Wdh.: Rechnen in $\mathbb{Z}$ modulo n

Für jedes $n \in \mathbb{Z}$ kann man eine Restklasse definieren:

$$\begin{aligned} [a]_n &:= \{x \in \mathbb{Z} \mid a \text{ und } x \text{ haben den gleichen Rest modulo } n\} \\ &= \{x \in \mathbb{Z} \mid \exists t \in Z \text{ so dass } a - x = t \cdot n\} \end{aligned}$$

Bsp.: $[3]_5 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$

Dann gilt:

- Für $a, b \in \{0, 1, \ldots, n-1\}$ mit $a \neq b$: $[a]_n \cap [b]_n = \emptyset$.
- Für alle $a \in Z$ gibt es ein $b \in \{0, 1, \ldots, n-1\}$ mit $[a]_n = [b]_n$.
- Auf der Menge der Restklassen $[a]_n$ kann man eine Addition $+_n$ und eine Multiplikation $\cdot_n$ definieren:

$$\begin{aligned} [a]_n +_n [b]_n &:= [a+b]_n \quad \text{und} \\ [a]_n \cdot_n [b]_n &:= [ab]_n. \end{aligned}$$

- Mit diesen Operationen bildet $\mathbb{Z}/n := \{[a]_n \mid a \in \{0, 1, \ldots, n-1\}\}$ einen Ring.

Beachte: $\boxed{\mathbb{Z}/n \text{ ist isomorph zu } \mathbb{Z}_n \text{ !!!}}$

Jetzt: Rechnen in $K[x]$ modulo eines Polynoms $\pi(x) \in K[x]$

Für jedes $f(x) \in K[x]$ kann man eine Restklasse definieren:

$$\begin{aligned} [f(x)]_\pi \quad &:= \quad \{g(x) \in K[x] \mid f(x) \text{ und } g(x) \text{ haben den gleichen Rest modulo } \pi(x)\} \\ &= \quad \{g(x) \in K[x] \mid \exists t(x) \in K[x] \text{ so dass } f(x) - g(x) = t(x) \cdot \pi(x)\} \end{aligned}$$

Dann gilt:

- Für $f, g \in K[x]$ mit grad$(f) \leq$ grad$(g) <$ grad(π) und $f \neq g$: $[f(x)]_\pi \cap [g(x)]_\pi = \emptyset$.
- Für alle $f \in K[x]$ gibt es ein $g \in K[x]$ mit grad$(g) <$ grad(π) und $[f(x)]_\pi = [g(x)]_\pi$.
- Auf der Menge der Restklassen $[f(x)]_\pi$ kann man eine Addition $+_n$ und eine Multiplikation $\cdot_\pi$ definieren:

$$\begin{aligned} [f(x)]_\pi \; +_\pi \; [g(x)]_\pi \quad &:= \quad [f(x) + g(x)]_\pi \quad \text{und} \\ [f(x)]_\pi \; \cdot_\pi \; [g(x)]_\pi \quad &:= \quad [f(x) \cdot g(x)]_\pi . \end{aligned}$$

- Mit diesen Operationen bildet $K[x]/\pi(x) := \{[f(x)]_\pi \mid f \in K[x], \text{grad}(f) < \text{grad}(\pi)\}$ einen Ring.

$\boxed{\text{Für welche Polynome } \pi(x) \text{ ist } K[x]/\pi(x) \text{ ein Körper?}}$

Wdh.: Wann ist $\mathbb{Z}/n$ ein Körper?

Haben gezeigt: Genau dann wenn n eine Primzahl ist!

Wdh: Eine Zahl $n \in \mathbb{N}$ heißt Primzahl, falls gilt:

$$n = ab \text{ mit } a, b \in \mathbb{N} \qquad \Longrightarrow \qquad (a = 1 \ \vee \ b = 1).$$

$$\boxed{\text{Was entspricht den “Primzahlen” in } K[x]\text{?}}$$

Def.: Ein Polynom $\pi(x) \in K[x]$ heißt **irreduzibel** über $K[x]$, falls gilt:

$$\pi(x) = f(x) \cdot g(x) \text{ mit } f(x), g(x) \in K[x] \qquad \Longrightarrow \qquad (\text{grad}(f) = 0 \ \vee \ \text{grad}(g) = 0).$$

(In anderen Worten: $\pi(x)$ ist genau dann irreduzibel, wenn es kein Polynom $f(x)$ in $K[x]$ gibt, das $\pi(x)$ teilt und dessen Grad mindestens 1 und kleiner als der Grad von $\pi(x)$ ist.)

$\mathbb{Z}_2[x]/(x^4+x^2+1)$	Kurzdarstellung
$[0]$	0000
$[1]$	0001
$[x]$	0010
$[x+1]$	0010
$[x^2]$	0100
$[x^2+1]$	0101
$[x^2+x]$	0110
$[x^2+x+1]$	0111
$[x^3]$	1000
$[x^3+1]$	1001
$[x^3+x]$	1010
$[x^3+x+1]$	1010
$[x^3+x^2]$	1100
$[x^3+x^2+1]$	1101
$[x^3+x^2+x]$	1110
$[x^3+x^2+x+1]$	1111

BEISPIEL:

$$\pi(x) = x^4 + x^2 + 1 \quad \longleftrightarrow \quad \pi = 10101$$

$$a(x) = x^3 + x \quad \longleftrightarrow \quad a = 01010$$

$$b(x) = x^3 + x^2 + 1 \quad \longleftrightarrow \quad b = 01101$$

Berechnung von $a(x) \cdot b(x)$ mod $\pi(x)$:

To do	**Realisierung**	**Ergebnis**
Berechne $a(x) \cdot b_3$	$b_3 = 1$, also $a \cdot b_3 = a$	01010
Multipliziere mit x	Shift nach links	10100
Berechne Rest mod $\pi(x)$	**XOR** mit $\pi = 10101$	00001
Addiere $a(x) \cdot b_2$	$b_2 = 1$, also **XOR** mit $a = 01010$	01011
Multipliziere mit x	Shift nach links	10110
Berechne Rest mod $\pi(x)$	**XOR** mit $\pi = 10101$	00011
Addiere $a(x) \cdot b_1$	$b_1 = 0 \Rightarrow$ Schritt entfällt	
Multipliziere mit x	Shift nach links	00110
Berechne Rest mod $\pi(x)$	führendes Bit = 0 $\Rightarrow$ Schritt entfällt	
Addiere $a(x) \cdot b_0$	$b_0 = 1$, also **XOR** mit $a = 01010$	01100

Ergebnis: $[a(x)] \cdot_\pi [b(x)] = [x^3 + x^2]$.