Feedback

○ Bonus, Aufgabe 6):

<u>zu Zeigen</u>: $z \in S \Rightarrow 1 + b - za \in S$

Lösung in vielen Abgaben:

$$a(1 + b - za) = 1$$
$$\Leftrightarrow a + ab - aza = 1$$
$$\Leftrightarrow \ldots$$
$$\Leftrightarrow 1 = 1$$

Ein Beweis sollte wie ein Pfad von Aussagen sein, der bei einer wahren Aussage/einer Annahme beginnt und durch Implikationen verbunden zu ___ führt!

○ Wir sind in $\langle R; +, -, 0, \cdot, 1 \rangle$, $a \in R$.

Darf man $a + a = 2a$ schreiben?

Nein! "2" ist nicht etwas, was wir in R kennen. 0,1 haben wir nur, weil wir die NE bezüglich "+", "·" so benannt haben. Das sind keine Zahlen da, nur Symbole! (wir nehmen 0,1 weil wir das von $\mathbb{Z}$ so kennen). Man könnte aber definieren $\forall a \in R \quad 2a := a + a$

○ R wie oben, $a, x, y \in R$.

Gilt

$$ax = 1 \quad \text{und} \quad ay = 1 \Rightarrow x = y?$$

Nein! Lemma 5.2. spricht nur von Inversen, also Elemente, die Links- <u>und</u> Rechtsinversen sind.

Was, wenn R kommutativ? L.5.2.

Ja. Dann gilt $1 = ax = xa \Rightarrow x = y$

Körper

Wieso ist $\frac{x}{0}$ nicht definiert? Wieso verlangen wir bei einem Körper nicht Invertierbarkeit von 0?

Inverse von Mult. $\hat{=}$ Division

$$0 \cdot x = 1 \Rightarrow x = \frac{1}{0}$$

aber wir wissen auch $0 \cdot x = 0$ nach den Ringeigenschaften.

$\Rightarrow$ Invertierbarkeit von 0 führt zu einem Widerspruch.

Polynome über einem Ring (R[X]), mögliche Vorstellungen

Sei R ein kommutativer Ring

ⓐ Wir konstruieren Tupel mit Elementen aus R

$$(a_0, a_1, \ldots, a_n) \quad \text{mit} \quad a_0, a_1, \ldots, a_n \in R \quad (\text{und } n \in \mathbb{N})$$

Alle solche Elemente packen wir in eine Menge

$$R[X] \hat{=} S = \{(a_0, a_1, \ldots, a_n) \mid n \in \mathbb{N} \land a_0, a_1, \ldots, a_n \in R\}$$

und definieren Operationen "⊞" und "⊡" auf die Elemente
in S   → wie gewohnt in Algebra!

Bsp.: +:
$$(a_0, a_1, \ldots, a_n)$$
$$\boxed{+}$$
$$(b_0, b_1, \ldots, b_n, \ldots, b_m)$$
$$:= (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, 0 + b_{n+1}, \ldots, 0 + b_m)$$

Addition in R

Wir definieren das so, dass $\langle S; ⊞, ⊟, (0,), ⊡, (1,) \rangle$
ein Ring definiert.

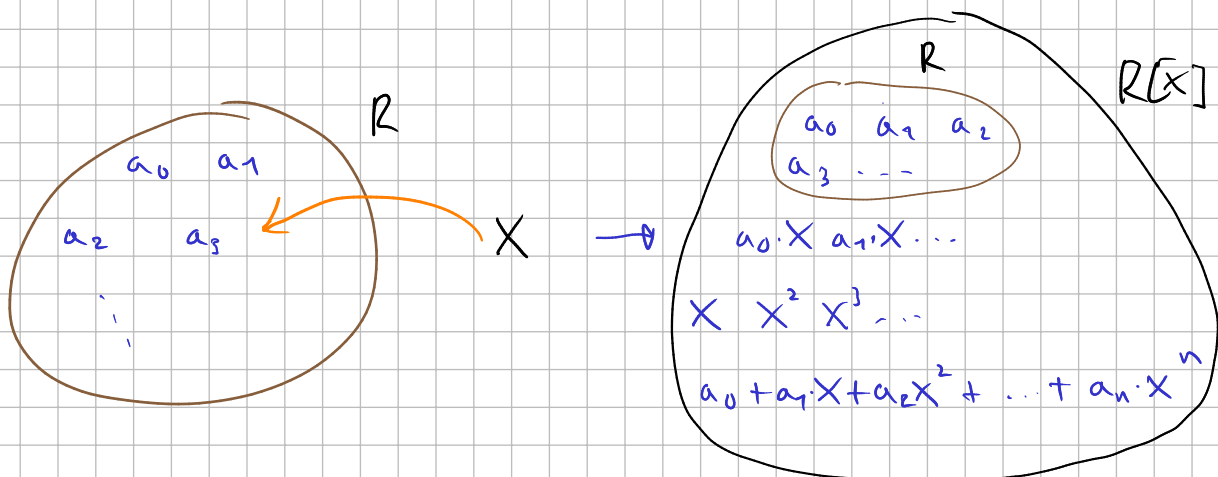ⓑ Wir erfinden ein Objekt "X" und "erweitern" R mit X, wir
nehmen es also zu R hinzu und bekommen R[X]. Daher die Notation "R[X]"
Analog wie bei Untergruppen, müssen wir dann schauen, dass
für alle $a, b \in R[X]$: $a \cdot b \in R[X]$, $a + b \in R[X]$

Konkret: $R \subseteq R[X]$, $X \in R[X]$. $a_0, a_1, \ldots \in R[X]$ und $X \in R[X]$
$$\Rightarrow a_0 \cdot X, a_1 \cdot X, \ldots \in R[X], \quad X \cdot X = X^2, X \cdot X \cdot X = X^3, X^4, \ldots \in R[X]$$
$$\Rightarrow a_0 + a_1 \cdot X + a_2 \cdot X^2 + \ldots + a_n \cdot X^n \in R[X]$$

Polynome über einem Körper

$\underbrace{a(x)}$ $\underbrace{m(x)}$

Teile $x^4 + 3x^2 + 4$ durch $4x^2 + 2x + 1$ in $\mathbb{Z}_5$ mit Rest.

Nach Satz 5.25 können wir das, weil

$$a(x) = m(x) \cdot \underbrace{q(x)}_{\text{was wir suchen}} + \underbrace{r(x)}_{\text{Rest}}$$

$4x \equiv_5 1 \Rightarrow x = 4$

$1x^4 + 3x^2 + 4 : 4x^2 + 2x + 1 = \underset{q(x)}{\underbrace{\underbrace{(4)}x^2 + 4(2)x + \underbrace{4\cdot 3}_{2}}_{3}}$

$-(4\cdot 4\cdot x^4 + 8x^3 + \overline{4x^2})$
$\quad \underbrace{1}$

$= -8x^3 - x^2 + 4$
$\quad \lfloor \mathbb{Z}_5$

$= (2)x^3 + 4x^2 + 4$

(wir berechnen da $a(x) - m(x) \cdot \underline{\quad} = $ Rest)

$-(2x^3 + 6x^2 + 3x)$
$\quad \underline{\quad\quad\quad\quad}$
$\quad -2x^2 - 3x + 4$

$= 3x^2 + 2x + 4$

$-(3x^2 + 4x + 2)$
$\quad \underline{\quad\quad\quad\quad}$

$= -2x + 2$

$= \underline{3x + 2} \rightarrow$ **der Rest $r(x)$**

Berechne
$$(x+3)(x+2)$$
in $\mathbb{Z}_5[x]_{x^2+4}$
$\quad \underbrace{\quad}_{m(x)}$

$(x+3)(x+2) \equiv_{m(x)} x^2 + \underbrace{2x + 3x}_{0} + 6 \equiv_{m(x)} x^2 + 6 - (x^2 + 4)$

$\equiv_{m(x)} 2$

$x^2 + 4$ in $\mathbb{Z}_5$

$a(1) = 0$, $a(4) = 0$

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

$\quad\quad\quad = (x+4)(x+1)$

$x^3 + 2x^2 + 1$ in $\mathbb{Z}_3$

$a(0) = 1$, $a(1) = 1 + 2 + 1 = 1$, $a(2) = \underbrace{8 + 2\cdot 4 + 1}_{\text{in } \mathbb{Z}} = 2 + 2 + 1 = 2$

$x^4 + x^2 + 1$ in $\mathbb{Z}_2$
Hinweis: $x^2 + x + 1$ ist das einzige irreduzible Polynom in $\mathbb{Z}_2$ von Grad 2.

$a(0) = 1$, $a(1) = 1$

Wenn nicht irreduzibel, dann teilt $\underline{x^2 + x + 1}$ $a(x)$. Aber $a(x) = (x^2 + x + 1)q(x)$
dann muss $\deg(q(x)) = 2$ gelten, also $q(x) = x^2 + x + 1$

Wir überprüfen: $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1$
$\quad\quad\quad\quad\quad\quad\quad 1+1=0$
$\quad\quad\quad\quad\quad = x^4 + x^2 + 1 = a(x)$

Faktorisierung

$p(x) \in F[x]_{m(x)}$ Nullteiler $\iff R_{m(x)}(p(x) \cdot q(x)) = 0$, $q(x) \in F[x]_{m(x)} \setminus \{0\}$

$\qquad \iff m(x) \mid p(x) \cdot q(x)$, $\deg(q(x)) < \deg(m(x))$

$\qquad \iff \gcd(m(x), p(x)) > 1$ q kann nicht alle Teiler von m(x) enthalten $\Rightarrow$ p(x) und m(x) haben Teiler gemeinsam

da müsste man noch genauer begründen für ein Beweis

$\rightarrow$ Strategie: wir schauen uns die nicht-konst. Teiler von $m(x)$ an. Alle vielfachen davon sind Nullteiler (da $\gcd(\text{Teiler}, m(x)) > 1$)   raten

$m(x) = x^2 + 2 \Rightarrow m(1) = 0 \Rightarrow x^2 + 2 = (x-1)(x+1) = (x+2)(x+1)$

$\in \mathbb{Z}_3$

alle Elemente haben die Form: $ax + b \Rightarrow 3^2 = 9$ Elemente

$\mathbb{Z}_3[x]_{x^2+2} = \{0, 1, 2, x, \boxed{x+1}, \boxed{x+2}, 2x, \boxed{2x+1}, \boxed{2x+2}\}$

$\rightarrow 1(x+2), 2(x+2)$ und $1(x+1), 2(x+1)$ sind Nullteiler

$\rightarrow$ alles ohne Nullteiler und 0 !

$\mathbb{Z}_3[x]^*_{x^2+2} = \{1, 2, x, 2x\}$

da wäre es schneller zu testen: $x(2x) = \dots$ $(2x)(2x) = \dots$

$2x(ax + b) \equiv_{m(x)} 1$ denke an $a = m \cdot q + r$

$\iff 2x(ax + b) = k(x) \cdot m(x) + 1$

    Grad 2 $\Rightarrow$ k hat Grad 0

$\iff 2x(ax + b) = k(x^2 + 2) + 1$

$\iff 2ax^2 + 2bx = kx^2 + 2k + 1$

$\Rightarrow 2a = k$

$\quad 2bx = 0$

$\quad 2k + 1 = 0$

$\Rightarrow k = 1, b = 0, a = 2$

$\Rightarrow (2x)^{-1} = 2x$
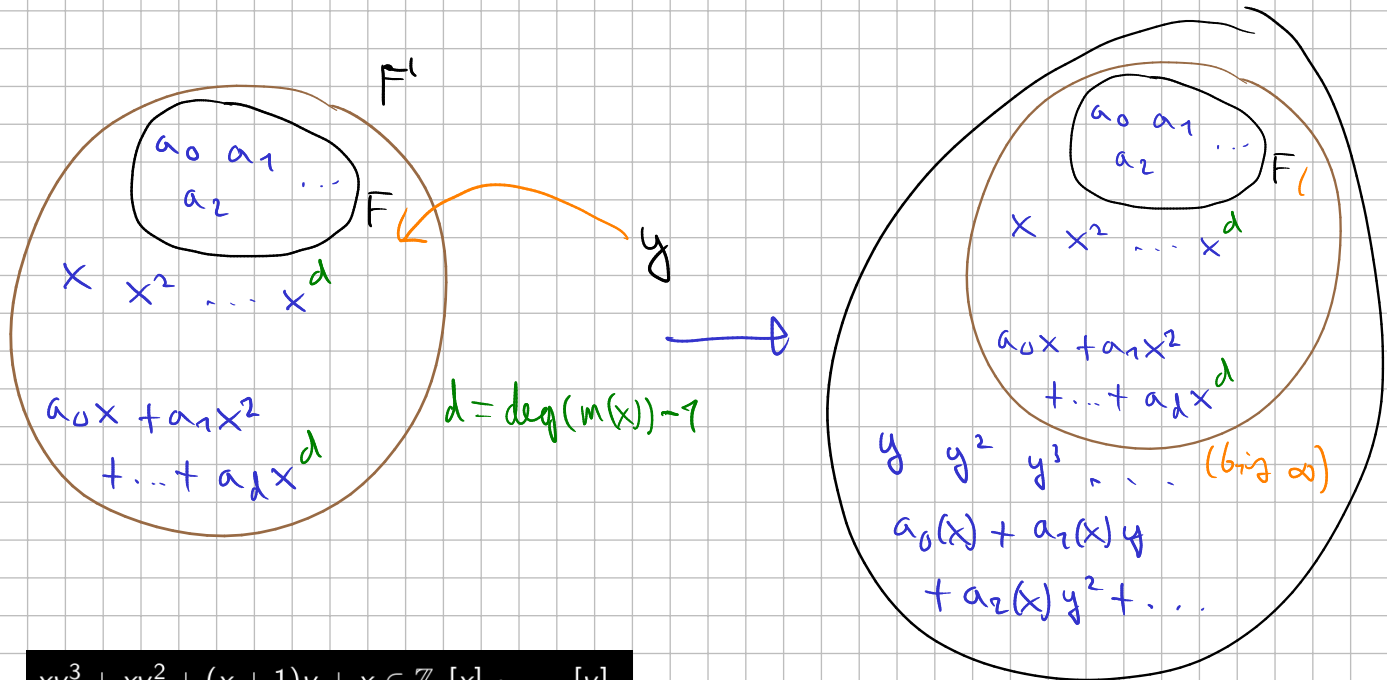
Polynome mit verschachtelten Variablen

Wir haben gesehen:

$F' = F[X]_{m(x)}$ mit $m(x)$ irreduzibel ist ein Körper.

$\Rightarrow$ Wir können wieder Polynome über F' betrachten und bekommen wieder alle Eigenschaften wie Modulorechnen, Nullstellen als Teiler, Faktorisierung in irreduzible Polynome, usw.!

$$F'[y] = F[X]_{m(x)}[y] \qquad\qquad F'[y] = F[X]_{m(x)}[y]$$

$d = \deg(m(x)) - 1$

$a_0 x + a_1 x^2 + \ldots + a_d x^d$

$y \quad y^2 \quad y^3 \quad \ldots \quad (bis \ \infty)$

$a_0(x) + a_1(x)y + a_2(x)y^2 + \ldots$

$xy^3 + xy^2 + (x+1)y + x \in \mathbb{Z}_2[x]_{x^2+x+1}[y].$

Grad $= 3 \Rightarrow$ Wenn es Teiler hat, dann gibt es einen mit Grad 1.

$\Rightarrow$ Nullstellen testen

$\mathbb{Z}_2[x]_{x^2+x+1} = \{0, 1, x, x+1\}$

$a(0) = x \neq 0$, $a(1) = \underbrace{x + x}_{0} + \underbrace{(x+1) + x}_{0} = 1 \neq 0$

$a(x) = x^4 + x^3 + \underbrace{(x+1)x + x}_{0}$

$\quad = x^4 + x^3 + x^2$

$\quad = x^4 + x^3 + x^2 - x^2(x^2 + x + 1) \quad \rightarrow$ subtrahiere vielfaches von $m(x)$ um in $\mathbb{Z}_2[x]_{m(x)}$ zu bleiben

$\quad = 0$

$\Rightarrow y + x \mid a(x)$!

$\Rightarrow$ nicht irreduzibel