

## Übung 10

### Nachbesprechung

- Achtet auf eure Darstellung. Die Abgaben müssen einfach verständlich sein

Körper  $\langle R; +, -, 0, \cdot, -1, 1 \rangle$

- $\langle R; +, -, 0 \rangle$  ist abelsche Gruppe
- $\langle R \setminus \{0\}; \cdot, -1, 1 \rangle$  ist abelsche Gruppe
- (Ring:  $\langle R; \cdot, 1 \rangle$  ist monoid)

Jeder Körper ist auch ein Ring

Für jede Primzahl  $p$  ist  $\mathbb{Z}_p$  ein Körper ( $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ )

$GF(p)$  bezeichnet Körper mit  $p$  Elementen

Polynome über einem Körper

$F[x]$  enthält Polynome, wobei Koeffizienten aus  $F$  sind

$a_d \cdot x^d + \dots + a_1 \cdot x + a_0 \in F[x]$  Wenn  $a_d, \dots, a_0 \in F$ . Grad  $d$  ist unbeschränkt

$F[x]$  ist ein Ring und kein Körper!

Thm. Sei  $F$  ein Körper. Für alle  $a(x), b(x)$   $b(x) \neq 0$  über  $F[x]$  existieren eindeutige Polynome  $r(x), q(x) \in F[x]$ , so dass  $a(x) = b(x)q(x) + r(x)$

Aufg. Seien  $a(x) = 2x^3 + x + 1$  und  $b(x) = 2x + 2$ . Finde  $q(x), r(x) \in \mathbb{Z}_3[x]$ , so dass  $a(x) = b(x)q(x) + r(x)$  über  $\mathbb{Z}_3[x]$ .

Polynomdivision:

$$\begin{array}{r} 2x^3 + 0x^2 + x + 1 : 2x + 2 = x^2 + 2x = q(x) \\ - (2x^3 + 2x^2) \\ \hline 0 + 1x^2 + x + 1 \\ 0 - 2 \equiv_3 1 \quad - (1x^2 + x) \\ \hline 2 \cdot 2 \equiv_3 1 \quad 1 = r(x) \end{array}$$

Koeffizienten immer mod 3

Kontrollieren:  $b(x) \cdot q(x) + r(x) = (2x+2)(x^2+2x) + 1 = 2x^3 + x^2 + 2x^2 + x + 1 = a(x) \quad \text{☺}$

## Irreduzible Polynome über $GF(n)$

Def.  $m(x)$  irreduzibel: die einzigen Teiler von  $m(x)$  über  $GF(n)[x]$  sind konst.  $\alpha \in GF(n)$  oder Vielfache von  $m(x)$ , also  $\alpha \cdot m(x)$  für  $\alpha \in GF(n)$ .  
(Für alle  $m(x) \in GF(n)[x]$  gilt  $\alpha | m(x)$  und  $\alpha \cdot m(x) | m(x)$  für alle  $\alpha \in GF(n)$ )

Für allgem.  $m(x) \in GF(n)[x]$  gilt

$m(x)$  ist irreduzibel  $\Rightarrow m(x)$  hat keine NS

$\Leftarrow$  gilt nur falls  $\deg(m(x)) \notin \{2, 3\}$

Polynom  $a(x) \in GF(n)[x]$ . Ist  $a(x)$  irreduzibel?

- $\deg(a(x)) = 1$ : alle irreduzibel
- $\deg(a(x)) \in \{2, 3\}$ : keine NS  $\Leftrightarrow$  irreduzibel
- $\deg(a(x)) = 4$ :
  - $a(x)$  hat NS  $\alpha \Rightarrow (x - \alpha)$  teilt  $a(x)$ , ist reduzibel
  - keine NS  $\Rightarrow a(x)$  ist irreduzibel oder  $a(x) = b(x) \cdot c(x)$  wobei  $b(x), c(x)$  irreduzible Polynome sind mit  $\deg(b(x)) = \deg(c(x)) = 2$

Aufg. Ist  $m(x) = x^2 + 3x + 2$  irreduzibel über  $R = \mathbb{Z}_5[x]$

$m(x)$  ist reduzibel, wenn  $a(x), b(x) \in R$  existieren mit  $\deg(a(x)) = \deg(b(x)) = 1$  und  $a(x) \cdot b(x) = m(x)$  ( $\Rightarrow a(x) | m(x)$ )

Für einen Körper  $F$  und  $\alpha \in F$  gilt:  $a(\alpha) = 0 \Leftrightarrow (x - \alpha) | m(x)$

Also reicht es zu prüfen, ob  $m(x)$  Nullstellen hat

$$m(0) = 2$$

$$m(1) = 1$$

$$\begin{aligned}
 m(2) &= 2 & \Rightarrow m(x) &= \alpha \cdot (x-4)(x-3) = \alpha' \cdot (x+1)(x+2) \\
 m(3) &= 0 & & \text{für ein } \alpha' \in \mathbb{Z}_5 \\
 m(4) &= 0 & \Rightarrow m(x) & \text{ ist reduzibel}
 \end{aligned}$$

Aufg. Zeige, dass  $m(x) = x^5 + x^2 + 1$  irreduzibel ist über  $\text{GF}(2)[X]$ .

1.) Zeige, dass  $m(x)$  keine NS hat

$$m(0) = 1$$

$$m(1) = 1$$

2.) Zeige, dass  $m(x)$  nicht durch ein irreduzibles Polynom mit Grad 2 teilbar ist.  $x^2 + x + 1$  ist das einzige irreduzible Polynom mit Grad 2 über  $\text{GF}(2)$ . Müssen  $x^2 + x + 1 \nmid m(x)$  zeigen mittels Polynomdivision.

$$x^5 + x^2 + 1 : x^2 + x + 1 = x^3 + x^2$$

$$\begin{array}{r}
 - (x^5 + x^4 + x^3) \\
 \hline
 x^4 + x^3 + x^2 + 0 + 1 \\
 - (x^4 + x^3 + x^2) \\
 \hline
 1
 \end{array}$$

1 ← Rest 1 Also gilt  $x^2 + x + 1 \nmid m(x)$

Da  $m(x)$  keinen Faktor von Grad 1 oder Grad 2 hat, ist  $m(x)$  irreduzibel.

Ring  $F[X]_{m(x)}$

$$F[X]_{m(x)} = \{a(x) \in F[X] \mid \deg(a(x)) < \deg(m(x))\}$$

Bsp. Welche Elemente enthält  $\mathbb{Z}_2[X]_{x^2+1}$ ?

Koeffizienten sind 0 oder 1 und alle Polyn. haben Grad  $< 2$ .

$$\mathbb{Z}_2[X]_{x^2+1} = \{0, 1, x, x+1\}, \quad |\mathbb{Z}_2[X]_{x^2+1}| = 2^2 = 4$$

$\mathbb{Z}_2[X]_{x^2+1} = \mathbb{Z}_2[X]_{x^2+x} = \{0, 1, x, x+1\}$ , nur die Operation ist anders

Aufg. Berechne  $x \cdot (x+1)$  in  $\mathbb{Z}_2[X]_{x^2+1}$

$$x(x+1) \equiv_{x^2+1} x^2 + x \equiv_{x^2+1} x^2 + x - (x^2 + 1) \equiv_{x^2+1} x - 1$$

↑  
Grad muss immer  $< 2$  sein

Aufg. Berechne  $(2x+2) \cdot (2x+1)$  in  $\mathbb{Z}_3[X]_{x^2+1}$

$$(2x+2)(2x+1) \equiv_{x^2+1} x^2 + 2x + x + 2 \equiv_{x^2+1} x^2 + 2 - (x^2 + 1) \equiv_{x^2+1} 1$$

↑  
Koeff. mod 3

Aufg. Finde alle Nullteiler in  $R := \mathbb{Z}_2[X]_{x^2+1}$  (Sei  $m(x) := x^2+1$ )

also  $a, b \in R$ , so dass  $a \cdot b = 0$

In  $\mathbb{Z}_n$ , alle  $a \in \mathbb{Z}_n$  mit  $\gcd(a, n) \neq 1$

Hier alle Teiler von  $x^2+1$ . Also müssen wir  $x^2+1$  über  $\mathbb{Z}_2$  faktorisieren

$$m(1) = 0, \text{ also gilt } (x+1) \mid x^2+1 : x^2+1 = (x+1)(x+1)$$

Nullteiler:  $\{x+1\}$

$R^*$  enthält alle  $a \in R$  mit  $\gcd(a, m(x)) = 1$

Also  $R^* = \{1, x\}$

Aufg. Sei  $A = \text{GF}(3)[X]_{x^2+2x+1}$ . Bestimme die Elemente in  $A^*$ .

Da  $x^2+2x+1 = (x+1)^2$ , ist  $\alpha \cdot (x+1) \notin A$  für alle  $\alpha \in \text{GF}(3)$ .

Also  $A = \{1, 2, x, x+2, 2x, 2x+1\}$

Finde einen Generator von  $A$ . Sei  $m(x) = x^2+2x+1$

$|A| = 6$ , also  $\text{ord}(a) \in \{1, 2, 3, 6\}$  für alle  $a \in A$ .

Prüfe, ob  $a^2 \equiv_{m(x)} 1$  oder  $a^3 \equiv_{m(x)} 1$  für  $a \in A$

$$x^2 \equiv_{m(x)} x + 2$$

$$x^3 \equiv_{m(x)} (x+2)x \equiv_{m(x)} x^2 + 2x - m(x) \equiv_{m(x)} 2$$

$$\Rightarrow \text{ord}(x) \notin \{1, 2, 3\}$$

$$\Rightarrow \text{ord}(x) = 6$$

$\Rightarrow x$  ist ein Generator

Aufg. Berechne die Inverse von  $x+4$  in  $R^* := \mathbb{Z}_5[X]_{x^2+1}^*$ .

Jedes Element in  $R^*$  ist von der Form  $ax+b$  für  $a, b \in \mathbb{Z}_5$

Wir wollen  $a$  und  $b$  so wählen, dass  $(x+4)(ax+b) \equiv_{x^2+1} 1$

$$(x+4)(ax+b) = ax^2 + (4a+b)x + 4b \equiv_{x^2+1} ax^2 + (4a+b)x + 4b$$
$$-(ax^2 + a) \equiv_{x^2+1} \underbrace{(4a+b)x}_{=0} + \underbrace{4b-a}_{=1} \equiv_{x^2+1} 1 \quad \text{Ziel}$$

Wir wollen also:

$$\cdot 4a+b \equiv_5 0 \Rightarrow b \equiv_5 -4a \equiv_5 a$$

$$\cdot 4b-a \equiv_5 1 \Rightarrow 3b \overset{\cdot 2}{\equiv_5} 1 \overset{\cdot 2}{\Rightarrow} 6b \equiv_5 b \equiv_5 2$$

Es gilt also  $a=b=2$  und die Inverse ist  $2x+2$

Thm.  $F[x]_{m(x)}$  ist ein Körper  $\Leftrightarrow m(x)$  ist irreduzibel über  $F$

Liste mit irreduziblen Polynomen über  $\text{GF}(p)$ :

$\text{GF}(2)$  : <https://oeis.org/A058943>

$\text{GF}(3)$  : <https://oeis.org/A058944>

$\text{GF}(5)$  : <https://oeis.org/A058945>

$\text{GF}(7)$  : <https://oeis.org/A058946>

Schreibt euch sie auf  
die Zusammenfassung

Aufg. Faktorisiere das Polynom  $a(y) = x \cdot y^3 + x \cdot y^2 + (x+1)y + x$   
 $\in \text{GF}(2)[x]_{x^2+x+1}[y]$  in irreduzible Polynome

Koeffizienten,  $F = \text{GF}(2)_{x^2+x+1}$

$$a(y) = a_d \cdot y^d + \dots + a_1 \cdot y + a_0 \in F[y], \text{ wobei } a_d, \dots, a_0 \in F = \{0, 1, x, x+1\}$$

$\deg(a(y)) = 3$ , also suchen wir Nullstellen

$$a(0) = x$$

$$a(1) = x + x + x + 1 + x = 1$$

$$a(x) = x^4 + x^3 + (x+1)x + x \equiv_{x^2+x+1} x^4 + x^3 + x^2 - x^2(x^2+x+1) \equiv 0$$

$$\Rightarrow (y-x) \text{ teilt } a(x)$$

$$a(\alpha) = 0 \Leftrightarrow (y-\alpha) \mid a(y)$$

Wir können jetzt  $a(x)$  durch  $(y+x)$  teilen

$$\begin{array}{r} x \cdot y^3 + x \cdot y^2 + (x+1) \cdot y + x : y+x = \underline{x \cdot y^2 + y + 1} \\ - (x \cdot y^3 + (x+1) \cdot y^2) \\ \hline 1 \cdot y^2 + (x+1) \cdot y + x \\ - (y^2 + x \cdot y) \\ \hline y + x \quad \text{Rest } 0 \end{array}$$

$$x^2 \equiv_{x^2+x+1} x^2 - (x^2+x+1) \equiv_{x^2+x+1} x+1$$

$$a(y) = (y+x)(\underline{x \cdot y^2 + y + 1})$$

↳ NS überprüfen (hat keine, also ist irreduzibel)