Österreichische Mathematische Gesellschaft

MATHE-BRIEF

Jänner 2022 — Nr. 113

Herausgegeben von der Österreichischen Mathematischen Gesellschaft
http://www.oemg.ac.at/Mathe–Brief ——— mathe–brief@oemg.ac.at

Ein Blick auf andere ganze Zahlen

Ganze Zahlen im Körper der rationalen Zahlen. Sei mit $\mathbb{Q}$ der Körper der rationalen Zahlen bezeichnet und mit $\mathbb{Z}$ der Ring der ganzen Zahlen. Bemerkenswert ist folgender Satz: Sei

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + x^n$$

ein Polynom mit ganzzahligen Koeffizienten (d.h. $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$). Ist die Zahl α eine Nullstelle von $P(x)$ und eine rationale Zahl, so ist α eine ganze Zahl.

Der Beweis ist einfach. Sei $\alpha = \frac{p}{q}$, wobei p und $q \in \mathbb{Z}$ teilerfremd sind, und $P(\alpha) = 0$. Dann ist

$$P(\alpha) = a_0 + a_1 \frac{p}{q} + a_2 \left(\frac{p}{q}\right)^2 + \cdots + \left(\frac{p}{q}\right)^n = 0$$
$$\Longrightarrow a_0 q^n + a_1 q^{n-1} p + \cdots + a_{n-1} q p^{n-1} + p^n = 0.$$

Also ist q ein Teiler von p^n, woraus $q = 1$ folgt.

Quadratische Zahlkörper. Wir betrachten nun *quadratische Zahlkörper* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, wo d eine quadratfreie ganze Zahl ist. $\mathbb{K}$ ist die Menge aller Zahlen der Form

$$\alpha = a + b\sqrt{d} \quad \text{mit } a, b \in \mathbb{Q}.$$

Die Bezeichnung „Zahlkörper“ bedeutet, dass 0 und 1 in der Menge enthalten sind und Addition, Subtraktion, Multiplikation und Division nicht aus der Menge hinausführen. Die meisten dieser Eigenschaften sind einfach nachzurechnen. Für die Division $x/y = x \cdot y^{-1}$ muss man sich überlegen, dass der Kehrwert α^{-1} einer solchen Zahl wieder dieselbe Gestalt hat. Dies geschieht durch

$$\alpha^{-1} = (a + b\sqrt{d}) \cdot \frac{a - b\sqrt{d}}{a - b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d}.$$

Aber kann nicht der Nenner $a^2 - b^2 d = 0$ sein? Ist $d < 0$, so ist $a^2 - b^2 d = a^2 + b^2 |d| > 0$. Ist $d > 0$, so ist $a^2 = b^2 d$, also $d = (a/b)^2$ und d wäre nicht quadratfrei. Wir vermerken noch, dass $\alpha = a + b\sqrt{d}$ Nullstelle des Polynoms $x^2 - 2ax + a^2 - b^2 d$ ist.

Ganze Zahlen in quadratischen Zahlkörpern. Wir nennen nun $\alpha = a + b\sqrt{d}$ eine *ganze Zahl* im Körper $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, wenn

$$\alpha^2 + A\alpha + B = 0,$$

wobei A und B ganze Zahlen aus $\mathbb{Z}$ sind.

Es gilt der folgende Satz: *Die ganzen Zahlen aus $\mathbb{K}$ bilden einen Ring, d.h. Summe, Differenz und Produkt von zwei solchen ganzen Zahlen in $\mathbb{K}$ ist wieder eine ganze Zahl in $\mathbb{K}$.*

(i) *Ist $d = 4k+2$ oder $d = 4k+3$, so haben die ganzen Zahlen in $\mathbb{K}$ die Form $\alpha = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$.*
(ii) *Ist $d = 4k+1$, so haben die ganzen Zahlen in $\mathbb{K}$ die Form $\alpha = \frac{p}{2} + \frac{q}{2}\sqrt{d}$ und $p+q$ gerade.*

Der Fall $d = 4k$ tritt nicht auf, weil d quadratfrei vorausgesetzt war. Es ist nicht schwer, für die in (i) angegebene Menge die Ring-Eigenschaften nachzurechnen. Im Fall (ii) setze

$$\rho = \frac{-1+\sqrt{d}}{2}$$

und verwende die Darstellung

$$\frac{p+q\sqrt{d}}{2} = \bar{p} + \bar{q}\rho, \text{ mit } \bar{p} = \frac{p+q}{2} \in \mathbb{Z}, \ \bar{q} = q \in \mathbb{Z}.$$

Summe, Differenz und zweier Zahlen dieser Gestalt haben wieder dieselbe Bauart. Das gilt auch für das Produkt, denn das beim Multiplizieren auftretende $\rho^2 = -\rho + \frac{d-1}{4}$ hat dieselbe Form, weil $(d-1)/4 = k$ ganzzahlig ist.

Nun zum Beweis unseres Satzes! Wenn $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}, b \neq 0$, eine ganze Zahl ist, erfüllt sie eine Gleichung

$$\alpha^2 + A\alpha + B = (a + b\sqrt{d})^2 + A(a + b\sqrt{d}) + B = 0$$

mit $A, B \in \mathbb{Z}$. Daraus folgt

$$a^2 + 2ab\sqrt{d} + b^2 d + Aa + Ab\sqrt{d} + B = 0$$

und daraus folgen die beiden Gleichungen

$$2ab + Ab = 0, a^2 + b^2 d + Aa + B = 0.$$

Dann ist (da $b \neq 0$) $A = -2a$ und $B = a^2 - b^2 d$. Daher gelten $2a \in \mathbb{Z}$ und $a^2 - b^2 d \in \mathbb{Z}$. In einem ersten Schritt überlegen wir uns, dass a, b entweder beide ganzzahlig sind, oder beide nicht ganzzahlig, mit 2 im Nenner. Wir unterscheiden zwei Fälle: (a) A ist gerade und (b) A ist eine ungerade Zahl.

(a) In diesem Fall ist $a \in \mathbb{Z}$ und daher auch $b^2 d \in \mathbb{Z}$. Es war d quadratfrei vorausgesetzt, also gilt $d = 4k+1$ oder $d = 4k+2$ oder $d = 4k+3$, und in Folge $b^2(4k+r) = 4b^2 k + b^2 r \in \mathbb{Z}$, mit $r = 1, 2, 3$. Es gilt also $b^2 \in \mathbb{Z}$ oder $2b^2 \in \mathbb{Z}$ oder $3b^2 \in \mathbb{Z}$, und in jedem dieser Fälle muss b ganzzahlig sein.

Umgekehrt gilt bei $b \in \mathbb{Z}$ dann $a^2 = B + b^2 d \in \mathbb{Z}$, also auch $a \in \mathbb{Z}$.

(b) Hier ist $A = 2e+1$ ungerade, und $a = \frac{2e+1}{2}$. Dann ist

$$a^2 - b^2 d = \frac{4e^2 + 4e + 1}{4} - b^2 d$$

und daher $\frac{1}{4}-b^2d\in\mathbb{Z}$. Daher ist $b=\frac{q}{2}$ mit $q\in\mathbb{Z}$. Es ist nicht möglich, dass q gerade ist, denn bei $b\in\mathbb{Z}$ wäre auch $a\in\mathbb{Z}$.

Wir haben damit den Fall $d=4k+1$ des Satzes bereits erledigt. Wir können in beiden Fällen (a)+(b) immer $a=\frac{p}{2}$, $b=\frac{q}{2}$ ansetzen. Die Tatsache, dass a,b beide gleichzeitig in $\mathbb{Z}$ oder nicht in $\mathbb{Z}$ sind, wird durch „$p+q$ gerade" ausgedrückt.

Um den Beweis abzuschließen, müssen wir noch nachweisen, dass der Fall (b) bei $d=4k+2$ und $d=4k+3$ nicht auftreten kann. Dazu erinnern wir uns an $\frac{1}{4}-b^2d\in\mathbb{Z}$. Ist $d=4k+2$ oder $4k+3$, so ergibt sich daraus

$$\frac{1}{4}-2b^2=\frac{1}{4}-\frac{q^2}{2}\in\mathbb{Z}\quad\text{oder}\quad\frac{1}{4}-3b^2=\frac{1}{4}-\frac{3q^2}{4}=\frac{1-3q^2}{4}\in\mathbb{Z}.$$

Diese Begingungen sind nicht erfüllbar: Ein Vielfaches von $\frac{1}{2}$ plus $\frac{1}{4}$ ergibt niemals eine ganze Zahl. Und $3q^2-1$ ist durch 4 teilbar nur dann, wenn $3q^2$ bei Division durch 4 den Rest 1 ergibt. Das geht auch nicht, denn der Ansatz $q=4\ell+r$, $r\in\{0,1,2,3\}$ ergibt $3q^2=3(4\ell+r)^2=3(16\ell^2+8\ell r+r^2)=4(\cdots)+3r^2$, und für $r=0,1,2,3$ ergibt das die Reste $0,3,0,3$.

Damit haben wir die in (i) und (ii) aufgezählte Unterscheidung vollständig beschrieben.

Beispiele für Zerlegungen von Primzahlen in Faktoren aus quadratischen Zahlkörpern. Zwei Beispiele sollte man betrachten. Ist $d=-1$, so werden die quadatischen ganzen Zahlen $\alpha=a+bi$ *Gaußsche ganze Zahlen* genannt. Trägt man sie auf der komplexen Ebene auf, so entsteht ein schönes quadratisches Gitter. Interessant ist es, dass nicht alle Primzahlen aus $\mathbb{Z}$ unzerlegbar bleiben! Es ist schon $2=(1+i)(1-i)$. Im Gegensatz dazu bleibt 3 unzerlegbar („3 ist träge") Denn $3=(a+bi)(a-bi)=a^2+b^2$ ist unlösbar. Das gilt auch für $p=7$, $p=11$ oder $p=19$. Jede Primzahl der Form $p=4k+3$ bleibt unzerlegbar, denn wenn a und b teilerfremd sind, so hat die Summe a^2+b^2 die Gestalt $4k+1$ oder $4k+2$. Hingegen ist $5=(1+2i)(1-2i)$, $13=(2+3i)(2-3i)$ und $17=(4+i)(4-i)$. Die Vermutung, dass jede Primzahl der Gestalt $p=4k+1$ eine Summe von zwei Quadraten ist, also $p=(a+bi)(a-bi)$ ist richtig, aber der Beweis ist anspruchsvoller!

Ist $d=-3$, so bilden in diesem Fall die ganze Zahlen in $\mathbb{K}=\mathbb{Q}(\sqrt{-3})$ ein schönes Sechseckmuster in der komplexen Ebene. In diesem Fall kann $p=2$ nicht zerlegt werden, ist also träge. Aber $3=(2+\rho)(2+\overline{\rho})$ mit $\overline{\rho}=\frac{-1-i\sqrt{3}}{2}$. Ist $\alpha=a+b\rho$, so ist

$$\alpha^2+(2a-b)\alpha+a^2-ab+b^2=0.$$

Ist nun $p=6k-1$, also $p=5,11,17,23,\ldots$, so sieht man leicht ein, dass a^2-ab+b^2 niemals die Gestalt $6k-1$ haben kann (man muss nur für a und b die Gestalt $6k+1$ bzw. $6k-1$ einsetzen). Diese Primzahlen sind also träge! Schwieriger ist es zu zeigen, dass alle Primzahlen der Form $p=6k+1$ zerlegbar sind. Beispiele dafür gibt es genug:$7=(3+\rho)(3+\overline{\rho})$, $13=(4+3\rho)(4+3\overline{\rho})$ und $19=(5+2\rho)(5+2\overline{\rho})$ – auch diesen Beweis können wir hier nicht darstellen.

Fritz Schweiger