F25T3A3 (Fortsetzung)

(b) Bestimmen Sie alle Paare (f, g) aus $\mathbb{Q}[x,y] \times \mathbb{Q}[x,y]$ mit der Eigenschaft

$$f \cdot (x^6 - y^6) + g \cdot (x^5 y + x^3 y^3 + x y^5) \overset{(*)}{=} 0$$

Bereits in Teil (a) haben wir den Einsetzungshom. $\phi : \mathbb{Q}[x,y] \to \mathbb{Q}[x]$, $h \mapsto h(x,0)$.

Ang., (f,g) ist ein Paar, das $(*)$ erfüllt.

$$\Rightarrow \phi(f) \cdot (x^6 - 1) + \phi(g) \cdot (x^5 + x^3 + x) \overset{(**)}{=} 0$$

Ang., (f,g) ist ein Paar, das $(*)$ erfüllt.

Eine Anwendung des Eukl. Alg. ergibt

$ggT(x^6-1, x^5+x^3+x) = x^4+x^2+1$

Polynomdiv. $\Rightarrow x^6-1 = (x^2-1)(x^4+x^2+1)$

und $x^5+x^3+x = x\cdot(x^4+x^2+1)$ also:

$(**) \Longleftrightarrow \phi(f)\cdot(x^2-1)\cdot(x^4+x^2+1) + \phi(g)\cdot x\cdot(x^4+x^2+1) = 0$

Kürzungsregel ($\mathbb{Q}[x]$ Int.-bereich)

$\Longleftrightarrow \phi(f)\cdot(x^2-1) + \phi(g)\cdot x = 0$

$\Longrightarrow \phi(f)(x+1)(x-1) + \phi(g)\cdot x = 0$

$\Longrightarrow \phi(g)\cdot x = -\phi(f)\cdot(x+1)\cdot(x-1)$

Es gilt also $x \mid \phi(f)$ und $(x+1)(x-1) \mid \phi(g)$.

(b) Beweisen Sie auf der Grundlage Ihrer Definition

Es gibt also ein $u \in \mathbb{Q}[x]$ mit $\phi(f) = u \cdot x$

und: $\phi(g) \cdot x = -ux(x+1)(x-1)$

$\Rightarrow \phi(g) = -u(x+1)(x-1)$

Genauso erhält man im Ring $\mathbb{Q}[x,y]$ für alle $f, g \in \mathbb{Q}[x]$:

$$f \cdot (x^6 - y^6) + g \cdot (x^5 y + x^3 y^3 + x y^5) = 0 \quad \Leftrightarrow$$

$$f \cdot (x^2 - y^2)(x^4 + x^2 y^2 + y^4) + g \cdot xy \cdot (x^4 + x^2 y^2 + y^4) = 0$$

$$\Leftrightarrow f \cdot (x+y)(x-y) + g \cdot x \cdot y = 0$$

Da also x, y Teiler von f sind, und $x \pm y$ Teiler von g, ist dies äquivalent dazu, dass ein $u \in \mathbb{Q}[x,y]$

existiert mit $f = u \cdot x \cdot y$, $g = -u(x+y)(x-y)$.
Also ist die gesuchte Menge gegeben durch

$$\{(u \cdot x \cdot y, -u(x+y)(x-y)) \mid u \in \mathbb{Q}[x,y]\}. \qquad \square$$

H22T3A2

(a) Geben Sie eine vollständige Def. des kgV zweier ganzer Zahlen an.

(b) Beweisen Sie auf der Grundlage Ihrer Definition für alle $a, b, c, d \in \mathbb{Z}$ die Gleichung

$$kgV(kgV(a,b), kgV(c,d)) = kgV(kgV(a,c), kgV(b,d)).$$

Für $f \in \mathbb{Q}[x,y]$ mit $\phi(f) = u \cdot x$

zu(a) Das kgV zweier bel. ganzer Zahlen a, b ist die eindeutig bestimmte Zahl $n \in \mathbb{N}_0$ mit folgenden Eigenschaften:

(i) $a \mid n$ und $b \mid n$

(ii) Ist $m \in \mathbb{N}_0$ mit $a \mid m$ und $b \mid m$, dann folgt $n \mid m$.

zu(b) Seien $a, b, c, d \in \mathbb{N}_0$ und $r = \mathrm{kgV}(\mathrm{kgV}(a,c), \mathrm{kgV}(b,d))$. Wir zeigen, dass r die definierenden Eigenschaften von $\mathrm{kgV}(\mathrm{kgV}(a,b), \mathrm{kgV}(c,d))$ besitzt, also

(i) $\operatorname{kgV}(a,b) \mid r$ und $\operatorname{kgV}(c,d) \mid r$

(ii) Ist $m \in \mathbb{N}_0$ mit $\operatorname{kgV}(a,b) \mid m$ und $\operatorname{kgV}(c,d) \mid m$, dann folgt $r \mid m$.

zu (i) Nach Def von r gilt $\operatorname{kgV}(a,c) \mid r$ und $\operatorname{kgV}(b,d) \mid r$. $a \mid \operatorname{kgV}(a,c)$, $\operatorname{kgV}(a,c) \mid r$ $\Rightarrow a \mid r$, ebenso: $b \mid \operatorname{kgV}(b,d)$, $\operatorname{kgV}(b,d) \mid r$ $\Rightarrow b \mid r$ dann: $a \mid r$ und $b \mid r \Rightarrow$ $\operatorname{kgV}(a,b) \mid r$. Ebenso zeigt man $\operatorname{kgV}(c,d) \mid r$ (Übung)

zu (ii) Sei $m \in \mathbb{N}_0$ mit $\operatorname{kgV}(a,b) \mid m$ und $\operatorname{kgV}(c,d) \mid m$. z.zg: $r \mid m$

Nach Def. von r genügt es zu zeigen, dass $\mathrm{kgV}(a,c) \mid m$ und $\mathrm{kgV}(b,d) \mid m$ gilt; denn nach Eig (ii) des kgV folgt daraus $r \mid m$.

$a \mid \mathrm{kgV}(a,b),\ \mathrm{kgV}(a,b) \mid m \Rightarrow a \mid m$

$b \mid \mathrm{kgV}(a,b),\ \mathrm{kgV}(a,b) \mid m \Rightarrow b \mid m$

$c \mid \mathrm{kgV}(c,d),\ \mathrm{kgV}(c,d) \mid m \Rightarrow c \mid m$

$d \mid \mathrm{kgV}(c,d),\ \mathrm{kgV}(c,d) \mid m \Rightarrow d \mid m$

$a \mid m,\ c \mid m \Rightarrow \mathrm{kgV}(a,c) \mid m$

$b \mid m,\ d \mid m \Rightarrow \mathrm{kgV}(b,d) \mid m.$ □

Irreduzibilitätskriterien

Satz:

(i) Sei K ein Körper, $f \in K[x]$. Gilt $\operatorname{grad}(f) \in \{2,3\}$ und besitzt f in K keine Nullstelle, dann ist f über K irreduzibel. Jedes Polynom vom Grad 1 in $K[x]$ ist irreduzibel (falsch über Ringen!).

(ii) Sei K ein Körper, $f \in K[x]$ und $\operatorname{grad}(f) \in \{4,5\}$. Hat f keine Nullstelle in K und wird f von keinem irreduziblen Pol. vom Grad 2 geteilt, dann ist

f in $K[x]$ irreduzibel.

(iii) Sei $f \in \mathbb{Z}[x]$ normiert und $a \in \mathbb{Z}$ der konstante Term von f. Ist $r \in \mathbb{Q}$ eine Nullstelle von f, dann gilt $r \in \mathbb{Z}$, und r ist ein Teiler von a.

(iv) Eisenstein-Kriterium: Ist R ein faktorielles Ring, $f = a_n x^n + \dots + a_1 x + a_0 \in R[x]$ ein primitives Polynom, und ist $p \in R$ ein Primelement mit $p \nmid a_n$, $p \mid a_k$ für $0 \le k < n$ und $p^2 \nmid a_0$, dann ist f in $R[x]$ irreduzibel (und auch über $K[x]$, wobei K den Quotientenkörper von R bezeichnet).

und ist $p \in R$ ein Primelement mit $p \nmid a_n$, $p \mid a_k$ für $0 \le k < n$ und $p^2 \nmid a_0$, dann ist f in $R[x]$ irreduzibel

(v) Reduktionskriterium: Sei R ein faktorieller Ring, $\mathfrak{p} \subseteq R$ ein maximales Ideal, $K = R/\mathfrak{p}$, $f \in R[x]$ primitiv, $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ mit $a_n \notin \mathfrak{p}$. Sei $\bar{f} \in K[x]$ das Bild von f in $K[x]$. Ist $\bar{f}$ in $K[x]$ irreduzibel, dann ist f in $R[x]$ irreduzibel. (Häufig: $R = \mathbb{Z}$, $\mathfrak{p} = (p)$ mit einer Primzahl p, $K = \mathbb{F}_p$)

Hinweis: Die Aussage $\bar{f}$ reduzibel $\Rightarrow$ f reduzibel ist im Allg. falsch, ebenso f irreduzibel $\Rightarrow$ $\bar{f}$ irreduzibel.

Aufgabe (Übung: F13T3A4)

(a) Bestimmen Sie alle irreduziblen Polynome vom Grad ≤ 3 in $\mathbb{F}_2[x]$.

(b) Zeigen Sie, dass $f = x^5 + 8x^4 - 6x^3 + 7x^2 - 4x + 15$ in $\mathbb{Q}[x]$ irreduzibel ist.

zu (a)

- Die Polynome in $\mathbb{F}_2[x]$ vom Grad 0 sind entweder Einheiten oder gleich null, also keine irreduziblen Elemente in $\mathbb{F}_2[x]$.
- Da $\mathbb{F}_2$ ein Körper ist, sind alle Polynome vom Grad 1 in $\mathbb{F}_2[x]$ irreduzibel, also x, $x+1$.

(ii)

(iv)

also keine irreduziblen Elemente in $\mathbb{F}_2[x]$.

- reduzible Polynome vom Grad 2 in $\mathbb{F}_2[x]$:
  x^2, $x\cdot(x+\bar{1}) = x^2+x$, $(x+\bar{1})^2 = x^2+\bar{2}x+\bar{1} = x^2+\bar{1}$
  Es gibt insgesamt 4 Polynome vom Grad 2, also ist $x^2+x+\bar{1}$ das einzige irreduzible
- reduzible Polynome vom Grad 3:
  Es gibt insgesamt 8 Polynome vom Grad 3.
  reduzible Polynome: x^3, $x^2(x+\bar{1}) = x^3+x^2$,
  $x(x+\bar{1})^2 = x(x^2+\bar{1}) = x^3+x$, $(x+1)^3 =$
  $(x^2+\bar{1})(x+\bar{1}) = x^3+x^2+x+\bar{1}$, $x\cdot(x^2+x+\bar{1})$
  $= x^3+x^2+x$, $(x+1)(x^2+x+1) = x^3+1$

Die einzigen irreduziblen Polynome vom Grad 3 sind also $x^3+x+\overline{1}$ und $x^3+x^2+\overline{1}$.

zu (6) Nach dem Reduktionskriterium genügt es zu zeigen, dass das Bild $\overline{f}$ von f in $\mathbb{F}_2[x]$ irreduzibel ist. Es ist $\overline{f} = x^5+x^2+\overline{1}$.

$\overline{f}(\overline{0}) = \overline{1} \neq \overline{0}$, $\overline{f}(\overline{1}) = \overline{3} = \overline{1} \neq \overline{0}$ $\Rightarrow$ $\overline{f}$ hat in $\mathbb{F}_2[x]$ keine Nullstellen. Angenommen, $\overline{f}$ ist demnach reduzibel. Wegen $\operatorname{grad}(\overline{f}) = 5$ ist $\overline{f}$ dann Produkt eines irreduziblen Polynoms g vom Grad 2 und eines irred. Polynoms h vom Grad 3.

$\bar{f}(\bar{0}) = \bar{1} + \bar{0}$ $\quad \rho(\bar{1}) = \bar{3} = \bar{1} + \bar{2}$ $\Rightarrow$ $\quad f$ ist

Teil (a) $\Rightarrow g = x^2 + x + \bar{1}$, $h \in \{x^3 + x + \bar{1}, x^3 + x^2 + \bar{1}\}$

aber: $(x^2 + x + \bar{1}) \cdot (x^3 + x + \bar{1}) = x^5 + x^4 + \bar{1} \neq f$

$(x^2 + x + \bar{1})(x^3 + x^2 + \bar{1}) = x^5 + x + \bar{1}$

Also ist f irreduzibel, und somit auch in $\mathbb{Z}[x]$, und damit auch in $\mathbb{Q}[x]$. $\square$

F21T3A1 Sei $f = x^{2021} + 105x^3 + 15x + 45$.

Entscheiden Sie, über welchen Ringen f ein irreduzibles Polynom ist.

(i) $K = \mathbb{Q}$ (ii) $K = \mathbb{R}$ (iii) $K = \mathbb{F}_2$

(iv) $K = \mathbb{Q}[t]/(f(t))$

zu (i) irreduzibel (Eisenstein-Krit. mit $p = 5$)

e von
$+x^2+\bar{1}$.

um genügt
f in $\mathbb{F}_2[x]$
$x^2+\bar{1}$.
$\neq \bar{0} \Rightarrow$
den. Ange-
. Wegen
ibt eines
Grad 2 und
Grad 3.

zu (ii) Jedes Polynom ungeraden Grades über $\mathbb{R}$ hat in $\mathbb{R}$ eine Nullstelle. $\Rightarrow$ f ist in $\mathbb{R}[x]$ reduzibel.

zu (iii) $f(\bar{1}) = \bar{1}+\bar{1}+\bar{1}+\bar{1} = \bar{4} = \bar{0}$
$\Rightarrow$ f hat in $\mathbb{F}_2$ eine Nullst $\xRightarrow{\text{grad}(f)>1}$
f ist in $\mathbb{F}_2[x]$ reduzibel

zu (iv) Da f in $\mathbb{Q}[x]$ irreduzibel ist, ist lt. Vl $R = \mathbb{Q}[t]/(f(t))$ ein Körper, der eine Nullstelle $x \in R$ von f besitzt, nämlich $x = t+(f(t))$. $\xRightarrow{\text{grad}(f)>1}$
f ist in $R[x]$ reduzibel $\square$