Algebra I, WiSe 2011\2012 – Lösung Blatt 12

12.1. Wir zeigen zunächst:

R Integritätsbereich, $a \in R \setminus \{0\}$ Keine Einheit

$\Rightarrow$ (a, X) in $R[X]$ Kein Hauptideal (*)

Dazu:

↗ $\exists\ f \in R[X]$ mit $(a, X) = (f)$.

$\Rightarrow$ $a \in (f)$ d.h. $a = g \cdot f$ für ein $g \in R[X] \setminus \{0\}$

$\Rightarrow$ $0 = \text{Grad}\, a = \text{Grad}\, g \cdot f$

R Integritäts-bereich $= \underbrace{\text{Grad}\, g}_{\geq 0} + \underbrace{\text{Grad}\, f}_{\geq 0}$

$\Rightarrow$ $\text{Grad}\, f = 0$, d.h. $f = c \in R \setminus \{0\}$.

Es ist $X \in (a, X) = (f)$

$\Rightarrow$ $\exists\ g \in R[X]$, $g(X) = a_0 + a_1 X + \dots + a_n X^n$ mit

$$c \cdot g(X) = X$$

d.h. $1 \cdot X = ca_0 + ca_1 X + \dots + ca_n X^n$

Koeff. vgl. $\Rightarrow$ $ca_0 = ca_2 = \dots = ca_n = 0$ und $ca_1 = 1$

$\Rightarrow$ c ist eine Einheit.

Also erhalten wir:

$$(a, X) = (c) = R[X].$$

Da $1 \in R[X]$ ist, existieren

$$h_1(X) = b_0 + b_1 X + \dots + b_m X^m$$

$$h_2(X) = c_0 + c_1 X + \dots + c_K X^K$$

in $R[X]$ mit

$$1 = h_1(X) \cdot a + h_2(X) \cdot X$$

$$= \underbrace{a b_0}_{=1} + \underbrace{a b_1 X + \dots + a b_m X^m + c_0 X + c_1 X^2 + \dots + c_K X^{K+}}_{=0 \text{ (Koeffizientenvergleich)}}$$

$\Rightarrow a b_0 = 1$

$\Rightarrow a$ ist Einheit ↯ a keine Einheit.

Damit ist (*) gezeigt.

Wir können nun direkt ein gesuchtes Gegenbeispiel angeben:

$\mathbb{Z}$ ist ZPE-Ring $\overset{\text{Gauß}}{\Rightarrow}$ $\mathbb{Z}[X]$ ist ZPE-Ring.

Da $2 \in \mathbb{Z}$ keine Einheit ist, folgt mit (*):

$(2, X) \subset \mathbb{Z}[X]$ kein Hauptideal.

$\Rightarrow \mathbb{Z}[X]$ ist kein Hauptidealring.

▨

12.2.

Mit dem Kriterium von Eisenstein:

(i) Lese das Polynom X^3-2 in $\mathbb{Z}[X]$ ($\mathbb{Z}$ ist ZPE-Ring).

$ggT(1,-2)=1 \Rightarrow$ Polynom primitiv

Wähle $p=2$ (Primelement), dann:

$$p \nmid 1 \quad p \mid -2 \quad \text{und} \quad p^2 \nmid -2$$

$\overset{\text{Eisenstein}}{\Rightarrow}$ $X^3-2 \in \mathbb{Z}[X]$ irreduzibel

$\Rightarrow$ $X^3-2 \in \mathbb{Q}[X]$ irreduzibel ($\mathbb{Q} = \text{Quot}(\mathbb{Z})$).

(iv) Analog zu (i): $ggT(1,-2,6,10)=1 \Rightarrow$ Polynom primitiv

Wähle $p=2 \Rightarrow$

$$p \nmid 1,\ p \mid -2,\ p \mid 6,\ p \mid 10,\ p^2 \nmid 10 \quad (p \mid 0).$$

$\Rightarrow X^5-2X^4+6X+10$ irreduzibel in $\mathbb{Q}[X]$.

(v) $X^2+Y^2-1 = Y^2+(X+1)(X-1) \in \mathbb{Q}[X,Y] = \mathbb{Q}[X][Y]$

Gauß $\Rightarrow \mathbb{Q}[X]$ ist ZPE-Ring.

$ggT(1,(X+1)(X-1))=1 \Rightarrow$ Polynom (nur in Y gelesen) ist primitiv.

Wähle $p=(X+1) \in \mathbb{Q}[X] \Rightarrow$ Primelement und

$$p \nmid 1,\ p \mid (X+1)(X-1),\ p^2 \nmid (X+1)(X-1)$$

$\overset{\text{Eisenstein}}{\Rightarrow}$ $Y^2+X^2-1 \in \mathbb{Q}[X,Y]$ irreduzibel.

Mit dem Gaußschen Lemma:

(ii) $ggT(1,5,1) = 1 \Rightarrow$ Polynom primitiv.

Also: Polynom in $\mathbb{Q}[X]$ irreduzibel
$\Leftrightarrow$ Polynom in $\mathbb{Z}[X]$ irreduzibel.

↗ $X^2 + 5X + 1$ in $\mathbb{Z}[X]$ reduzibel

$ggT=1 \Rightarrow$ also kein konstantes Primelement

$X^2 + 5X + 1 = (X+a)(X+b)$ für $a, b \in \mathbb{Z}$

$\Rightarrow a \cdot b = 1$ d.h. $a=b=1$ oder $a=b=-1$.

$\Rightarrow f(1)=0$ oder $f(-1)=0$.

Aber: $f(1) = 7 \neq 0$ und $f(-1) = -3 \neq 0$ ↯

$\Rightarrow$ Polynom in $\mathbb{Z}[X]$ und damit in $\mathbb{Q}[X]$ irreduzibel.

(iii) Analog: $ggT(1, 39, 4, 8) = 1$.

Wäre $X^3 + 39X^2 - 4X + 8$ in $\mathbb{Z}[X]$ reduzibel, so hätte ein Faktor Grad 1, wäre also von der Form $(X-a)$ mit $a \in \mathbb{Z}$.

$\Rightarrow a \mid 8$ d.h. $a \in \{-1, 1, -2, 2, -4, 4, -8, 8\}$.

Das Polynom hätte also an der Stelle $-a$ eine Nullstelle. Aber:

$f(-1) = 50 \neq 0$, $f(1) = 44 \neq 0$, $f(-2) = 164 \neq 0$

$f(2) = 164 \neq 0$, $f(-4) = 584 \neq 0$, $f(4) = 680 \neq 0$

$f(-8) = 2024 \neq 0$, $f(8) = 2984 \neq 0$. ↯

$\Rightarrow$ Polynom irreduzibel

12.3.

$ggT(1,n) = 1 \Rightarrow f_n(X)$ $\forall n \in \mathbb{Z}$ primitiv.

Also: $\forall n \in \mathbb{Z}$: $f_n(X)$ reduzibel in $\mathbb{Q}[X]$
$\Leftrightarrow f_n(X)$ reduzibel in $\mathbb{Z}[X]$.

Da $ggT(1,n) = 1$ ist, folgt:

f_n reduzibel in $\mathbb{Z}[X]$
$\Leftrightarrow \exists\, a,b,c \in \mathbb{Z}$ mit
$$X^3 + nX^2 + X + 1 = (X^2 + aX + b)(X + c)$$

Koeffizientenvergleich liefert, dass $b \cdot c = 1$ gelten muss.
Fallunterscheidung (andere Möglichkeiten gibt es nicht, wenn f_n reduzibel sein soll):

$\underline{b = c = 1}$:

$$(X^2 + aX + 1)(X + 1) = X^3 + (a+1)X^2 + (a+1)X + 1$$
$$= X^3 + nX^2 + X + 1$$

Also muss $a = 0$ d.h. $n = 1$ gelten und in diesem Fall ist f_n reduzibel.

$\underline{b = c = -1}$:

$$(X^2 + aX - 1)(X - 1) = X^3 + (a-1)X^2 + (-a-1)X + 1$$
$$= X^3 + nX^2 + X + 1$$

Also muss $a = -2$, d.h. $n = -3$ gelten und in diesem Fall ist f_n reduzibel.

Insgesamt: f_n reduzibel $\Leftrightarrow n \in \{1, -3\}$.

12.4. (i) $K[X]$ ist euklidischer Ring, also insbesondere Hauptidealring. Daher können wir schließen:

$$f \text{ irreduzibel} \Rightarrow (f) \text{ ist maximales Ideal}$$

$$\overset{\text{VL}}{\Rightarrow} \frac{K[X]}{(f)} \text{ ist ein Körper.}$$

(ii) Wir schreiben zunächst $f(X) = a_0 + a_1 X + \dots + a_n X^n$, einmotig, $a_n \neq 0$.

- Behauptung: Sind $g, h \in K[X]$ mit Grad $g < n$ und Grad $h < n$, dann gilt:

$$\bar{g} = \bar{h} \iff g = h.$$

Denn:

$g = h \Rightarrow \bar{g} = \bar{h}$ ist klar. Gelte also $\bar{g} = \bar{h}$.

↗ $g \neq h$. Wegen $\bar{g} = \bar{h}$ folgt $g - h \in (f)$ d.h.

$$g - h = p \cdot f \quad \text{für ein } p \in K[X]$$

Da $g \neq h$ gilt, muss $p \neq 0$ sein und wir erhalten

$$n > \text{Grad}(g-h) = \text{Grad}(p \cdot f) = \underbrace{\text{Grad}(p)}_{\geq 0} + \underbrace{\text{Grad}(f)}_{= n}$$

$$\geq n$$

d.h. $n > n$ ↯ Es gilt also doch $g = h$.

- Behauptung: Ist $g \in K[X]$ mit Grad $g \geq n$, so existiert ein $p \in K[X]$ mit Grad $p < n$ und

$$\overline{g} = \overline{p}$$

Dazu: K Körper $\Rightarrow$ $K[X]$ euklidischer Ring (bzgl. Grad)
Wir dividieren g mit Rest durch f, d.h. $\exists\, s, r \in K[X]$ mit

$$g = s \cdot f + r \quad \text{und} \quad \text{Grad } r < \text{Grad } f = n$$
$$\text{oder} \quad r = 0, \text{ d.h. } -\infty = \text{Grad } r < n$$

Definiere $p := r$, dann Grad $p < n$ und da $s \cdot f \in (f)$, folgt:

$$\overline{g} = \underbrace{\overline{s \cdot f}}_{= \overline{0}} + \overline{p} = \overline{p} \qquad \text{ok.}$$

- Beide Behauptungen zusammen zeigen offenbar, dass

$$K[X]/(f)$$

genau aus den verschiedenen (!) Elementen

$$\overline{a_0} + \overline{a_1}\,\overline{X} + \dots + \overline{a_{n-1}}\,\overline{X}^{n-1} \quad \text{mit } a_i \in K$$

besteht. Wegen $|K| = q$ folgt daher

$$\left| K[X]/(f) \right| = |K|^n = q^n .$$

(iii) Vom Grad 0 gibt es Keines (Körper).

Grad 1:

X und $X+1$ irreduzibel (d.h. alle möglichen).

Grad 2:

Reduzibel sind genau die Produkte von Grad 1-Polynomen

also:

$$X^2, \quad (X+1)^2 = X^2+1, \quad X(X+1) = X^2+X$$

Bleibt als einziges irreduzibles Polynom vom Grad 2:

$$X^2+X+1$$

Also: Die irreduziblen Polynome vom Grad ≤ 2 sind

X

$X+1$

X^2+X+1

(iv) Ein Körper mit 4 Elementen ist nach (ii) und (iii) gegeben durch

$$\mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1) \qquad (= \mathbb{F}_4)$$

Verknüpfungstafeln (rechnen..)

+	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{X+1}$	$\overline{X}$
$\overline{X}$	$\overline{X}$	$\overline{X+1}$	$\overline{0}$	$\overline{1}$
$\overline{X+1}$	$\overline{X+1}$	$\overline{X}$	$\overline{1}$	$\overline{0}$

·	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{X}$	$\overline{X+1}$
$\overline{X}$	$\overline{0}$	$\overline{X}$	$\overline{X+1}$	$\overline{1}$
$\overline{X+1}$	$\overline{0}$	$\overline{X+1}$	$\overline{1}$	$\overline{X}$

∎