M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 4

Aufgabe 13 Man zeige oder widerlege.

Sei R ein Integritätsbereich. Sei $a \in R^\times \smallsetminus \mathrm{U}(R) \subseteq R$ prim.

(1) Es ist $R/(a)$ ein Körper.

(2) Ist $R/(a)$ endlich als Menge, dann ist $R/(a)$ ein Körper.

(3) Es ist $b := a^2$ nicht prim.

(4) Sei $u \in \mathrm{U}(R)$. Es ist $u \cdot a \in R^\times \smallsetminus \mathrm{U}(R)$ prim.

Lösung.
Zu (1). Die Aussage ist falsch. So etwa ist $X \in \mathbb{Z}[X]$ prim, da wir den Ringisomorphismus

$$\varphi \,:\, \mathbb{Z}[X]/(X) \,\tilde{\to}\, \mathbb{Z} \,:\, f(X) \,\mapsto\, f(0)$$

haben und $\mathbb{Z}$ ein Integritätsbereich ist. Oder aber, da X irreduzibel ist und da $\mathbb{Z}[X]$ faktoriell ist.
Aber $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ ist kein Körper.

Zu (2). Die Aussage ist richtig. Zunächst ist $R/(a)$ ein Integritätsbereich, da a prim ist.
Es bleibt zu zeigen, daß ein endlicher Integritätsbereich S bereits ein Körper ist. Sei $s \in S^\times$. Wir müssen ein $t \in S^\times$ mit $st = 1$ finden.
Die Abbildung $S \to S : x \mapsto sx$ ist injektiv, da für $x, \tilde{x} \in S$ aus $sx = s\tilde{x}$ folgt, daß $s(x - \tilde{x}) = 0$ ist, wegen $s \neq 0$ und S Integritätsbereich also $x - \tilde{x} = 0$, d.h. $x = \tilde{x}$.
Da nun S endlich ist, ist diese injektive Abbildung tatsächlich bijektiv. Insbesondere liegt 1 in ihrem Bild. D.h. es gibt ein $t \in S$ mit $st = 1$.

Zu (3). Die Aussage ist richtig. Es genügt zu zeigen, daß b nicht irreduzibel ist; vgl. Bemerkung 55.(5). Es ist $b = a \cdot a$. Es ist der erste Faktor a keine Einheit in R. *Annahme*, es ist $a = ub$ für ein $u \in \mathrm{U}(R)$. Da R ein Integritätsbereich ist, folgt aus $a = ua^2$ dann $1 = ua$, und damit, daß $a \in \mathrm{U}(R)$ ist. *Widerspruch.* Somit ist b nicht irreduzibel; vgl. Bemerkung 55.(2).

Zu (4). Die Aussage ist richtig. Denn zum einen ist $u \cdot a$ weder 0 noch eine Einheit. Sodann ist die Eigenschaft, daß a prim ist, ist über eine Eigenschaft des Ideals (a) definiert; vgl. Definition 54.(2). Und wegen $u \in \mathrm{U}(R)$ ist $(a) = (u \cdot a)$. Also ist auch $u \cdot a$ prim.

Aufgabe 14 Sei R ein faktorieller Integritätsbereich. Sei $K := \mathrm{Quot}(R)$. Sei $p \in R$ prim.

Man zeige.

(1) Seien $x, y \in R^\times$. Sei $g \in R^\times$ ein größter gemeinsamer Teiler von x und y.
Sei $a \in R^\times$ ein Teiler von x und y.

Dann ist a ein Teiler von g. Ferner ist $\frac{g}{a}$ ein größter gemeinsamer Teiler von $\frac{x}{a}$ und $\frac{y}{a}$.

(2) Seien $x, y \in K$. Es ist $\mathrm{v}_p(x \cdot y) = \mathrm{v}_p(x) + \mathrm{v}_p(y)$.

(3) Seien $x, y \in K$. Es ist $\mathrm{v}_p(x + y) \geqslant \min\{\, \mathrm{v}_p(x),\, \mathrm{v}_p(y) \,\}$.

Falls $\mathrm{v}_p(x) \neq \mathrm{v}_p(y)$, dann ist $\mathrm{v}_p(x + y) = \min\{\, \mathrm{v}_p(x),\, \mathrm{v}_p(y) \,\}$.

Lösung.
Zu (1). Da a ein Teiler ist von x und von y, ist a auch ein Teiler von g; vgl. Definition 62.(ii).
Wir wollen zeigen, daß $\frac{g}{a}$ ein größter gemeinsamer Teiler von $\frac{x}{a}$ und $\frac{y}{a}$ ist. Wir verwenden dazu Definition 62.
Zu (i). Es ist $\frac{g}{a}$ ein Teiler von $\frac{x}{a}$ und von $\frac{y}{a}$, da g ein Teiler von x und von y ist.
Zu (ii). Sei $z \in R$ ein Teiler von $\frac{x}{a}$ und von $\frac{y}{a}$. Wir haben zu zeigen, daß z ein Teiler von $\frac{g}{a}$ ist.
In der Tat ist za ein Teiler von x und von y, damit auch von g. Sei $zab = g$, für ein geeignetes $b \in R$. Dann ist auch $zb = \frac{g}{a}$ und also z ein Teiler von $\frac{g}{a}$.

Zu (2). Ist $x = 0$ oder $y = 0$, so steht auf beiden Seiten ∞.
Seien nun $x,\, y \in K^\times$. Wir schreiben $x = \frac{a}{c}$ und $y = \frac{b}{d}$, wobei $a,\, b,\, c,\, d \in R^\times$.
Es ist $\mathrm{v}_p(x \cdot y) = \mathrm{v}_p(\frac{ab}{cd}) = \mathrm{v}_p(ab) - \mathrm{v}_p(cd)$.
Es ist $\mathrm{v}_p(x) + \mathrm{v}_p(y) = \mathrm{v}_p(\frac{a}{c}) + \mathrm{v}_p(\frac{b}{d}) = \mathrm{v}_p(a) + \mathrm{v}_p(b) - \mathrm{v}_p(c) - \mathrm{v}_p(d)$.
Es genügt also zu zeigen, daß $\mathrm{v}_p(ab) \stackrel{!}{=} \mathrm{v}_p(a) + \mathrm{v}_p(b)$ ist.
Da $p^{\mathrm{v}_p(a)}$ ein Teiler von a ist und $p^{\mathrm{v}_p(b)}$ ein Teiler von b, ist $p^{\mathrm{v}_p(a)+\mathrm{v}_p(b)}$ ein Teiler von ab.
Wegen der Maximalität von $\mathrm{v}_p(a)$ ist p kein Teiler von $a' := p^{-\mathrm{v}_p(a)} \cdot a \in R$. Wegen der Maximalität von $\mathrm{v}_p(b)$ ist p kein Teiler von $b' := p^{-\mathrm{v}_p(b)} \cdot b \in R$. Da p prim ist, ist p auch kein Teiler von $a'b' = p^{-(\mathrm{v}_p(a)+\mathrm{v}_p(b))}ab$. Somit hat der Exponent $\mathrm{v}_p(a) + \mathrm{v}_p(b)$ auch die von $\mathrm{v}_p(ab)$ verlangte Maximalität.
Insgesamt haben wir $\mathrm{v}_p(a) + \mathrm{v}_p(b) = \mathrm{v}_p(ab)$.

Zu (3). Ist $x = 0$ und $y = 0$, so steht auf beiden Seiten ∞.
Ist $x \neq 0$ und $y = 0$, so steht auf beiden Seiten $\mathrm{v}_p(x)$.
Ist $x = 0$ und $y \neq 0$, so steht auf beiden Seiten $\mathrm{v}_p(y)$.
Seien nun $x,\, y \in K^\times$. Wir schreiben $x = \frac{a}{c}$ und $y = \frac{b}{c}$ mit einem gemeinsamen Nenner c, wobei $a,\, b,\, c \in R^\times$.
Es ist $\mathrm{v}_p(x + y) = \mathrm{v}_p(\frac{a+b}{c}) = \mathrm{v}_p(a + b) - \mathrm{v}_p(c)$.
Es ist
$$\min\{\,\mathrm{v}_p(x),\, \mathrm{v}_p(y)\,\} = \min\{\,\mathrm{v}_p(\tfrac{a}{c}),\, \mathrm{v}_p(\tfrac{b}{c})\,\} = \min\{\,\mathrm{v}_p(a) - \mathrm{v}_p(c),\, \mathrm{v}_p(b) - \mathrm{v}_p(c)\,\} = \min\{\,\mathrm{v}_p(a),\, \mathrm{v}_p(b)\,\} - \mathrm{v}_p(c)\ .$$
Da auf beiden Seiten der Summand $-\mathrm{v}_p(c)$ steht, ist o.E. $x = a$ und $y = b$.
Es ist o.E. $\mathrm{v}_p(a) \leqslant \mathrm{v}_p(b)$. Also ist $\min\{\,\mathrm{v}_p(a),\, \mathrm{v}_p(b)\,\} = \mathrm{v}_p(a)$.
Wir schreiben $a = p^{\mathrm{v}_p(a)} \cdot a'$ und $b = p^{\mathrm{v}_p(b)} \cdot b'$ mit $a',\, b' \in R$, welche nicht von p geteilt werden.
Es ist $a + b = p^{\mathrm{v}_p(a)} \cdot a' + p^{\mathrm{v}_p(b)} \cdot b' = p^{\mathrm{v}_p(a)} \cdot (a' + p^{\mathrm{v}_p(b)-\mathrm{v}_p(a)}b')$. Dies zeigt

$$\min\{\,\mathrm{v}_p(a),\, \mathrm{v}_p(b)\,\} \;=\; \mathrm{v}_p(a) \;\leqslant\; \mathrm{v}_p(a + b)\ .$$

Ist $\mathrm{v}_p(a) < \mathrm{v}_p(b)$, dann ist $a' + p^{\mathrm{v}_p(b)-\mathrm{v}_p(a)}b'$ nicht durch p teilbar. Also ist $\mathrm{v}_p(a)$ der maximale Exponent e mit p^e teilt $a + b$. Somit ist diesenfalls

$$\min\{\,\mathrm{v}_p(a),\, \mathrm{v}_p(b)\,\} \;=\; \mathrm{v}_p(a) \;=\; \mathrm{v}_p(a + b)\ .$$

Aufgabe 15

(1) In $\mathbb{Z}$ berechne man $\mathrm{v}_2(600)$.

(2) Man finde ein $x \in \mathbb{Z}^\times$ mit $\mathrm{v}_3(x) = 4$ und $\mathrm{v}_2(x) = 1$. Ist x dadurch eindeutig bestimmt?

(3) Man finde $x,\, y \in \mathbb{Z}^\times$ mit $\mathrm{v}_3(x + y) - \min\{\mathrm{v}_3(x), \mathrm{v}_3(y)\} = 2$.

(4) Man finde $f(X) \in \mathbb{Q}[X]$ mit $\mathrm{v}_X(f(X)) < \mathrm{v}_{X^2+1}(f(X)) < \mathrm{v}_X(f(X)^2)$.

Lösung.
Zu (1). Es ist $600 = 2^3 \cdot 3^1 \cdot 5^2$. Also ist $\mathrm{v}_2(600) = 3$.

Zu (2). Für $x = 3^4 \cdot 2^1 = 162$ ist $\mathrm{v}_3(x) = 4$ und $\mathrm{v}_2(x) = 1$.
Aber auch für $\tilde{x} = -3^4 \cdot 2^1 \cdot 5^7$ ist $\mathrm{v}_3(\tilde{x}) = 4$ und $\mathrm{v}_2(\tilde{x}) = 1$. Also ist x nicht eindeutig bestimmt.

Zu (3). Sei $x = 1$ und $y = 8$. Dann ist

$$\mathrm{v}_3(x + y) - \min\{\mathrm{v}_3(x), \mathrm{v}_3(y)\} \;=\; \mathrm{v}_3(9) - \min\{\mathrm{v}_3(1), \mathrm{v}_3(8)\} \;=\; 2 - \min\{0, 0\} \;=\; 2\ .$$

Zu (4). Sei $f(X) = X^2(X^2+1)^3$. Dann ist

$$\mathrm{v}_X(X^2(X^2+1)^3) \;=\; 2 \;<\; \mathrm{v}_{X^2+1}(X^2(X^2+1)^3) \;=\; 3 \;<\; \mathrm{v}_X((X^2(X^2+1)^3)^2) \;=\; 4\,.$$

Aufgabe 16

(1) Man zeige: Es ist $(X,Y) \subseteq \mathbb{Q}[X,Y]$ kein Hauptideal; folglich ist $\mathbb{Q}[X,Y]$ kein Hauptidealbereich.

(2) Sei $R := \mathbb{F}_2[X]$. Man bestimme alle irreduziblen Elemente in $R^\times \smallsetminus \mathrm{U}(R)$ von Grad $\leqslant 3$.

Lösung.
Zu (1). *Annahme,* doch. Wir wählen $g(X,Y) \in \mathbb{Q}[X,Y]$ mit $(g(X,Y)) = (X,Y)$.
Dann ist X ein Vielfaches von $g(X,Y)$. Folglich tritt in $g(X,Y)$ kein Monom X^iY^j mit $j>0$ auf.
Dann ist Y ein Vielfaches von $g(X,Y)$. Folglich tritt in $g(X,Y)$ kein Monom X^iY^j mit $i>0$ auf.
Also ist $g(X,Y) = c$ für ein $c \in \mathbb{Q}$. Da $X \neq 0$, ist $c \neq 0$ und somit $c \in \mathrm{U}(\mathbb{Q}[X,Y])$. Also ist $(X,Y) = (c) = \mathbb{Q}[X,Y]$.
Folglich gibt es $u(X,Y)$, $v(X,Y) \in \mathbb{Q}[X,Y]$ mit $u(X,Y)\cdot X + v(X,Y)\cdot Y = 1$.
Also ist auch $0 = u(0,0)\cdot 0 + v(0,0)\cdot 0 = 1$. Wir haben einen *Widerspruch.*

Zu (2). Vorüberlegungen in $\mathbb{F}_2[X]$.
Ein Polynom hat genau dann die Nullstelle 0, wenn sein konstanter Term 0 ist.
Ein Polynom hat genau dann die Nullstelle 0, wenn es eine gerade Anzahl an auftretenden Monomen hat.
Bei einem Polynom von Grad 2 oder Grad 3 genügt es zu wissen, daß keine Nullstelle in $\mathbb{F}_2$ vorliegt, um es als irreduzibel zu erkennen.

Untersuchen wir nun die möglichen Grade.
Von Grad 0 gibt es nur Einheiten in $\mathbb{F}_2[X]$.
Von Grad 1 erhalten wir die irreduziblen Polynome X und $X+1$.
Von Grad 2 erhalten wir das irreduzible Polynom X^2+X+1. Das andere Polynom mit konstantem Term 1 hat eine gerade Anzahl von auftretenden Monomen.
Von Grad 3 erhalten wir die irreduzible Polynom X^3+X+1 und X^3+X^2+1. Die anderen Polynome mit konstantem Term 1 haben eine gerade Anzahl von auftretenden Monomen.