Einführung in die Algebra und Diskrete Mathematik
Übungsblatt 5

23.04.2015

1. (Beispiel 2.11, (1)) Sei R ein kommutativer Ring mit Eins. Zeigen Sie:
   (a) Das Produkt invertierbarer Elemente ist wieder invertierbar.
   (b) Jeder Teiler eines invertierbaren Elements ist wieder invertierbar.
   (c) Ein Element $r \in R$ ist genau dann invertierbar, wenn das von r erzeugte Ideal (r) gleich ganz R ist.

   Lösung. (a) Seien $u, v \in R$ invertierbar. Dann ist $(uv)(u^{-1}v^{-1}) = (uu^{-1})(vv^{-1}) = 1 \cdot 1 = 1$. Also ist auch uv invertierbar.
   (b) Sei $u \in R$ invertierbar und $t \in R$ mit $t \mid u$. Also gibt es ein $r \in R$ mit $u = rt$. Multipliziert man beide Seiten mit u^{-1}, erhält man $1 = (u^{-1}r)t$; somit ist t invertierbar mit $t^{-1} = u^{-1}r$.
   (c) Sei $(r) = R$. Dann kann insbesondere die Eins dargestellt werden in der Form $1 = rx$ für ein $x \in R$. Somit ist r invertierbar. Sei umgekehrt r invertierbar und $s \in R\backslash\{0\}$ beliebig. Wegen $s = (sr^{-1})r$ ist $s \in (r)$ und natürlich ist auch $0 \in (r)$, weswegen $(r) = R$ gilt.

   □

2. (Beispiel 2.11, (2)) Zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist. (*Hinweis:* Begründen Sie, dass für jedes $r \in R\backslash\{0\}$ die Abbildung $f_r : R \to R; x \mapsto r \cdot x$ bijektiv ist).

   Lösung. Seien $x, y \in R$. Aus $f_r(x) = f_r(y)$ folgt $rx = ry$ und $r(x - y) = 0$. Da R ein Integritätsbereich ist und $r \neq 0$, folgern wir $x - y = 0$, also $x = y$. Die Abbildung f_r ist also injektiv. Da es sich hier aber um eine Abbildung von R auf sich selbst handelt und R endlich ist, ist f_r sogar bijektiv. Es gibt also ein $s \in R$, sodass $f_r(s) = rs = 1$. Also ist $r \in R$ invertierbar und R somit ein Körper. □

3. Wir betrachten die Menge $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Wir definieren darauf folgende Operationen:

$$(a + b\sqrt{2}) \oplus (c + d\sqrt{2}) := (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2}) \odot (c + d\sqrt{2}) := (ac + 2bd) + (ad + bc)\sqrt{2}$$

(a) Weisen Sie nach, dass $(\mathbb{Z}[\sqrt{2}], \oplus, \odot)$ ein Integritätsbereich ist.

(b) Zeigen Sie, dass $(\mathbb{Z}[\sqrt{2}], \oplus, \odot)$ sogar ein Euklidischer Bereich ist.

(c) Ist $(\mathbb{Z}[\sqrt{2}], \oplus, \odot)$ ein Körper?

Lösung. Da $\mathbb{Z}[\sqrt{2}]$ ein Unterring von $\mathbb{R}$ ist, handelt es sich tatsächlich um einen Integritätsbereich. Wir definieren nun für $a = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ die Funktion $\delta(a) := |x^2 - 2y^2|$. Die Identität $\delta(ab) = \delta(a)\delta(b)$ für alle $a, b \in \mathbb{Z}[\sqrt{2}]$ ist schnell nachgerechnet. Seien nun $a, b \in \mathbb{Z}[\sqrt{2}]$ mit $b \neq 0$ und $u', v' \in \mathbb{Q}$ so, dass $a = b(u' + v'\sqrt{2})$. Wir wählen nun $u, v \in \mathbb{Z}$ so, dass $|u - u'| \leq \frac{1}{2}$ und $|v - v'| \leq \frac{1}{2}$ (wie im Beweis von Satz 2.16) und setzen $q := u + vi$ und $r := a - qb$. Dann gilt

$$\begin{aligned}\delta(r) =& \delta(a - qb) = \delta(b(u' + v'\sqrt{2} - (u + v\sqrt{2})))\\ =& \delta(b)\delta((u' - u) + (v' - v)\sqrt{2}) = \delta(b)|(u' - u)^2 - 2(v' - v)^2| \leq \frac{1}{4}\delta(b).\end{aligned}$$

Da $\delta(b) \neq 0$ für $b \neq 0$, erhalten wir also $\delta(r) \leq \delta(b)$ wie gefordert. $(\mathbb{Z}[\sqrt{2}], \oplus, \odot)$ ist aber kein Körper, da etwa $a = \sqrt{2}$ nicht invertierbar ist, denn aus $\sqrt{2}(x + y\sqrt{2}) = 2y + x\sqrt{2} = 1$ folgt $x = 0$ und $2y = 1$, wobei die letzte Gleichung aber keine Lösung in $\mathbb{Z}$ hat. □

4. Wir betrachten die Menge $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Wir definieren darauf folgende Operationen:

$$\begin{aligned}(a + b\sqrt{-5}) \oplus (c + d\sqrt{-5}) &:= (a + c) + (b + d)\sqrt{-5}\\ (a + b\sqrt{-5}) \odot (c + d\sqrt{-5}) &:= (ac - 5bd) + (ad + bc)\sqrt{-5}\end{aligned}$$

Zusätzlich definieren wir eine Norm durch $\|a + b\sqrt{-5}\| = \sqrt{a^2 + 5b^2}$. Begründen Sie, dass $(\mathbb{Z}[\sqrt{-5}], \oplus, \odot)$ ein Integritätsbereich ist und zeigen Sie, dass $2 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel, aber nicht prim ist.

Lösung. Als Unterring von $\mathbb{Q}[\sqrt{5}]$ bzw. von $\mathbb{C}$ ist $(\mathbb{Z}[\sqrt{-5}], \oplus, \odot)$ ein Integritätsbereich. Offenbar ist 2 nicht invertierbar, denn die Bedingung $2(x + y\sqrt{-5}) = 1$ hätte $2x = 1$ zur Folge, was in $\mathbb{Z}$ nicht lösbar ist. Seien $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ mit $\alpha \cdot \beta = 2$, also

$$2 = \alpha \cdot \beta = (a + b\sqrt{-5})(c + d\sqrt{-5}) \text{ mit } a, b, c, d \in \mathbb{Z}.$$

Wir bilden auf beiden Seiten das Quadrat der Norm und erhalten

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Diese Gleichheit kann offenbar nur für $b = d = 0$ und $ac = 2$ erfüllt sein. Also ist entweder $\alpha = \pm 1$ oder $\beta = \pm 1$ und 2 ist tatsächlich irreduzibel. Andererseits gilt zwar $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, aber $2 \nmid (1 + \sqrt{-5})$ und $2 \nmid (1 - \sqrt{-5})$, was zeigt, dass 2 nicht prim ist. □

5. Sei n eine natürliche Zahl mit $n \equiv 3 \pmod 4$. Begründen Sie, dass es keine $a, b \in \mathbb{N}$ gibt, sodass $n = a^2 + b^2$.

Lösung. Wir unterscheiden drei Fälle. Seien zunächst a und b beide gerade, also $a = 2x$ und $b = 2y$ für ein $x, y \in \mathbb{N}$. Dann ist $a^2 + b^2 = 4(x^2 + y^2) \equiv 0 \pmod 4$. Falls $a = 2x$ gerade und $b = 2y + 1$ ungerade ist (oder umgekehrt), folgt $a^2 + b^2 = 4(x^2 + y^2 + y) + 1 \equiv 1 \pmod 4$. Für a, b ungerade erhalten wir analog $a^2 + b^2 \equiv 2 \pmod 4$. Also ist die Summe zweier Quadrate entweder kongruent 0, 1 oder 2 modulo 4, niemals aber kongruent 3 modulo 4. □