M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 5

Aufgabe 17

(1) Man finde in $\mathbb{Z}[X]$ Elemente $u(X)$ und $v(X)$ mit einem größten gemeinsamen Teiler $g(X)$, für welche gilt:

$$(u(X), v(X)) \subset (g(X)) .$$

(2) Ist $\mathbb{Z}[X]$ ein Hauptidealbereich?

Lösung.
Zu (1). Es ist $g(X) := 1$ der größte gemeinsame Teiler von $u(X) := 2$ und $v(X) := X$. Denn jeder Teiler von 2 ist konstant. Und jeder Teiler von X hat Leitkoeffizient 1. Es ist

$$(2, X) = (u(X), v(X)) \subset (g(X)) = (1) = \mathbb{Z}[X] .$$

Denn *wäre* $(2, X) = (1)$, dann gäbe es $s(X)$, $t(X) \in \mathbb{Z}[X]$ mit $1 = 2 \cdot s(X, Y) + X \cdot t(X, Y)$. Dann wäre aber auch $1 = 2 \cdot s(0, 0) + 0 \cdot t(0, 0) = 2 \cdot s(0, 0)$, wobei $s(0, 0) \in \mathbb{Z}$. Was *nicht sein kann*.

Zu (2). Nein, $\mathbb{Z}[X]$ ist kein Hauptidealbereich. Denn *wäre* $\mathbb{Z}[X]$ ein Hauptidealbereich, dann wäre in (1) auch stets $(u(X), v(X)) = (g(X))$, wenn $g(X)$ ein größter gemeinsamer Teiler von $u(X)$ und $v(X)$ ist; cf. Bemerkung 66. Dies ist aber in (1) *widerlegt* worden.

Aufgabe 18

(1) In $\mathbb{Z}$ berechne man $\mathrm{ggT}(784, 910)$ mittels Euklidischem Algorithmus.

(2) In $\mathbb{Z}$ berechne man $\mathrm{ggT}(784, 910)$ mittels Primfaktorzerlegungen.

(3) In $\mathbb{F}_3[X]$ berechne man $\mathrm{ggT}(X^9 + X^3 + 1, X^4 + X^2 + X)$.

(4) In $\mathbb{Z}[\mathrm{i}]$ berechne man einen größten gemeinsamen Teiler von 2 und $\mathrm{i} - 3$.

Lösung.
Zu (1). Wir iterieren wie folgt die Division mit Rest.

$$\begin{aligned} 910 &= 1 \cdot 784 + 126 \\ 784 &= 6 \cdot 126 + 28 \\ 126 &= 4 \cdot 28 + 14 \\ 28 &= 2 \cdot 14 + 0 \end{aligned}$$

Also ist $\mathrm{ggT}(784, 910) = 14$.

Zu (2). Es ist $784 = 2^4 \cdot 5^0 \cdot 7^2 \cdot 13^0$. Es ist $910 = 2^1 \cdot 5^1 \cdot 7^1 \cdot 13^1$.
Verwendung des minimalen jeweiligen Exponenten gibt $\mathrm{ggT}(784, 910) = 2^1 \cdot 5^0 \cdot 7^1 \cdot 13^0 = 14$.

Zu (3). Wir iterieren wie folgt die Division mit Rest.

$$\begin{aligned} X^9 + X^3 + 1 &= (X^5 - X^3 - X^2 + X - 1) \cdot (X^4 + X^2 + X) + (X^3 + X + 1) \\ X^4 + X^2 + X &= X \cdot (X^3 + X + 1) + 0 \end{aligned}$$

Also ist $\mathrm{ggT}(X^9 + X^3 + 1, X^4 + X^2 + 1) = X^3 + X + 1$.

Zu (4). Wir iterieren wie folgt die Division mit Rest, bezüglich der Gradfunktion d, für welche $d(z) = |z|^2$ ist für $z \in \mathbb{Z}[\mathrm{i}]$.

$$\begin{aligned} \mathrm{i} - 3 &= (-2) \cdot 2 + (\mathrm{i} + 1) \\ 2 &= (\mathrm{i} - 1) \cdot (\mathrm{i} + 1) + 0 \end{aligned}$$

Also ist $\mathrm{i} + 1$ ein größter gemeinsamer Teiler von 2 und $\mathrm{i} - 3$.

Aufgabe 19 Man zeige oder widerlege.

(1) Sei R ein faktorieller Integritätsbereich. Seien $x, y \in R^\times$.

Es sind x und y assoziiert genau dann, wenn $\mathrm{v}_p(x) = \mathrm{v}_p(y)$ ist für alle primen $p \in R$.

(2) Sei R ein faktorieller Integritätsbereich. Sei $f(X) \in R[X]$. Sei $g \in R$ ein größter gemeinsamer Teiler der Koeffizienten von $f(X)$.

Es ist $f(X)$ genau dann primitiv, wenn $g \in \mathrm{U}(R)$ ist.

(3) Sei R ein faktorieller Integritätsbereich. Sei $K := \mathrm{Quot}(R)$. Seien $f(X), g(X) \in R[X]$.

Genau dann ist $f(X)$ in $R[X]$ ein Teiler von $g(X)$,
wenn $f(X)$ in $K[X]$ ein Teiler von $g(X)$ ist.

(4) Sei $R = \mathbb{Z}[\mathrm{i}]$. Es ist $R[X]$ ein Hauptidealbereich.

Lösung.
Zu (1). Die Aussage ist richtig.
Wir rechnen in $K := \mathrm{Quot}(R)$. Wir wählen $P \subseteq R$ derart, daß jedes Primelement von R zu genau einem Element von P assoziiert ist.
Sei zum einen $\mathrm{v}_p(x) = \mathrm{v}_p(y)$ ist für alle primen $p \in R$. Sei $z := \frac{x}{y}$.
Dann ist $z = u \cdot \prod_{p \in P} p^{\mathrm{v}_p(z)} = u$ für ein $u \in \mathrm{U}(R)$. Also ist $x = uy$. Somit sind x und y assoziiert.
Seien zum anderen x und y assoziiert. Dann gibt es ein $u \in \mathrm{U}(R)$ mit $x = uy$. Sei $p \in R$ prim. Dann ist

$$\mathrm{v}_p(x) \;=\; \mathrm{v}_p(yu) = \mathrm{v}_p(y) + \mathrm{v}_p(u) \overset{\text{Bem. 61.(3)}}{=} \mathrm{v}_p(y)\ .$$

Zu (2). Die Aussage ist richtig. Wir schreiben $f(X) = \sum_{i \in [0,n]} a_i X^i$, wobei $n \geqslant 0$ und $a_i \in R$ für $i \in [0, n]$.
Denn es ist $f(X)$ genau dann primitiv, wenn $\mathrm{v}_q(f(X)) = 0$ ist für alle primen $q \in R$, d.h. wenn für $q \in R$ prim gilt:

$$0 \;=\; \min\{\, \mathrm{v}_q(a_i) \,:\, i \in [0,n] \,\} \;=\; \mathrm{v}_q(g)\ ,$$

d.h. wenn $g \in \mathrm{U}(R)$.

Zu (3). Die Aussage ist falsch. So zum Beispiel ist 2 in $\mathbb{Q}[X]$ ein Teiler von 1, aber nicht in $\mathbb{Z}[X]$.

Zu (4). Die Aussage ist falsch. Z.B. ist $(2, X) \subseteq \mathbb{Z}[\mathrm{i}][X]$ kein Hauptideal. *Annahme,* doch. Dann gibt es ein $f(X) \in \mathbb{Z}[\mathrm{i}][X]$ mit $(2, X) = (f(X))$. Da $f(X)$ ein Teiler von 2 ist, ist $f(X)$ konstant. Da $f(X)$ ein Teiler von X ist, ist diese Konstante eine Einheit in $\mathbb{Z}[\mathrm{i}]$. Aber dann ist $(f(X)) = \mathbb{Z}[\mathrm{i}][X]$. Insbesondere gibt es $u(X), v(X) \in \mathbb{Z}[\mathrm{i}][X]$ mit $u(X) \cdot 2 + v(X) \cdot X = 1$. Einsetzen von 0 gibt $u(0) \cdot 2 = 1$. Aber 2 ist keine Einheit in $\mathbb{Z}[\mathrm{i}]$. *Widerspruch.*

Aufgabe 20

(1) In S_5 berechne man $(1,2,4)(3,5) \circ (1,5,3,4)$.

(2) In S_5 berechne man $(1,3,5) \circ (2,3,4)(1,5) \circ (1,3,5)^{-1}$.

(3) In S_5 bestimme man $\{\, (1,2,3,4)^k \,:\, k \in \mathbb{Z} \,\}$.

(4) Man gebe die Primfaktorzerlegung von $|\,\mathrm{GL}_3(\mathbb{F}_3)|$ an.

Lösung.
Zu (1). Es ist $(1,2,4)(3,5) \circ (1,5,3,4) = (1,3)(2,4)(5) = (1,3)(2,4)$.

Zu (2). Es ist $(1,3,5) \circ (2,3,4)(1,5) \circ (1,3,5)^{-1} = (1,3,5) \circ (2,3,4)(1,5) \circ (5,3,1) = (1,3)(2,5,4)$.
Alternativ kann man auch $(1,3,5) \circ (2,3,4)(1,5) \circ (1,3,5)^{-1} = {}^{(1,3,5)}(2,3,4)(1,5) = (2,5,4)(3,1) = (1,3)(2,5,4)$ rechnen mit der Konjugationsregel.

Zu (3). Es ist $(1,2,3,4)^0 = \mathrm{id}$, $(1,2,3,4)^1 = (1,2,3,4)$, $(1,2,3,4)^2 = (1,3)(2,4)$, $(1,2,3,4)^3 = (1,4,3,2)$ und $(1,2,3,4)^4 = \mathrm{id}$. Also ist

$$\{\, (1,2,3,4)^k \,:\, k \in \mathbb{Z} \,\} \;=\; \{\, \mathrm{id},\, (1,2,3,4), (1,3)(2,3),\, (1,4,3,2) \,\}\,.$$

Zu (4). In der ersten Spalte eines Elements von $\mathrm{GL}_3(\mathbb{F}_3)$ kann ein beliebiges Element von $\mathbb{F}_3^{3\times 1}$ ungleich 0 stehen. In der zweiten eines, das nicht im Aufspann der ersten Spalte liegt. In der zweiten eines, das nicht im Aufspann der ersten beiden Spalten liegt.
Somit wird

$$|\,\mathrm{GL}_3(\mathbb{F}_3)| \;=\; (3^3-3^0)(3^3-3^1)(3^3-3^2) \;=\; 26\cdot 24\cdot 18 \;=\; 2^5\cdot 3^3\cdot 13\,.$$