Probestudium 2018
- Übungsblatt 4 -

Prof. Dr. Werner Bley
Dominik Bullach
Martin Hofer
Pascal Stucky

Aufgabe 1 (mittel)
Überprüfen Sie, ob die folgenden Teilmengen des jeweiligen Rings Ideale sind:

(a) $2\mathbb{Z} \subseteq \mathbb{Z}$,

(b) $\mathbb{Z} \subseteq \mathbb{Q}$,

(c) $I := \{25x + y(7+i) \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}[i]$.

Aufgabe 2 (leicht)
Bestimmen Sie mithilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von f und g. Finden Sie anschließend a und b mit

$$\mathrm{ggT}(x, y) = a \cdot f + b \cdot g.$$

(a) $f = 16170$ und $g = 1326$,

(b) $f = x^4 - 3x^3 - x^2 + 5x - 6$ und $g = x^3 - 3x^2 + x - 3$.

Aufgabe 3 (leicht)
Teilen Sie $12 + 14i$ durch $32 - 6i$ mit Rest, d. h. finden Sie $\gamma, \rho \in \mathbb{Z}[i]$ mit

$$12 + 14i = \gamma \cdot (32 - 6i) + \rho,$$

wobei $|\rho| < |32 - 6i|$.

Aufgabe 4 (leicht)
Überprüfen Sie, ob -1 ein Quadrat modulo 29 ist, d. h. finden Sie ggf. eine ganze Zahl n mit

$$n^2 \equiv -1 \mod 29.$$

Aufgabe 5 (schwer)

(a) Zeigen Sie, dass $(x, y) \subseteq \mathbb{C}[x, y]$ kein Hauptideal ist.

(b) Zeigen Sie, dass $(2, x) \subseteq \mathbb{Z}[x]$ kein Hauptideal ist.

Lösungen

Aufgabe 1

(a) Seien $a, b \in 2\mathbb{Z}$. Dann gibt es $\alpha, \beta \in \mathbb{Z}$, sodass $a = 2\alpha$ und $b = 2\beta$. Es folgt

$$a + b = 2\alpha + 2\beta = 2(\alpha + \beta) \in 2\mathbb{Z} \ .$$

Sei $r \in \mathbb{Z}$, dann ist

$$r \cdot a = r \cdot 2\alpha = 2(r\alpha) \in 2\mathbb{Z} \ .$$

Somit ist $2\mathbb{Z}$ ein Ideal.

(b) Seien $a, b \in \mathbb{Z}$. Dann ist auch $a + b \in \mathbb{Z}$. Betrachten wir aber nun $r \in \mathbb{Q}$, dann ist $r \cdot a$ nicht unbedingt in $\mathbb{Z}$. Wählen wir z.B. $a = 1$ und $r = \frac{1}{2}$, dann ist

$$r \cdot a = \frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z} \ .$$

Somit ist $\mathbb{Z}$ kein Ideal in $\mathbb{Q}$.

(c) Seien $a, b \in I$, d.h. es gibt $x, y, w, z \in \mathbb{Z}$, sodass $a = 25x + y(7 + i)$ und $b = 25w + z(7 + i)$. Dann gilt

$$a + b = 25x + y(7 + i) + 25w + z(7 + i) = 25(x + w) + (y + z)(7 + i) \in I \ .$$

Sei nun $r \in \mathbb{Z}[i]$, d.h. es gibt $\alpha, \beta \in \mathbb{Z}$, sodass $r = \alpha + i\beta$. Dann erhalten wir

$$\begin{aligned} r \cdot a &= (\alpha + i\beta)(25x + y(7 + i)) \\ &= \alpha \cdot 25x + \alpha y(7 + i) + i\beta \cdot 25x + i\beta y(7 + i) \\ &= 25x\alpha + 7y\alpha - y\beta + i(y\alpha + 25x\beta + 7y\beta) \\ &= 25x\alpha + 7y\alpha - y\beta + (7 + i)(y\alpha + 25x\beta + 7y\beta) - 7(y\alpha + 25x\beta + 7y\beta) \\ &= 25x\alpha - 50y\beta + 25x\beta + (7 + i)(y\alpha + 25x\beta + 7y\beta) \\ &= 25(x\alpha - 2y\beta + x\beta) + (7 + i)(y\alpha + 25x\beta + 7y\beta) \in I \ . \end{aligned}$$

Somit ist I ein Ideal.

Aufgabe 2

(a) Wir führen den euklidischen Algorithmus durch und berechnen

$$\begin{array}{ccccc} 16170 & = & 12 \cdot 1326 & + & 258 \\ 1326 & = & 5 \cdot 258 & + & 36 \\ 258 & = & 7 \cdot 36 & + & 6 \\ 36 & = & 6 \cdot 6 & + & 0 \end{array}$$

Daraus erhalten wir also

$$\mathrm{ggT}(16170, 1326) = 6 \ .$$

Rückwärts einsetzen liefert nun

$$\begin{aligned} 6 &= 258 - 7 \cdot 36 \\ &= 258 - 7 \cdot (1326 - 5 \cdot 258) \\ &= 36 \cdot 258 - 7 \cdot 1326 \\ &= 36 \cdot (16170 - 12 \cdot 1326) - 7 \cdot 1326 \\ &= 36 \cdot 16170 - 439 \cdot 1326 \ . \end{aligned}$$

(b) Durch Polynomdivison erhalten wir hier mit dem euklidischen Algorithmus

$$\begin{array}{rcccc}
x^4-3x^3-x^2+5x-6 & = & x\cdot(x^3-3x^2+x-3) & + & -2x^2+8x-6 \\
x^3-3x^2+x-3 & = & \left(-\tfrac{1}{2}x-\tfrac{1}{2}\right)\cdot(-2x^2+8x-6) & + & 2x-6 \\
-2x^2+8x-6 & = & (-x+1)\cdot(2x-6) & + & 0
\end{array}$$

Somit ist

$$\operatorname{ggT}(f,g)=2x-6$$

und wir erhalten durch rückwärts einsetzen

$$\begin{aligned}
2x-6 &= x^3-3x^2+x-3-\left(-\frac{1}{2}x-\frac{1}{2}\right)\cdot(-2x^2+8x-6)\\
&= x^3-3x^2+x-3-\left(-\frac{1}{2}x-\frac{1}{2}\right)\cdot(x^4-3x^3-x^2+5x-6-x\cdot(x^3-3x^2+x-3))\\
&= \left(-\frac{1}{2}x^2-\frac{1}{2}x+1\right)(x^3-3x^2+x-3)+\left(-\frac{1}{2}x-\frac{1}{2}\right)\cdot(x^4-3x^3-x^2+5x-6)\ .
\end{aligned}$$

Aufgabe 3

Wir gehen entsprechend dem Beweis zu Satz 3.1 vor: Es ist

$$\frac{12+14i}{32-6i}=\frac{(12+14i)\cdot(32+6i)}{(32-6i)\cdot(32+6i)}=\frac{12\cdot 32+32\cdot 14i+12\cdot 6i-6\cdot 14}{32^2+6^2}=\frac{300+520i}{1060}.$$

Also $\frac{12+14i}{32-6i}=\tilde{a}+\tilde{b}i$ mit

$$\tilde{a}=\frac{300}{1060}=\frac{15}{53}\quad\text{und}\quad\tilde{b}=\frac{520}{1060}=\frac{26}{53}.$$

Wegen

$$\tilde{a}=\frac{15}{53}<\frac{15}{54}<\frac{27}{54}=\frac{1}{2}\quad\text{und}\quad\tilde{b}=\frac{26}{53}<\frac{26}{54}<\frac{27}{54}=\frac{1}{2}$$

runden wir sowohl $\tilde{a}$ als auch $\tilde{b}$ auf 0 ab und setzen

$$\gamma=0+0i=0.$$

Folglich ist dann $\rho=12+14i$.

Zugegebenermaßen waren die Zahlen für die Aufgabe nicht optimal gewählt. Etwas interessanter wäre es gewesen, $32-6i$ durch $12+14i$ mit Rest zu teilen. In dem Fall hätte man nämlich

$$32-6i=(1-2i)\cdot(12+14i)+(-8+4i)$$

als Ergebnis erhalten.

Aufgabe 4

Laut eine Kriterium aus der Vorlesung (s. Seite 20 im Skript) gibt es wegen $29\equiv 1 \mod 4$ zumindest ein solches n. Wie in der Vorlesung berechnen wir nun die Potenzen $2^k \mod 29$:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2^k	2	4	8	16	3	6	12	24	19	9	18	7	14	28

Aus der Tabelle lesen wir ab, dass $2^{14}\equiv 28\equiv -1 \mod 29$, also setze $n=2^7$.

Aufgabe 5

(a) Angenommen (x, y) wäre ein Hauptideal in $\mathbb{C}[x, y]$, d.h. es gibt ein $f \in \mathbb{C}[x, y]$ mit $(x, y) = (f)$. Dann gibt es $g, h \in \mathbb{C}[x, y]$ mit $x = fg$ und $y = fh$. Betrachten wir nun den Grad in der Variablen y, so erhalten wir

$$0 = \operatorname{grad}_y(x) = \operatorname{grad}_y(fg) = \operatorname{grad}_y(f) + \operatorname{grad}_y(g)$$

und somit folgt $\operatorname{grad}_y(f) = 0$. Genauso erhalten wir für den Grad in der Variablen x

$$0 = \operatorname{grad}_x(y) = \operatorname{grad}_x(fh) = \operatorname{grad}_x(f) + \operatorname{grad}_x(h) \ ,$$

d.h. es gilt auch $\operatorname{grad}_x(f) = 0$. Somit folgt $f \in \mathbb{C}$ und da $f \neq 0$ ist, ist f invertierbar. Somit gilt $1 \in (f) = (x, y)$, d.h. es gibt Polynome $k, l \in \mathbb{C}[x, y]$ mit $1 = k \cdot x + l \cdot y$. Das Polynom rechts hat nun eine Nullstell bei $(x, y) = (0, 0)$, das konstante Polynom links jedoch nicht. Somit können die Polynome nicht übereinstimmen und es folgt $1 \notin (x, y)$. insgesamt liefert dies einen Widerspruch und wir erhalten, dass (x, y) kein Hauptideal ist.

(b) Angenommen $(2, x)$ ist ein Hauptideal in $\mathbb{Z}[x]$, dann gibt es ein $f \in \mathbb{Z}[x]$ mit $(f) = (2, x)$. Somit existieren $g, h \in \mathbb{Z}[x]$, sodass $2 = fg$ und $x = fh$. Da 2 ein Polynom von Grad 0 ist und $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$ gilt, folgt $\operatorname{grad}(f) = \operatorname{grad}(g) = 0$. Somit ist f eine ganze Zahl und ein Teiler von x, d.h. f ist entweder 1 oder -1. In beiden Fällen folgt, dass $1 \in (2, x)$ ist. Somit gibt es Polynome $k, l \in Z[x]$, sodass $1 = k \cdot 2 + l \cdot x$. Vergleichen wir nun die konstanten Terme auf beiden Seiten, so sehen wir, dass der konstante Term von $k \cdot 2$ gleich 1 sein muss. Sei $k = k_0 + k_1 x + ... + k_n x^n$, dann ist der konstante Term von $k \cdot 2$ gegeben durch $2k_0$. Wir erhalten also die Gleichung $2k_0 = 1$, diese hat jedoch in $\mathbb{Z}$ keine Lösung. Somit folgt $1 \notin (2, x)$ und daher ist $(2, x)$ kein Hauptideal.