Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – Lösungsideen zum 5. Übungsblatt

Aufgabe 1. Ist r nilpotent, so sicher auch sr für jedes $s \in R$, denn aus $r^n = 0$ folgt $(sr)^n = s^n r^n = 0$. Sind aber r und s nilpotent, so auch $r + s$: aus $r^n = 0$, $s^m = 0$ folgt nämlich $(r + s)^{n+m} = 0$, denn nach der binomischen Formel ist das eine Summe mit Summanden der Form $r^i s^{n+m-i}$ (und irgendwelchen Binomialkoeffizienten), und für jedes i zwischen 0 und $n + m$ ist $i \geqslant n$ oder $n + m - i \geqslant m$. (Andernfalls bilde man die Summe beider Ungleichungen, um den Widerspruch $n + m < n + m$ zu erhalten.)

Aufgabe 2. Für einen solchen Ringhomomorphismus muß $f(1) = 1_R$ sein; daraus folgt aber $f(-1_{\mathbb{Z}}) = -1_R$, $f(2) = 1_R + 1_R$ usw. Das zeigt die *Eindeutigkeit*. (Eine präzise Version von „usw." wäre vollständige Induktion, aber wir turnen gleich noch genug Induktionsbeweise.)
Für die *Existenz* definieren wir $f : \mathbb{Z} \to R$ so, wir wir müssen, also induktiv folgendermaßen:

$$f(a) := \begin{cases} 0_R & \text{für } a = 0, \\ f(a-1) + 1_R & \text{für } a > 0, \\ -f(-a) & \text{für } a < 0. \end{cases}$$

Es bleibt zu zeigen, daß f tatsächlich ein Ringhomomorphismus ist. Die Eigenschaften $f(0) = 0_R$ und $f(1) = 1_R$ sind klar. Die Regel $f(a+b) = f(a)+f(b)$ beweisen wir mit Vorwärts- und Rückwärtsinduktion nach b (wobei wir uns a als feste ganze Zahl denken dürfen). Ein halbwegs geschickter Induktionsanfang ist wohl der Fall $b = -a$, denn er folgt sofort aus der Definition von f (aber $b = 0$ ginge natürlich genausogut). Ist nun $b \geqslant -a$, so haben wir

$$f(a+b) \overset{\text{Def.}}{=} f(a+b\mp 1) \pm 1_R \overset{\text{Ind.}}{=} f(a) + f(b \mp 1) \pm 1_R \overset{\text{Ind.}}{=} f(a) + f(b).$$

Auf die gleiche Art beweisen wir die Regel $f(ab) = f(a)f(b)$ durch Induktion nach b, wobei der Fall $b = 0$ klar ist. Für $b \geqslant 0$ erhalten wir

$$\begin{aligned} f(ab) &= f(a(b \mp 1) \pm a) = f(a(b \mp 1)) \pm f(a) \overset{\text{Ind.}}{=} f(a)f(b \mp 1) \pm f(a) \\ &= f(a)[f(b \mp 1) \pm 1] = f(a)f(b). \end{aligned}$$

Da nun f ein Ringhomomorphismus ist, ist $\ker(f)$ ein Ideal in $\mathbb{Z}$, und da $\mathbb{Z}$ Hauptidealring ist, gibt es ein $n \in \mathbb{Z}$ mit $\ker(f) = n\mathbb{Z}$. Da aber $n\mathbb{Z} = m\mathbb{Z}$ genau dann gilt, wenn $n = \pm m$, gibt es genau ein solches n, das nichtnegativ ist.

Aufgabe 3.

i) Nicht ganz klar ist nur die Abgeschlossenheit bezüglich Multiplikation, aber die sieht man anhand der Formel

$$(a + b\sqrt{d})(A + B\sqrt{d}) = (aA + bBd) + (aB + bA)\sqrt{d}.$$

ii) Es sei $d < 0$ und $0 \neq z = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$. Ein eventuelles Inverses von z in unserem Ring muß dasselbe sein wie das in $\mathbb{C}$, also

$$z^{-1} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 + b^2\,|d|} - \frac{b}{a^2 + b^2\,|d|}\sqrt{d},$$

falls nicht gerade $a^2 + b^2\,|d| = 0$ ist, aber daraus würde ja $a = b = 0$, also $z = 0$ folgen. Die auftretenden Koeffizienten müssen wieder ganze Zahlen sein, und insbesondere muß also $a = 0$ oder $|a| \geqslant a^2 + b^2\,|d| \geqslant a^2 \geqslant |a|$ sein. Wenn $a \neq 0$ ist, folgt daraus aber $b = 0$ und $a^2 = |a|$, also $a = \pm 1$, d.h. $z = \pm 1$. Ist aber $a = 0$, so muß immer noch $b \neq 0$ ein Vielfaches von $b^2\,|d|$ sein, und das kann auch nur zuteffen für $|d| = 1$, $b = \pm 1$. Das liefert also im Fall $d = -1$ noch die zusätzlichen möglichen Einheiten $\pm\sqrt{-1} = \pm i$, und natürlich sind alle diese Elemente auch wirklich invertierbar. Etwas stromlinienförmiger, aber weniger naheliegend ist der folgende lehrbuchtaugliche Beweis: die Abbildung $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$, $a + b\sqrt{d} \mapsto a^2 + b^2\,|d|$, ist multiplikativ, das heißt $N(zw) = N(z)N(w)$. Das rechnet man direkt nach, wobei das Geschehen durchsichtiger wird, wenn man zuerst zeigt, daß $\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$, $a + b\sqrt{d} \mapsto a - b\sqrt{d}$, ein Ringhomomorphismus ist (und dann ist $N(z) = z \cdot \sigma(z)$). Damit zeigt man nun, daß $z \in \mathbb{Z}[\sqrt{d}]$ genau dann invertierbar ist, wenn $N(z) = 1$ ist, und die Gleichung $a^2 + b^2\,|d| = 1$ impliziert schnell die Behauptung.

iii) Der Kern ist die Erkenntnis, daß das Element $z = 1 + \sqrt{2}$ invertierbar ist, denn das Inverse $-1 + \sqrt{2}$ liegt ebenfalls in $\mathbb{Z}[\sqrt{2}]$. Die Potenzen z^n für $n \in \mathbb{Z}$ sind aber paarweise verschieden, und das sind unendlich viele Elemente von $\mathbb{Z}[\sqrt{2}]^\times$. – Man kann sogar zeigen, daß die Einheiten in $\mathbb{Z}[\sqrt{2}]$ genau die Form $\pm(1 \pm \sqrt{2})^n$ für $n \geqslant 0$ haben. (Kann Spaß machen!)

Aufgabe 4. Es gilt $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Dies sind tatsächlich zwei wesentlich verschiedene Faktorisierungen in irreduzible Elemente: Zum einen unterscheiden sich $1 \pm \sqrt{-3}$ und ± 2 sicher nicht nur um eine Einheit, denn die Einheiten in $\mathbb{Z}[\sqrt{-3}]$ sind nur ± 1 nach Aufgabe 3, ii). Zum anderen sind 2 und $1 \pm \sqrt{-3}$ irreduzibel; das sieht man am einfachsten mit der „Normabbildung“ N aus dem Lösungsvorschlag zu Aufgabe 3, ii), wobei ich nur die Irreduzibilität von 2 vorführe: Wären $z, w \in \mathbb{Z}[\sqrt{-3}]$ mit $2 = zw$, so hätten wir $N(z)N(w) = N(zw) = N(2) = 4$. Da N nur nichtnegative ganzzahlige Werte annimmt, folgt daraus (notfalls nach Vertauschen von z und w) $N(z) = 1$ oder $N(z) = 2$. Aber $N(z) = 2$ kann nicht sein, denn es gibt keine ganzen Zahlen a, b mit $a^2 + 3b^2 = 2$ (aus dieser Gleichung würde $b = 0$ und damit $a^2 = 2$ folgen). Also ist $N(z) = 1$, d.h. z ist invertierbar.

Zusatzaufgabe.

i) Es sei $f : \mathbb{Z} \to R$ der Homomorphismus aus Aufgabe 1. Ist R nullteilerfrei, so auch $f(\mathbb{Z})$ als Unterring von R. Aber wegen $f(\mathbb{Z}) \cong \mathbb{Z}/\ker(f) = \mathbb{Z}/n\mathbb{Z}$ mit $n = \operatorname{char} R$ ist $n\mathbb{Z}$ ein Primideal, also n eine Primzahl.

ii) Es sei $R = \mathbb{Z}[\sqrt{-1}]$ und $I \subset R$ ein Ideal. I enthält ein Element $0 \neq z_0 \in I$ mit minimalem Betrag $a > 0$ (denn besäße I Elemente von beliebig kleinem Betrag, so müßten ihre Differenzen auch beliebig klein werden, aber die liegen ebenfalls in R, und Elemente von R haben mindestens den Betrag 1). Ich behaupte, daß $I = Rz_0$ ist.
Dazu zeigen wir: Zu jeder komplexen Zahl z gibt es einen Punkt in Rz_0, der um weniger als a von z entfernt ist. Das liegt nun an der konkreten Wahl von $d = -1$: denn Rz_0 ist eine um z_0 gedrehstreckte Version von $R = \mathbb{Z}[\sqrt{-1}]$, also die Knotenmenge eines quadratischen Gitters mit Maschenweite $|z_0| = a$. Jeder Punkt der komplexen Ebene liegt in einer Masche dieses Gitters und hat damit sogar höchstens den Abstand $a/\sqrt{2}$ vom nächsten Gitterknoten (eine Zeichnung hilft hier).

Jetzt geht's schnell: Sei $z \in I$ ein beliebiges Element. Es gibt ein $r \in R$, so daß rz_0 minimalen Abstand b von z hat (gleiches Argument wie oben). Ich behaupte $b = 0$ (und bin damit fertig, denn $z = rz_0 \in Rz_0$). Andernfalls wäre nämlich einerseits $b \geqslant a$ (denn $b = |z - rz_0|$, aber $z - rz_0$ liegt in I!), andererseits $b < a$ (sogar $b \leqslant a/\sqrt{2}$). Das ist sicherlich ein Widerspruch.
Dieses Argument funktioniert im übrigen auch für $d = -2$ (statt Höchstabstand $a/\sqrt{2}$ bekommt man den Höchstabstand $a\sqrt{3}/2 < a$). Auch $\mathbb{Z}[\sqrt{-2}]$ ist also ein Hauptidealring. Der Ring $\mathbb{Z}[\sqrt{-3}]$ ist dagegen nach Aufgabe 4 nicht einmal faktoriell.