Quadratische Zahlkörper

2

In diesem Kapitel legen wir die Grundlagen für das Rechnen in quadratischen Zahlringen. Wir klären, was ein quadratischer Zahlkörper ist und welche seiner Elemente wir als „ganz“ betrachten wollen.

2.1 Quadratische Zahlkörper

In diesem Abschnitt wollen wir klären, in welchen Zahlbereichen wir künftig rechnen werden. Im nächsten Kapitel folgen dann exakte Definitionen arithmetischer Begriffe wie Teilbarkeit, von Einheiten und Primelementen, und erst danach werden wir der Frage nachgehen können, wie man die Eulersche Beweisidee der Lösung der diophantischen Gleichung $y^2 + 2 = x^3$ auf sicheren Boden stellen und dann auf andere Fälle übertragen kann.

Sei $m \in \mathbb{Z} \setminus \{0, 1\}$ eine ganze quadratfreie Zahl; dann heißt die Menge $k = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$ ein *quadratischer Zahlkörper*. Man nennt k reell- bzw. imaginärquadratisch, je nachdem $m > 0$ oder $m < 0$ gilt. Dass k tatsächlich ein Körper ist, rechnet man leicht nach. Das Element $\alpha = a + b\sqrt{m} \in k$ ist Nullstelle des quadratischen Polynoms $P_\alpha(x) = x^2 - 2ax + a^2 - mb^2 \in \mathbb{Q}[x]$; dessen zweite Nullstelle $\alpha' = a - b\sqrt{m}$ nennt man die *Konjugierte* von α. Weiter heißt

$$\begin{array}{lcccl} N\alpha & = & \alpha\alpha' & = a^2 - mb^2 & \text{die } \textit{Norm} \text{ von } \alpha, \\ \operatorname{Tr}\alpha & = & \alpha + \alpha' & = 2a & \text{die } \textit{Spur} \text{ von } \alpha, \text{ und} \\ \operatorname{disc}(\alpha) & = & (\alpha - \alpha')^2 & = 4mb^2 & \text{die } \textit{Diskriminante} \text{ von } \alpha. \end{array}$$

Ursprünglicher Sinn und Zweck der Einführung quadratischer Zahlringe waren zahlentheoretische Probleme in den gewöhnlichen ganzen Zahlen. Um von Aussagen in quadratischen Zahlringen R auf solche in $\mathbb{Z}$ zu kommen, sind natürlich Abbildungen $R \longrightarrow \mathbb{Z}$ wichtig. Da wir vor allem multiplikative Strukturen betrachten werden (Zerlegung in Faktoren, Teilbarkeit, Einheiten), sind multiplikative Abbildungen wie die Norm von besonderer Bedeutung (vgl. etwa Übung 2.4).

© Springer-Verlag GmbH Deutschland 2017

F. Lemmermeyer, *Quadratische Zahlkörper*, DOI 10.1007/978-3-662-53822-7_2

Proposition 2.1. *Für alle $\alpha, \beta \in k$ gilt*

$$N(\alpha\beta) = N\alpha\, N\beta \quad \text{und} \quad \operatorname{Tr}(\alpha+\beta) = \operatorname{Tr}\alpha + \operatorname{Tr}\beta.$$

Weiter ist $N\alpha = 0$ genau dann, wenn $\alpha = 0$ ist, und $\operatorname{disc}(\alpha) = 0$ genau dann, wenn $\alpha \in \mathbb{Q}$ ist.

Den Beweis überlassen wir den Lesern als Übung 2.3.

Die Abbildung $\sigma : k \longrightarrow k : \alpha \longmapsto \sigma(\alpha) := \alpha'$ heißt auch der *nichttriviale Automorphismus* von $k/\mathbb{Q}$. Wegen $\sigma \circ \sigma = \mathrm{id}$ (die identische Abbildung) ist $\{\mathrm{id}, \sigma\}$ eine Gruppe der Ordnung 2, die man die *Galoisgruppe* von $k/\mathbb{Q}$ nennt und mit $\operatorname{Gal}(k/\mathbb{Q})$ bezeichnet.

Die Galoisgruppe einer Körpererweiterung ist benannt nach Évariste Galois (1811–1832), einem französischen Mathematiker, der nach einem Duell im Alter von 20 Jahren starb. Galois revolutionierte die Mathematik durch die Einführung gruppentheoretischer Hilfsmittel in die Theorie der Auflösung von Gleichungen durch Radikale. Diese „Galoistheorie" verwandelte sich erst im Laufe der Zeit (mit Ernst Steinitz, um wenigstens einen Namen zu nennen) von einer Theorie der Polynome zu einer Theorie der Körpererweiterungen. Welch immense Bedeutung für die Arithmetik der Zahlkörper die Galoistheorie selbst in einem so einfachen Fall wie dem von quadratischen Erweiterungen besitzt, werden wir in Kap. 7 sehen.

Quadratische Körpererweiterungen als Vektorräume

Sind $k \subseteq K$ Körper, so kann man K als k-Vektorraum auffassen: Die Vektoren sind die Elemente aus K (diese bilden bekanntlich eine additive Gruppe), die Skalare sind die Elemente von k, und die Skalarmultiplikation ist die gewöhnliche Multiplikation in K. Die Dimension von K als k-Vektorraum nennt man auch seinen *Grad* über k und schreibt $(K : k) := \dim_k K$. Beispielsweise hat $\mathbb{Q}(\sqrt{m})$ Grad 2 über $\mathbb{Q}$, denn $\{1, \sqrt{m}\}$ ist eine Basis, weil sich jedes Element von K eindeutig als $\mathbb{Q}$-Linearkombination von 1 und $\sqrt{m}$ schreiben lässt.

Die Interpretation von quadratischen Zahlkörpern als Vektorräume kann man weiter treiben als hier angedeutet. Legen wir die Basis $1 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ und $\sqrt{m} = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ fest, schreiben also $\alpha = a + b\sqrt{m} = \left(\begin{smallmatrix}a\\b\end{smallmatrix}\right)$, dann ist die Multiplikation mit α eine lineare Abbildung und als solche durch eine 2×2-Matrix beschreibbar, in deren Spalten die Bilder der Basisvektoren stehen. Also ist diese Matrix durch $M_\alpha = \left(\begin{smallmatrix}a & mb\\ b & a\end{smallmatrix}\right)$ gegeben wegen $\sqrt{m} \cdot (a + b\sqrt{m}) = mb + a\sqrt{m}$. Jetzt stellt man fest, dass die Determinante von M_α gleich der Norm und die Spur von M_α gleich der Spur von α ist.

2.2 Ganzheitsringe

Unsere erste Aufgabe ist es, die „ganzen“ Elemente in diesen quadratischen Zahlkörpern zu identifizieren. Die offensichtliche Lösung wäre, einfach den Ring $\mathbb{Z}[\sqrt{m}]$ als Ganzheitsring zu wählen, also genau die Zahlen der Form $a + b\sqrt{m}$ mit $a, b \in \mathbb{Z}$ als ganz zu betrachten. Dass diese Wahl nicht optimal ist, stellt sich aber erst heraus, wenn man versucht, in solchen Ringen eine Theorie der Ideale aufzubauen (s. Übung 5.12).

Der richtige Gedanke ist, nach dem maximalen Ring $\mathcal{O}$ in $K = \mathbb{Q}(\sqrt{m})$ zu fragen, der die beiden folgenden Eigenschaften hat:

- $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$: Die rationalen „ganzen“ Zahlen in K sind genau die rationalen ganzen Zahlen.
- $\mathcal{O}^\sigma = \mathcal{O}$: Mit $\alpha = r + s\sqrt{m}$ ist auch dessen Konjugiertes $\alpha^\sigma = r - s\sqrt{m}$ ganz.

Ist nun $\alpha = r + s\sqrt{m} \in \mathcal{O}$, dann auch $\alpha^\sigma = r - s\sqrt{m}$, sowie $\operatorname{Tr}\alpha = \alpha + \alpha^\sigma = 2r$ und $N\alpha = \alpha\alpha^\sigma = r^2 - ms^2$. Wenn also α *ganz* ist, muss das Polynom

$$P_\alpha(x) = (x - \alpha)(x - \alpha^\sigma) = x^2 - \operatorname{Tr}(\alpha)x + N\alpha = rx^2 - 2rx + r^2 - ms^2$$

ganzzahlige Koeffizienten haben. Wir werden daher ein $\alpha \in K$ eine *ganze algebraische Zahl* nennen, wenn $P_\alpha(x)$ ganzzahlige Koeffizienten besitzt. Die Menge der ganzen Elemente von k nennt man den Ganzheitsring $\mathcal{O}_k$. Dass diese Menge ein Ring ist, werden wir zeigen, nachdem wir die ganzen Elemente charakterisiert haben.

Satz 2.2. *Die ganzen Zahlen im quadratischen Zahlkörper $k = \mathbb{Q}(\sqrt{m})$ sind gegeben durch*

$$\mathcal{O}_k = \begin{cases} \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}, & m \equiv 2, 3 \bmod 4, \\ \left\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \bmod 2\right\}, & m \equiv 1 \bmod 4. \end{cases}$$

Beweis. Sei $\alpha = r + s\sqrt{m}$ ganz mit $r, s \in \mathbb{Q}$; damit sind $\operatorname{Tr}\alpha = 2r$ und $N\alpha = r^2 - ms^2$ ganz. Setzt man $2r \in \mathbb{Z}$ in die zweite Gleichung ein, so findet man, dass $4ms^2$ ganz ist. Da m quadratfrei ist, muss dann sogar $4s^2$, also schließlich $2s$ ganz sein. Das geht so: Sei $4s^2 = x^2/y^2$ mit teilerfremden $x, y \in \mathbb{Z}$; da $4ms^2$ ganz ist, folgt $y^2 \mid mx^2$; wegen $\operatorname{ggT}(x, y) = 1$ muss dann $y^2 \mid m$ sein, und die Quadratfreiheit von m zeigt $y = \pm 1$.

Wir dürfen daher $2r = a$ und $2s = b$ schreiben mit $a, b \in \mathbb{Z}$. Jetzt nutzen wir noch einmal aus, dass $N\alpha = r^2 - ms^2$ ganz ist und finden, dass $a^2 - mb^2 \equiv 0 \bmod 4$ sein muss.

- Ist $m \equiv 2 \bmod 4$, so folgt $2 \mid a$, $4 \mid a^2$ und $2 \mid b$, also $r, s \in \mathbb{Z}$: Jede ganze Zahl hat die Form $r + s\sqrt{m}$ mit ganzen Zahlen $r, s \in \mathbb{Z}$.

- Ist $m \equiv 3 \bmod 4$, so folgt $0 \equiv a^2 - mb^2 \equiv a^2 + b^2 \bmod 4$; dies geht nur, wenn a und b gerade sind, und wie eben folgt, dass r und s ganz sein müssen.
- Ist schließlich $m \equiv 1 \bmod 4$, so erhalten wir die Kongruenz $0 \equiv a^2 - mb^2 \equiv a^2 - b^2 \bmod 4$, welche genau dann richtig ist, wenn $a \equiv b \bmod 2$ gilt. Also haben alle ganzen Zahlen hier die Form $\frac{1}{2}(a + b\sqrt{m})$, wo a und b entweder beide gerade oder beide ungerade sind. Dass diese Zahlen auch wirklich ganz sind, rechnet man einfach nach.

Damit ist alles bewiesen. □

Der Körper $k = \mathbb{Q}(\sqrt{m})$ besteht aus allen $\mathbb{Q}$-Linearkombinationen von 1 und $\sqrt{m}$. Man kann (und sollte) sich daher fragen, ob etwas Ähnliches für $\mathcal{O}_k$ gilt, d. h. ob es ein $\omega \in \mathcal{O}_k$ gibt, sodass $\mathcal{O}_k$ aus allen $\mathbb{Z}$-Linearkombinationen von 1 und ω besteht (in diesem Fall schreiben wir $\mathcal{O}_k = \mathbb{Z} \oplus \omega\mathbb{Z}$ und nennen $\{1, \omega\}$ eine *Ganzheitsbasis*). Dies ist in der Tat der Fall:

Korollar 2.3. *Es gilt $\mathcal{O}_k = \mathbb{Z} \oplus \omega\mathbb{Z}$ mit*

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

Insbesondere ist $\mathcal{O}_k$ ein Ring.

Beweis. Nur im zweiten Fall ist wirklich etwas zu zeigen. Sei also $m \equiv 1 \bmod 4$ und $\alpha = \frac{1}{2}(a + b\sqrt{m})$ mit $a \equiv b \bmod 2$; setzt man $c = \frac{a-b}{2}$ und $d = b$, so ist $\alpha = c + d\omega$ mit $c, d \in \mathbb{Z}$. Die Umkehrung ist genauso trivial.

Dass $\mathcal{O}_k$ ein Ring ist, sieht man jetzt dadurch ein, dass man zeigt, dass Summe, Differenz und Produkt zweier Zahlen der Form $a + b\omega$ mit $a, b \in \mathbb{Z}$ wieder diese Form haben (wir hätten dies bereits im Anschluss an Satz 2.2 machen können, hätten dann aber wesentlich mehr rechnen müssen). Dazu ist im Wesentlichen nur zu zeigen, dass das Produkt zweier Zahlen wieder diese Form hat, und das läuft auf den Nachweis hinaus, dass $\omega^2 = r + s\omega$ mit $r, s \in \mathbb{Z}$ gilt. Tatsächlich ist $\omega^2 = m = m + 0\omega$ für $m \equiv 2, 3 \bmod 4$, und $\omega^2 = \frac{1+m+2\sqrt{m}}{4} = \frac{m-1}{4} + \omega$ für $m \equiv 1 \bmod 4$. □

Die Größe $\Delta = \operatorname{disc} k := \left|\begin{smallmatrix} 1 & \omega \\ 1 & \omega' \end{smallmatrix}\right|^2 = (\omega - \omega')^2$ heißt die *Diskriminante* von k. Man findet $\operatorname{disc} k = 4m$, falls $m \equiv 2, 3 \bmod 4$, und $\operatorname{disc} k = m$, falls $m \equiv 1 \bmod 4$ ist. Die Diskriminante ist ein nützlicher Begriff, da sie Fallunterscheidungen zu vermeiden hilft. Beispielsweise ist $\left\{1, \frac{\Delta+\sqrt{\Delta}}{2}\right\}$ für jeden quadratischen Zahlkörper mit Diskriminante Δ eine Ganzheitsbasis.

Unser nächstes Ergebnis rechtfertigt im Nachhinein unsere Definition ganzer Zahlen in quadratischen Zahlkörpern:

Proposition 2.4. *Die im Ganzheitsring $\mathcal{O}_k$ enthaltenen rationalen Zahlen sind die gewöhnlichen ganzen Zahlen: $\mathcal{O}_k \cap \mathbb{Q} = \mathbb{Z}$.*

Beweis. Wegen $\mathbb{Z} \subseteq \mathcal{O}_k \cap \mathbb{Q}$ ist nur die andere Inklusion zu zeigen. Sei also $\alpha \in \mathcal{O}_k$; dann gilt $\alpha = \frac{1}{2}(a + b\sqrt{m})$ mit $a \equiv b \bmod 2$. Wenn $\alpha \in \mathbb{Q}$ sein soll, muss $b = 0$ sein; also ist a gerade, folglich $\alpha = \frac{a}{2} \in \mathbb{Z}$. □

Man kann zeigen, dass $\mathcal{O}_k$ der maximale Teilring von k mit der Eigenschaft $\mathcal{O}_k \cap \mathbb{Q} = \mathbb{Z}$ ist; man nennt $\mathcal{O}_k$ deshalb oft die *Maximalordnung* von k. Ein Ring $\mathcal{O} \subset k$ heißt *Ordnung*, wenn $\mathcal{O}$ den Ring $\mathbb{Z}$ echt enthält und seinerseits in $\mathcal{O}_k$ enthalten ist, wenn also $\mathbb{Z} \subsetneq \mathcal{O} \subseteq \mathcal{O}_k$ gilt. Mit Proposition 2.4 folgt daraus sofort, dass jede Ordnung $\mathcal{O}$ die Eigenschaft $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ besitzt.

Allgemein sind *algebraische Zahlen* per definitionem Nullstellen von Polynomen mit rationalen Koeffizienten; eine algebraische Zahl α heißt *ganz*, wenn α Nullstelle eines Polynoms $\in \mathbb{Z}[x]$ und Leitkoeffizient 1 ist. Die algebraischen Zahlen bilden einen Körper, die ganzen algebraischen Zahlen einen Ring. Beispiele für nichtquadratische Zahlkörper sind der rein kubische Zahlkörper

$$\mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,:\, a, b, c \in \mathbb{Q}\right\}$$

oder der Kreisteilungskörper

$$\mathbb{Q}(\zeta) = \left\{a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{p-2}\zeta^{p-2} \,:\, a_j \in \mathbb{Q}\right\},$$

wo ζ eine Nullstelle von $\frac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$ und $p \geq 5$ prim ist.

2.3 Der Einheitskreis

Die Elemente eines quadratischen Zahlkörpers, die Norm 1 besitzen, bilden offenbar eine Gruppe bezüglich der Multiplikation, da mit $N\alpha = 1$ und $N\beta = 1$ sicherlich auch $N(\alpha\beta) = 1$ und $N(\alpha/\beta) = 1$ gilt. Die Elemente $x + yi$ mit Norm 1 im Gaußschen Zahlkörper $\mathbb{Q}(i)$ sind durch $N(x + yi) = x^2 + y^2 = 1$ charakterisiert, liegen also auf dem Einheitskreis. Elemente der Norm 1 kann man sich leicht verschaffen, indem man den Quotienten zweier Elemente derselben Norm betrachtet: So hat $\frac{m+ni}{m-ni}$ die Norm $\frac{m^2+n^2}{m^2+n^2} = 1$, und aus

$$\frac{m + ni}{m - ni} = \frac{(m + ni)^2}{(m - ni)(m + ni)} = \frac{m^2 - n^2 + 2mni}{m^2 + n^2}$$

kann man einmal mehr die Parametrisierung

$$x = \frac{m^2 - n^2}{m^2 + n^2}, \quad y = \frac{2mn}{m^2 + n^2}$$

ablesen. Dass man im Wesentlichen alle rationalen Punkte auf dem Einheitskreis auf diese Art bekommt, dass also alle Elemente der Norm 1 sich als Quotient $\frac{m+ni}{m-ni}$

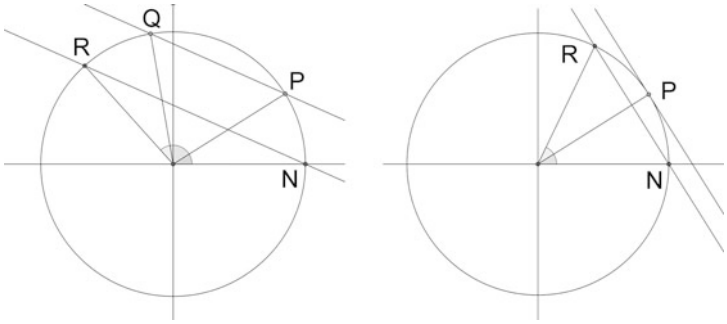

Abb. 2.1 Addition auf dem Einheitskreis: $P \oplus Q = R$ bzw. $2P = R$

schreiben lassen, ist der Inhalt von Hilberts Satz 90, dem wir in Kap. 7 begegnen werden.

Es ist nun eine natürliche Frage, ob man die Gruppenstruktur der rationalen Punkte auf dem Einheitskreis, der durch die Multiplikation solcher Elemente gegeben ist, auch geometrisch interpretieren kann. Dies ist in der Tat der Fall (vgl. Abb. 2.1):

Satz 2.5. *Die Gaußschen Zahlen $a+bi \in \mathbb{Q}(i)$ mit Norm 1 entsprechen eineindeutig den rationalen Punkten auf dem Einheitskreis in der Gaußschen Zahlenebene. Sind $P(a,b)$ und $Q(c,d)$ zwei solche rationalen Punkte, dann erhält man denjenigen Punkt R, der dem Produkt von $(a+bi)(c+di)$ entspricht, als zweiten Schnittpunkt der Parallelen zu PQ durch den Punkt $N(1,0)$, falls P und Q verschieden sind, bzw. als zweiten Schnittpunkt der Tangente in P, falls P und Q gleich sind.*

Der Punkt R, der dem Produkt $(a+bi)(c+di) = ac-bd+(ad+bc)i$ entspricht, hat die Koordinaten $(ac-bd, ad+bc)$. Wir müssen zeigen, dass die Geraden NR und PQ parallel sind; dabei nehmen wir zuerst an, dass P und Q verschiedene x-Koordinaten besitzen. Zu zeigen ist dann die Gleichheit der Steigungen

$$\frac{d-b}{c-a} = \frac{ad+bc}{ac-bd-1}.$$

Wegschaffen der Nenner liefert

$$(d-b)(ac-bd-1) = (ad+bc)(c-a),$$

was zur Gleichung

$$(a^2+b^2-1)d = (c^2+d^2-1)b$$

äquivalent ist. Diese letzte Gleichung ist aber wegen $a^2+b^2 = c^2+d^2 = 1$ sicherlich richtig.

Ist $P \neq Q$, aber haben beide Punkte die gleiche x-Koordinate, dann ist die Gerade PQ parallel zur y-Achse, und die Parallele zu PQ durch N berührt den Kreis in N; in diesem Falle ist also $R = N$. Algebraisch entspricht dies der Multiplikation

$$(a + bi)(a - bi) = a^2 + b^2 = 1.$$

Ist schließlich $P = Q$, so ist die Tangente orthogonal zur Geraden, die den Ursprung und P verbindet, hat also die Steigung $m = -\frac{a}{b}$. Andererseits ist $(a + bi)^2 = a^2 - b^2 + 2abi$, d. h. die Gerade durch N und $R(a^2 - b^2, 2ab)$ hat Steigung $\frac{2ab}{a^2-b^2-1}$. Wegen $a^2 = 1 - b^2$ ist $a^2 - b^2 - 1 = (1 - b^2) - b^2 - 1 = -2b^2$, also $\frac{2ab}{a^2-b^2-1} = \frac{2ab}{-2b^2} = -\frac{a}{b}$ wie erwünscht.

Da sich bei der Multiplikation komplexer Zahlen die Steigungswinkel addieren, beruht das Gruppengesetz auf dem Einheitskreis auf der Addition der dazugehörigen Winkel.

Die Elemente der Norm 1 bilden auch in anderen imaginärquadratischen Zahlkörpern eine Gruppe, deren Gruppengesetz eine ganz ähnliche geometrische Interpretation besitzt. Statt eines Kreises hat man jetzt Ellipsen zu betrachten, und sogar die Additivität der Winkel überträgt sich, wenn man Winkel nur entsprechend definiert.

2.4 Die Platonsche Hyperbel

In reell-quadratischen Zahlkörpern dagegen liegen die Punkte (x, y), die Elementen $x + y\sqrt{m}$ mit Norm 1 entsprechen, auf einer Hyperbel. Während es in imaginärquadratischen Körpern allein aus geometrischen Gründen nur endlich viele ganzzahlige Punkte auf den Norm-1-Ellipsen geben kann (in fast allen Fällen nämlich nur $(\pm 1, 0)$; lediglich für $m = -3$ und $m = -4$ existieren weitere ganzzahligen Punkte), sieht die Sache im reellen Fall ganz anders aus.

Als einfachstes Beispiel behandeln wir die Elemente mit Norm 1 in $\mathbb{Z}[\sqrt{2}]$, also Zahlen $x + y\sqrt{2}$ mit $x^2 - 2y^2 = 1$. Es ist leicht zu sehen, dass etwa $3 + 2\sqrt{2}$ ein solches Element ist, dass also $(3, 2)$ ein ganzzahliger Punkt auf der Hyperbel $\mathcal{H} : x^2 - 2y^2 = 1$ ist. Da auch $N(1, 0)$ ein solcher Punkt ist, können wir in Anlehnung an die Addition der Punkte auf dem Einheitskreis eine Addition von Punkten auf $\mathcal{H}$ definieren, indem wir für zwei (rationale oder ganzzahlige) Punkte P und Q auf $\mathcal{H}$ deren Summe $P \oplus Q = R$ als den zweiten Schnittpunkt der Parallelen zu PQ durch N mit der Hyperbel definieren (vgl. Abb. 2.2).

Hier erhalten wir wie zuvor auf dem Einheitskreis den folgenden

Satz 2.6. *Die Zahlen $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ mit Norm 1 entsprechen eineindeutig den rationalen Punkten $P(a, b)$ auf der Hyperbel $\mathcal{H} : x^2 - 2y^2 = 1$. Sind $P(a, b)$ und $Q(c, d)$ zwei solche rationalen Punkte, dann erhält man denjenigen Punkt R, der dem Produkt von $(a + b\sqrt{2})(c + d\sqrt{2})$ entspricht, als zweiten Schnittpunkt der Parallelen zu PQ durch den Punkt $N(1, 0)$, falls P und Q verschieden sind, bzw. als zweiten Schnittpunkt der Tangente in P, falls P und Q gleich sind.*

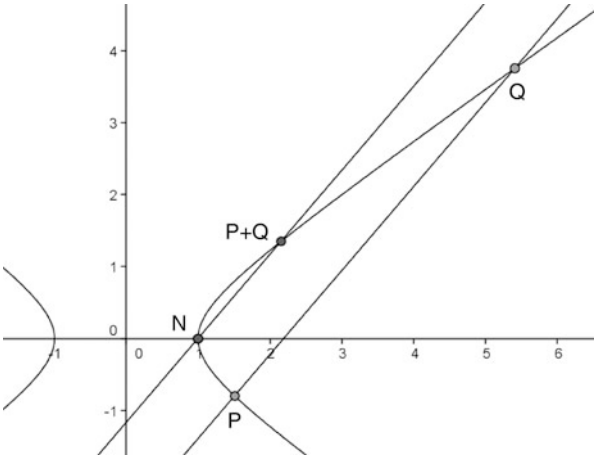

Abb. 2.2 Addition von Punkten auf der Platonschen Hyperbel

Der Beweis läuft wie im Falle des Einheitskreises. Allerdings hat die Hyperbel $\mathcal{H}$, wie wir gleich sehen werden, im Gegensatz zum Einheitskreis unendlich viele ganzzahlige Punkte. Diese entstehen aus $P(3,2)$ durch wiederholte Addition; der Punkt $n \cdot P$ entspricht algebraisch der Zahl $(3+2\sqrt{2})^n$. Wir behaupten nun, dass es außer den ganzzahligen Vielfachen von P, also algebraisch den Potenzen $(3+2\sqrt{2})^n$ mit $n \in \mathbb{Z}$, keine weiteren ganzzahligen Punkte auf dem rechten Ast der Hyperbel $\mathcal{H}$ gibt. Sei dazu Q ein beliebiger ganzzahliger Punkt auf diesem Ast, der nicht die Form nP hat; dann gibt es, da die x-Koordinate von nP unbegrenzt wächst, Zahlen n und $n+1$ derart, dass Q echt zwischen nP und $(n+1)P$ liegt. Subtraktion von nP ergibt, dass $Q \ominus nP$ ein ganzzahliger Punkt ist, der echt zwischen $N(1,0)$ und $P(3,2)$ liegt. Einen solchen gibt es aber nicht.

Da man die ganzzahligen Punkte auf dem linken Ast der Hyperbel $\mathcal{H}$ geometrisch durch Spiegeln an der y-Achse, algebraisch durch Multiplikation mit -1 erhält, haben wir gezeigt:

Satz 2.7. *Die Einheiten der Norm* 1 *im Ring* $\mathbb{Z}[\sqrt{2}]$ *sind gegeben durch*

$$\varepsilon = (-1)^m \left(3+2\sqrt{2}\right)^n$$

mit $0 \le m \le 1$ *und* $n \in \mathbb{Z}$.

Aus diesen erhält man alle Einheiten der Norm -1 *durch Multiplikation mit* $1+\sqrt{2}$. *Wegen* $3+2\sqrt{2} = (1+\sqrt{2})^2$ *hat also jede Einheit in* $\mathbb{Z}[\sqrt{2}]$ *die Form*

$$\varepsilon = (-1)^m \left(1+\sqrt{2}\right)^n .$$

Platonsche Seiten- und Diagonalzahlen

Wir haben bereits erwähnt, dass Euler vor allem durch seinen Freund Goldbach (1690–1764) zur Beschäftigung mit der Zahlentheorie angeregt worden ist. In einem seiner Briefe an Euler [45] behauptete er, nicht nur den Fermatschen Satz bewiesen zu haben, wonach 1 die einzige vierte Potenz unter den Dreieckszahlen ist, sondern schärfer, dass dies auch die einzige Quadratzahl unter allen Dreieckszahlen ist. Dreieckszahlen sind Zahlen der Form $T_n = \frac{n(n+1)}{2}$, weil sich T_n Kieselsteine immer in Dreiecksform anordnen lassen (siehe [43]). Euler antwortete postwendend, dass es unendlich viele Quadratzahlen unter den Dreieckszahlen gebe; aus $T_n = m^2$ folgt nämlich durch quadratische Ergänzung $(2n+1)^2 - 2(2m)^2 = 1$, somit müssen $x = 2n+1$ und $y = 2m$ der Gleichung $x^2 - 2y^2 = 1$ genügen. Die kleinste Lösung ist offenbar $(x, y) = (3, 2)$, was auf $(m, n) = (1, 1)$ führt. Die nächste Lösung $(x, y) = (17, 12)$ liefert die Dreieckszahl $T_8 = 36$, die offenkundig eine Quadratzahl ist.

Die hier auftretenden Zahlenpaare (x, y) gehören zu den Platonschen Seiten- und Diagonalzahlen. Platon (427–347) hat in seinen Schriften nebenbei bemerkt, dass ein Quadrat der Kantenlänge $s = 5$ eine Diagonale hat, die sich von $d = 7$ nicht viel unterscheidet; in der Tat ist ja die Diagonale nach Pythagoras gegeben durch $\sqrt{2 \cdot 5^2} = \sqrt{50}$, während $7^2 = 49$ ist. Die gute Approximation $\sqrt{2} = \frac{7}{5}$ rührt also von der Gleichung $7^2 - 2 \cdot 5^2 = 1$ her. Theon von Smyrna (ca. 70–135 n. Chr.; Smyrna heißt heute Izmir) hat dann die Regel erklärt, dass wenn x_n und y_n Zahlen mit $x_n^2 - 2y_n^2 = \pm 1$ sind, $x_{n+1}^2 - 2y_{n+1}^2 = \mp 1$ ist, wenn man

$$x_{n+1} = x_n + 2y_n \quad \text{und} \quad y_{n+1} = x_n + y_n$$

setzt.

Wie wir oben gesehen haben, erhält man die ganzzahligen Lösungen der Gleichung $x^2 - 2y^2 = \pm 1$, indem man

$$x_n + y_n\sqrt{2} = \pm\left(1 + \sqrt{2}\right)^n$$

setzt. Nimmt man das positive Vorzeichen, so gilt

$$x_n + y_n\sqrt{2} = \left(1 + \sqrt{2}\right)^n, \qquad x_n - y_n\sqrt{2} = \left(1 - \sqrt{2}\right)^n,$$

und dies impliziert

$$x_n = \frac{\left(1 + \sqrt{2}\right)^n + \left(1 - \sqrt{2}\right)^n}{2}, \quad y_n = \frac{\left(1 + \sqrt{2}\right)^n - \left(1 - \sqrt{2}\right)^n}{2\sqrt{2}}.$$

2.5 Die Fibonacci-Hyperbel

In diesem Abschnitt gehen wir auf einige Zusammenhänge zwischen den Fibonacci-Zahlen und quadratischen Irrationalitäten ein, insbesondere der Binetschen Formel. Fibonacci (1170–1250), eigentlich Leonardo von Pisa, war Sohn eines Händlers aus Pisa und wurde auf seinen Reisen in Nordafrika mit den arabischen Ziffern bekannt, für deren Verbreitung er sich in seinem *Liber Abaci* stark machte.

Die nach Fibonacci benannten Zahlen U_n, die in diesem Buch erstmals aufgetaucht sind, werden rekursiv definiert durch

$$U_1 = U_2 = 1, \quad U_{n+1} = U_n + U_{n-1} \quad \text{für } n \geq 1.$$

Man findet leicht, dass die Reihe der Fibonacci-Zahlen gegeben ist durch

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots,$$

und es stellt sich die Frage, ob es für U_n auch eine explizite Formel gibt.

Erzeugende Funktionen

Setzt man die erzeugende Funktion als

$$f(q) = \sum_{n=1}^{\infty} U_n q^n$$

an, so folgt aus der Rekursion $U_{n+1} = U_n + U_{n-1}$ die Beziehung

$$f(q) - qf(q) - q^2 f(q) = q, \quad \text{also} \quad f(q) = \frac{q}{1 - q - q^2}.$$

An dieser Stelle erinnern wir an ein Zitat von Erich Hecke. Dieser schreibt in [31, S. 225], dass

> „die genauere Kenntnis des Verhaltens einer analytischen Funktion in der Nähe ihrer singulären Stellen eine Quelle von arithmetischen Sätzen ist."

Im vorliegenden Fall sind die Pole von f gegeben durch $\frac{1}{\omega}$ und $\frac{1}{\omega'}$ mit $\omega = \frac{1+\sqrt{5}}{2}$ und $\omega' = \frac{1-\sqrt{5}}{2}$. Die Berechnung der Partialbruchzerlegung einer rationalen Funktion $f(q) = A(q)/B(q)$ wird erleichtert durch die Eulerschen Formeln. Der Ansatz

$$\frac{A(q)}{B(q)} = \sum_j \frac{a_j}{q - b_j} \tag{2.1}$$

mit $a_j, b_j \in \mathbb{R}$, wobei die b_j die (möglicherweise komplexen) Wurzeln des Polynoms B sind, wird möglich sein, wenn wir annehmen, dass B nur einfache Wurzeln besitzt.

Zur Bestimmung der a_k multiplizieren wir (2.1) mit $q - b_k$ und lassen $q \to b_k$ gehen. Auf der rechten Seite erhalten wir dann

$$\lim_{q \to b_k} (q - b_k) \sum_j \frac{a_j}{q - b_j} = a_k .$$

Um die linke Seite auszuwerten benutzen wir die Regel von L'Hospital und finden

$$\lim_{q \to b_k} (q - b_k) \frac{A(q)}{B(q)} = \lim_{q \to b_k} \frac{A(q) + (q - b_k)A'(q)}{B'(q)} = \frac{A(b_k)}{B'(b_k)} .$$

Dies zeigt

Proposition 2.8 (Eulersche Formeln). *Seien $A(q)$ und $B(q)$ Polynome in $\mathbb{C}[q]$, wobei B nur einfache Wurzeln besitzt. Dann sind die Koeffizienten a_k in der Partialbruchzerlegung (2.1) bestimmt durch*

$$a_k = \frac{A(b_k)}{B'(b_k)} . \tag{2.2}$$

Die Partialbruchzerlegung von f ist daher gegeben durch

$$f(q) = \frac{q}{1 - q - q^2} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \omega q} - \frac{1}{1 - \omega' q} \right) .$$

Entwickeln in eine geometrische Reihe liefert

$$\begin{aligned} f(q) &= \frac{1}{\sqrt{5}} \left(1 + \omega q + \omega^2 q^2 + \omega^3 q^3 + \ldots - 1 - \omega' q - \omega'^2 q^2 - \omega'^3 q^3 - \ldots \right) \\ &= \frac{1}{\sqrt{5}} \left((\omega - \omega') q + (\omega^2 - \omega'^2) q^2 + (\omega^3 - \omega'^3) q^3 + \ldots \right) . \end{aligned}$$

Ein Vergleich mit der Definition der erzeugenden Funktion ergibt die Binetsche Formel

$$U_n = \frac{\omega^n - \omega'^n}{\omega - \omega'} . \tag{2.3}$$

Gruppengesetz

Die Fibonacci-Zahlen tauchen selbstverständlich auch im Zusammenhang mit der Hyperbel $\mathcal{F} : x^2 - xy - y^2 = 1$ auf, die man aus dem Nenner der erzeugenden Funktion $f(q)$ ablesen kann.

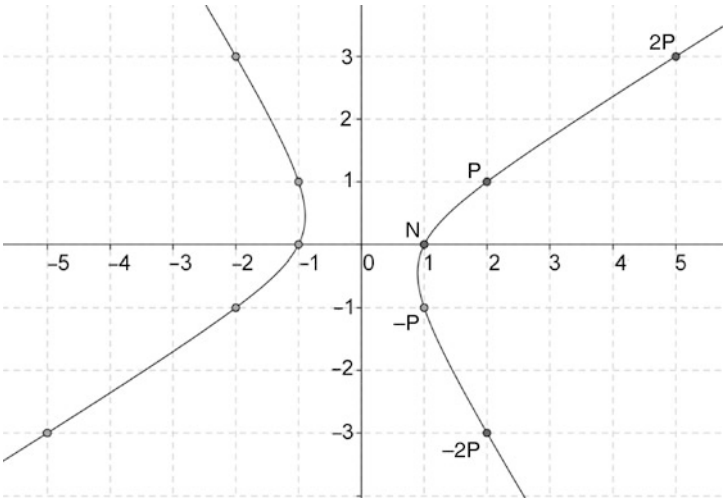

Abb. 2.3 Ganzzahlige Punkte auf der Fibonacci-Hyperbel

Satz 2.9. *Das Gruppengesetz auf der Hyperbel* $\mathcal{F} : x^2 - xy - y^2 = 1$ *mit neutralem Element* $N(1, 0)$*, bei dem die Summe zweier Punkte* P *und* Q *der zweite Schnittpunkt der Parallelen zu* PQ *durch* N *ist, ist gegeben durch die Formel* $(x_1, y_1) \oplus (x_2, y_2) = (x_2, y_3)$ *mit*

$$x_3 = x_1x_2 + y_1y_2, \quad y_3 = x_1y_2 + x_2y_1 - y_1y_2.$$

Den einfachen Beweis überlassen wir den Lesern als Übung 2.26.

Aus dem ganzzahligen Punkt $P = (2, 1)$ auf der Fibonacci-Hyperbel (vgl. Abb. 2.3) erhält man so durch Vervielfachung die Punkte

$$2P = (5, 3), \quad 3P = (13, 8), \quad 4P = (34, 21), \ldots$$

Mittels vollständiger Induktion beweist man leicht, dass $kP = (U_{2k+1}, U_{2k})$ für alle natürlichen Zahlen k gilt.

Wie im Falle der Platonschen Hyperbel kann man zeigen, dass alle ganzzahligen Punkte auf dem rechten Ast der Fibonacci-Hyperbel Vielfache von $(2, 1)$ sind. Allerdings hat man im vorliegenden Fall eine zweite Technik zur Verfügung, die in jüngster Zeit unter dem Namen „Vieta-Jumping“ bekannt geworden ist.

Die grundlegende Beobachtung dabei ist folgende: Ist $P = (x, y)$ irgendein ganzzahliger Punkt auf der Fibonacci-Hyperbel, dann gibt es einen zweiten ganzzahligen Punkt $P^* = (x, y')$ mit derselben x-Koordinate. Dies liegt daran, dass die Gleichung $x^2 - xy - y^2 = 1$ für festes x zwei Lösungen hat, und dass nach Vieta beide Lösungen ganzzahlig sein müssen, sobald nur eine es ist. Aus demselben Grund gibt es auch einen Punkt $P_* = (x', y)$ mit derselben y-Koordinate wie P.

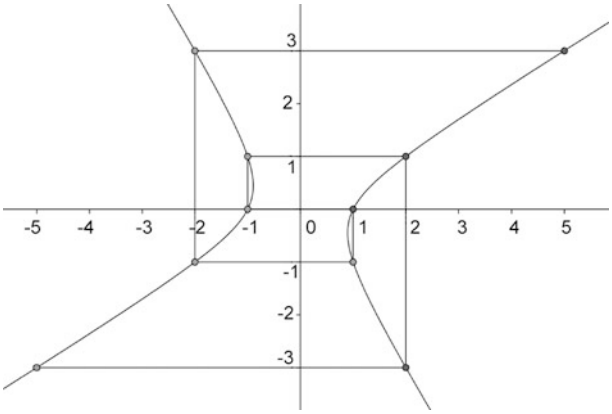

Abb. 2.4 Vieta-Jumping auf der Fibonacci-Hyperbel

Das Herumspringen mit Vieta auf Kegelschnitten (vgl. Abb. 2.4) hat mit dem Gruppengesetz zu tun; offenbar ist in unserem Falle $P + P^* = (1, -1)$ und $P + P_* = (-1, 0)$, wie man aus der geometrischen Definition des Gruppengesetzes mühelos erkennt.

Um zu zeigen, dass alle ganzzahligen Punkte auf der Fibonacci-Hyperbel die Form kP oder $kP \oplus (-1, 0)$ besitzen, geht man von irgendeinem ganzzahligen Punkt $Q(x, y)$ aus. Ist $x > y \geq 1$, dann ist $Q_* = (x', y)$ ein ganzzahliger Punkt mit $x' < y$; ist dagegen $y > x > 1$, so ist $Q^* = (x, y')$ ein ganzzahliger Punkt mit $y < x'$. Wiederholung dieses Abstiegs führt irgendwann auf einen ganzzahligen Punkt mit $x = \pm 1$, also einen der vier Punkte $(\pm 1, 0)$ oder $(\pm 1, \mp 1)$. Umgekehrt ist zu zeigen, dass alle Punkte, die durch die beiden Operationen P^* und P_* aus $P(1, 0)$ entstehen, die Form kP oder $kP \oplus (-1, 0)$ haben. Die Ausarbeitung der Details sei einmal mehr den Lesern überlassen.

Zusammenfassung

Wir haben die folgenden Begriffe eingeführt, die für den Rest der Vorlesung von grundlegender Bedeutung sind:

- Quadratische Zahlkörper
- Norm, Spur und Diskriminante
- Galoisgruppe quadratischer Erweiterungen (von $\mathbb{Q}$)
- Ganzheitsring (Maximalordnung)
- Ganzheitsbasis

Für eine Einführung in die Theorie der Gruppengesetze auf Kegelschnitte siehe auch [44].

2.6 Übungen

2.1 Man überzeuge sich von der Gültigkeit der Gleichung

$$\begin{pmatrix} U_n & U_{n+1} \\ U_{n+1} & U_{n+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n+1}$$

für die Fibonacci-Zahlen U_n. Diagonalisiere $T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ (d. h. finde eine invertierbare Matrix $S \in M_2(\mathbb{C})$ mit $S^{-1}TS = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right) =: D$) und beachte, dass $T^n = (SDS^{-1})^n = SD^nS^{-1}$ gilt. Da man Diagonalmatrizen einfach potenzieren kann, erhält man nun eine Formel für die Zahlen U_n.

2.2 Man beweise die Vermutung $p \mid U_{p\pm1}$ mit elementaren Mitteln durch Entwickeln von α^p mittels der binomischen Formel. Man zeige auch, dass für prime $p \equiv \pm1 \bmod 5$ immer $p \mid U_{p-1}$, für prime $p \equiv \pm2 \bmod 5$ dagegen $p \mid U_{p+1}$ gilt; letzteres stammt von Lagrange.
Joseph Louis Lagrange (1736–1813) war ein italienisch-französischer Mathematiker, der in der Zahlentheorie vor allem für seine Beweise des Vierquadratesatzes (jede natürliche Zahl ist Summe von höchstens vier Quadratzahlen) und der Lösbarkeit der Pellschen Gleichung, sowie für seine Theorie der Reduktion binärer quadratischer Formen bekannt ist.
Hinweis: Zeige, dass in beliebigen Ringen die Kongruenz $(a+b)^p \equiv a^p + b^p \bmod p$ gilt.

2.3 Beweise Proposition 2.1.

2.4 Zeige: Ist $\alpha \mid \beta$ in $\mathcal{O}_k$, dann gilt $N\alpha \mid N\beta$ in $\mathbb{Z}$.

2.5 Sei $x^2 + px + q = 0$ eine quadratische Gleichung mit den Lösungen ω und ω'. Zeige, dass $\operatorname{disc}\omega = (\omega-\omega')^2 = p^2-4q$ mit der Diskriminante der quadratischen Gleichung übereinstimmt. Was passiert im Falle von Gleichungen $ax^2+bx+c=0$?

2.6 Zeige, dass folgende Aussagen äquivalent sind:
1. $\mathbb{Q}(\sqrt{m}) = \{a+b\sqrt{m}, a, b \in \mathbb{Q}\}$ ist ein Körper.
2. $x^2 - m$ ist irreduzibel in $\mathbb{Q}[x]$.
3. Die Zahl m ist keine Quadratzahl.
4. Aus $N(a+b\sqrt{m}) = a^2 - mb^2 = 0$ folgt $a = b = 0$.

2.7 Sei m quadratfrei und $K = \mathbb{Q}(\sqrt{m})$. Zeige, dass die Quadratwurzel $\sqrt{b}$ einer ganzen Zahl genau dann in K liegt, wenn b bis auf das Quadrat einer rationalen Zahl a gleich m ist, wenn also $b = a^2m$ gilt.

2.8 Betrachte $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, wo m keine Quadratzahl ist. Zeige:
1. $\operatorname{Tr}(\alpha) = 0$ genau dann, wenn $a = 0$ ist.
2. $\operatorname{disc}\alpha = 0$ genau dann, wenn $b = 0$ ist.
3. $N\alpha = 0$ genau dann, wenn $a = b = 0$ ist.

2.9 Zeige, dass $\sigma : k \longrightarrow k$ ein Ringhomomorphismus ist, d. h. dass $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ und $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ für alle $\alpha, \beta \in k$ gilt. Zeige weiter, dass ein $\alpha \in k$ genau dann in $\mathbb{Q}$ liegt, wenn $\alpha = \sigma(\alpha)$ ist.

2.10 Sei $K/\mathbb{Q}$ eine quadratische Erweiterung. Verifiziere, dass K ein k-Vektorraum ist.
Zeige, dass die Multiplikation mit $\alpha = a + b\sqrt{m} \in K$ eine lineare Abbildung $K \to K$ ist, welche in Matrixdarstellung bezüglich der $\mathbb{Q}$-Basis $\{1, \sqrt{m}\}$ von K durch $x \mapsto Ax$ gegeben ist, wobei $x = \binom{r}{s}$ das Element $r + s\sqrt{m}$ beschreibt und A gegeben ist durch $A = \left(\begin{smallmatrix} a & mb \\ b & a \end{smallmatrix}\right)$.
Zeige, dass $N\alpha = \det A$ und $\operatorname{Tr}\alpha = \operatorname{Tr} A$ gilt, und dass Norm und Spur nicht von der Wahl der Basis abhängen.

2.11 Zeige, dass α genau dann ganz ist, wenn auch $\sigma(\alpha)$ ganz ist.

2.12 Ist $\{1, \omega\}$ eine Ganzheitsbasis von $\mathcal{O}_k$, dann auch $\{1, \omega - a\}$ für jedes $a \in \mathbb{Z}$. Zeige allgemeiner: Ist $\{\omega_1, \omega_2\}$ eine Ganzheitsbasis und sind a, b, c, d ganze Zahlen mit $ad - bc = 1$, dann ist auch $\{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2\}$ eine Ganzheitsbasis.

2.13 Bestimme alle $m < 0$, für die der Ganzheitsring $\mathcal{O}_k$ von $k = \mathbb{Q}(\sqrt{m})$ ein Element der Norm 2 oder 3 enthält.

2.14 Eine abelsche Gruppe M heißt G-Modul, wenn die Gruppe G auf ihr operiert, d. h. wenn es eine Abbildung $G \times M \longrightarrow M : (g, m) \longmapsto gm$ gibt mit den Eigenschaften
1. $g(m + m') = gm + gm'$,
2. $(gg')m = g(g'm)$,
3. $1m = m$

für alle $g, g' \in G$ und alle $m, m' \in M$. Zeige, dass die Galoisgruppe $G = \operatorname{Gal}(k/\mathbb{Q})$ auf den abelschen Gruppen k, $k^\times$ und $\mathcal{O}_k$ via $(\sigma, \alpha) \longmapsto \sigma(\alpha)$ operiert.

2.15 Löse die Gleichung $x^2 + y^2 = 2z^2$ mit „Eulers Trick“: Schreibe die Gleichung in der Form $(x + y)^2 + (x - y)^2 = (2z)^2$.

2.16 Eine Ganzheitsbasis der Form $\{\omega, \sigma(\omega)\}$ (das soll bedeuten: $\mathcal{O}_k = \omega\mathbb{Z} \oplus \sigma(\omega)\mathbb{Z}$) heißt *normale Ganzheitsbasis*. Zeige, dass $\mathcal{O}_k$ genau dann eine solche besitzt, wenn $m \equiv 1 \bmod 4$ gilt, d. h. wenn $\operatorname{disc} k$ ungerade ist.

2.17 Zeige, dass $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ ein Körper ist, die Teilmenge aller Zahlen der Form $a + b\sqrt[3]{2}$ dagegen nicht.

2.18 Zeige, dass Eulers Schwierigkeiten mit der Gleichung $32 = 5^2 + 7$ daher rühren, dass er in $\mathbb{Z}[\sqrt{-7}]$ anstatt im Ganzheitsring $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ gerechnet hat. Rechne nach, dass

$$\frac{5 + \sqrt{-7}}{2} = \left(\frac{-1 - \sqrt{-7}}{2}\right)^3$$

ist, und zerlege auch $\frac{181+\sqrt{-7}}{2}$ in geeignete Faktoren.

2.19 Leite aus der Tatsache, dass Addition von Punkten auf dem Einheitskreis der Addition der entsprechenden Winkel entspricht, die Additionstheoreme für die trigonometrischen Funktionen her.

2.20 Projiziere die Punkte auf dem Einheitskreis von $Z(-1, 0)$ aus auf die Tangente t in N, und ordne dem Punkt Z den „unendlich fernen“ Punkt auf t zu.

Welches Gruppengesetz wird dabei vom Gruppengesetz auf dem Einheitskreis auf t induziert?

2.21 Die Umkehrung der Verdopplungsformel $2(x, y) = (x^2 - y^2, 2xy)$ für rationale Punkte auf dem Kreis ist die Halbierungsformel, die dem Ziehen der Quadratwurzel der dem Punkt (x, y) entsprechenden komplexen Zahl $x + yi$ entspricht. Zeige, dass die beiden Lösungen von $\frac{1}{2}(x, y)$ gegeben sind durch $\left(\pm \sqrt{\frac{1+x}{2}}, \pm \sqrt{\frac{1-x}{2}} \right)$, wobei die Vorzeichen so zu wählen sind, dass ihr Produkt mit dem Vorzeichen von xy übereinstimmt.
Eine weitere Möglichkeit, diese Formel herzuleiten, besteht darin, die Mittelsenkrechte der Sehne NR mit $N(1, 0)$ und $R(x, y)$ mit dem Einheitskreis zu schneiden. Zeige, dass sich auch daraus die Halbierungsformel ergibt.
Man überlege sich endlich, dass aus $\cos \frac{\pi}{4} = \sin \frac{\pi}{4} = \frac{1}{2}\sqrt{2}$ durch wiederholtes Anwenden der Halbierungsformel folgt, dass

$$\cos \frac{\pi}{8} = \frac{1}{2}\sqrt{2 + \sqrt{2}}, \qquad \sin \frac{\pi}{8} = \frac{1}{2}\sqrt{2 - \sqrt{2}},$$
$$\cos \frac{\pi}{16} = \frac{1}{2}\sqrt{2 + \sqrt{2 + \sqrt{2}}}, \qquad \sin \frac{\pi}{16} = \frac{1}{2}\sqrt{2 - \sqrt{2 + \sqrt{2}}}$$

usw.

2.22 Zeige, dass das Gruppengesetz auf der Hyperbel $xy = 1$ mit neutralem Element $N(1, 1)$ gegeben ist durch $(x_1, y_1) \oplus (x_2, y_2) = (x_1x_2, y_1y_2)$.

2.23 Zeige, dass das Gruppengesetz auf der Parabel $y = x^2$ mit neutralem Element $N(0, 0)$ gegeben ist durch $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + 2x_1x_2)$.

2.24 Zeige, dass die erzeugende Funktion $f(q)$ der Fibonacci-Zahlen der Funktionalgleichung

$$f\left(\frac{1}{q}\right) = f(-q).$$

genügt.

2.25 Zeige, dass für die Fibonacci-Zahlen U_n gilt:

$$\lim_{n\to\infty} \frac{U_{n+1}}{U_n} = \frac{\sqrt{5} + 1}{2}.$$

2.26 Beweise Satz 2.9: Zeige, dass
1. $P_3(x_3, y_3)$ auf der Fibonacci-Hyperbel $x^2 - xy - y^2 = 1$ liegt, und dass
2. die Steigung der Geraden durch P_1 und P_2 gleich derjenigen durch P_3 und N ist.

2.27 Bestimme alle ganzzahligen Punkte auf der Fibonacci-Hyperbel mit Hilfe von Vieta-Jumping.

2.28 Betrachte die Lucas-Lehmer-Hyperbel $x^2 - 3y^2 = 1$. Zeige, dass das Gruppengesetz mit neutralem Element $N(1, 0)$ gegeben ist durch

$$(x_1, y_1) + (x_2, y_2) = (x_1x_2 + 3y_1y_2, x_1y_2 + x_2y_1).$$

Zeige, dass die ganzzahligen Punkte auf dieser Hyperbel gegeben sind durch Vielfache von $P(2,1)$ und deren Negative. Zeige weiter, dass $2^k P = (x_k, y_k)$ ist mit $x_{k+1} = 2x_k^2 - 1$.

2.29 Sei n eine ungerade natürliche Zahl. Zeige, dass n genau dann prim ist, wenn es eine Zahl a gibt derart, dass $a^{n-1} \equiv 1 \bmod n$ ist, aber $a^k \not\equiv 1 \bmod n$ für jeden echten Teiler k von $n-1$.
Folgere daraus, dass $n = 2^m + 1$ genau dann prim ist, wenn $3^{(n-1)/2} \equiv -1 \bmod n$ gilt (Test von Pépin).
In der Sprache der Kegelschnitte formuliert lautet dieser Primzahltest so: Eine ungerade Zahl n ist genau dann prim, wenn es einen Punkt P auf der über $\mathbb{Z}/n\mathbb{Z}$ definierten Hyperbel $xy = 1$ gibt, für den zwar $(n-1)P = (1,1)$ gilt, aber $kP \neq (1,1)$ für jeden echten Teiler k von $n-1$.
Für $n = 17$ und $P = (3,6)$ (die Koordinaten sind modulo 17 zu lesen) ist etwa $2P = (9,2)$, $4P = (13,4)$, $8P = (-1,-1)$ und $16P = (1,1)$, und dies zeigt, dass 17 prim ist.

2.30 Sei p eine Primzahl mit $(\frac{3}{p}) = -1$. Zeige, dass die Punkte modulo p auf dem Kegelschnitt $x^2 - 3y^2 = 1$ eine zyklische Gruppe der Ordnung $p+1$ bilden. Zeige weiter, dass $p = 2^q - 1$ genau dann prim ist, wenn $\frac{p+1}{2} P = (-1,0)$ ist für $P = (2,1)$. Zeige weiter, dass dies gleichbedeutend ist mit $\frac{p+1}{4} P = (0,b)$ für ein geeignetes b modulo p.

http://www.springer.com/978-3-662-53821-0

Quadratische Zahlkörper
Eine Einführung mit vielen Beispielen
Lemmermeyer, F.
2017, VIII, 189 S. 10 Abb., Softcover
ISBN: 978-3-662-53821-0