathbb{Q}[\sqrt{D}]$ ist Wurzel der quadratischen Gleichung

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

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

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

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

b) Nach Definition ist

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

c) Ist offensichtlich, denn nach dem Satz von VIÈTE sind α und $\overline{\alpha}$ Nullstellen der Gleichung

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

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 auch $\mathrm{N}(\alpha)\cdot\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = 1$. Die Norm ist also eine Einheit von $\mathbb{Z}$, d.h. $\mathrm{N}(\alpha) = \pm 1$.

Ist umgekehrt $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \pm 1$, 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

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

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

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

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 assozierter 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 des 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 $\nu\colon R\setminus\{0\}\to\mathbb{N}_0$, so daß gilt: Ist $x|y$, so ist $\nu(x)\le\nu(y)$, 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.

Wie angekündigt, gilt

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 mit Koeffizienten aus R von x und y 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 (r_i) von Divisionsresten 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.

∎

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 $\nu: R \setminus \{0\} \to \mathbb{N}_0$ 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 eine Einheit: Bei der Division $1 : x = q$ Rest r ist nämlich entweder $r = 0$ oder aber $\nu(r) < \nu(x) = 0$. Letzteres ist nicht möglich, also ist $qx = 1$ und x 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. Da y und z Teiler von x sind, sind $\nu(y), \nu(z) \leq \nu(x)$. Wir wollen uns überlegen, daß sie tatsächlich sogar echt kleiner sind.

Dazu 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.

Nach Induktionsvoraussetzung lassen sich daher y und z als Produkte von Einheiten und Potenzen irreduzibler Elemente schreiben, und 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 $n = 0$ haben wir oben gesehen, daß x eine Einheit sein muß, und 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. $p_1 = wq_j$ ist bis auf eine Einheit w gleich q_j. Da p_i keine Einheit ist, ist $\nu(x/p_i) < \nu(x)$; nach Induktionsannahme hat also $x/p_i = x/(wq_j)$ 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.

Für einen EUKLIDischen Ring 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 $|\mathrm{N}(r - sq)| < |\mathrm{N}(s)|$ ist. Division durch s macht daraus die Ungleichung

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

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 $|\mathrm{N}(x - q)| < 1$ ist. Dies zeig 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 $23 + 5i$ 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 $2 + 3i$. Da in der Definition eines EUKLIDischen Rings von Eindeutigkeit keine Rede war, ist dies kein Problem. (Auch beim EUKLIDischen Algorithmus wird nie gebraucht, daß das Ergebnis der Division mit Rest eindeutig ist; in der Tat läßt sich der sogar für $\mathbb{Z}$ gelegentlich dadurch etwas beschleunigen, daß man bei der Division mit Rest auch negative Reste zuläßt und stets das Ergebnis nimmt, bei dem der Betrag des Rests minimal ist.)

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

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

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 weden, 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:

$$W(q) = \left\{ z \in \mathbb{C} \;\middle|\; \forall q' \in \mathcal{O}_{-D} : |z - q| \le |z - q'| \right\}$$

Offensichtlich liegt jedes $z \in \mathbb{C}$ in mindestens einem dieser Wirkungsbereiche, und falls

$$W(q) \subseteq \left\{ z \in \mathbb{C} \;\middle|\; |z - q| < 1 \right\},$$

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.

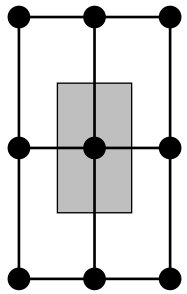
Der Wirkungsbereich eines Gitterpunkts z unterscheidet sich von dem des Nullpunkts nur durch eine Verschiebung um z; entsprechendes gilt auch für die Kreise mit Radius eins um die beiden Punkte. Daher reicht es, zu untersuchen, wann der Wirkungsbereich des Nullpunkts ganz im Innern des Einheitskreises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

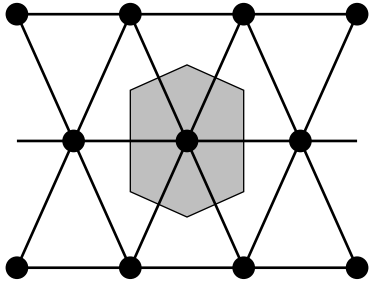
Die Struktur des Wirkungsbereichs hängt ab von $-D \bmod 4$: Falls $D \not\equiv -1 \bmod 4$, d.h. $D \not\equiv 3 \bmod 4$, ist $\mathcal{O}_{-D} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-D}]$. In der komplexen Zahlenebene bilden diese Punkte ein Rechteckgitter mit den Gitterpunkten $q = r + is\sqrt{D}$ 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 $D \le 2$ 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 $D \equiv 1 \bmod 4$ 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 die 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.