Übungsstunde 10

Nachbesprechung Bonus

- Die * Operation in Ringen ist nicht kommutativ!
- Def. Unit: $u * v = v * u = 1$ für ein $v \in R$
- Es reicht nicht nur $u * v = 1$ oder nur $v * u = 1$ zu zeigen

Let $\langle R; +, -, 0, \cdot, 1 \rangle$ be a ring, and let $a \in R$ and $b \in R$. Prove the following statements:

a) If R is an integral domain and if $a^m = b^m$ and $a^n = b^n$ for some positive integers m and n with $\gcd(m, n) = 1$, then $a = b$.

b) If $1 - ab$ is a unit, then $1 - ba$ is also a unit. *Hint: if* $x = (1 - ab)^{-1}$ *consider the ring element* $1 + bxa$.

Polynome

Polynomdivision - Aufgabe

Wir betrachten Polynome über $\mathbb{Z}_3$.

Ist $x^3 + 2x^2 + x + 2$ durch $2x + 1$ teilbar?

Polynomdivision

Wir betrachten die Polynome über $\mathbb{Z}_5$:

$$(2x^5 + 3x^4 + 2x^3 + 4x + 1) : (3x^3 + x^2 + 4x + 2) = 4x^2 + 3x + 1$$

$-(2x^5 + 4x^4 + x^3 + 3x^2)$

$4x^4 + x^3 + 2x^2 + 4x + 1$

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

$3x^3 + 3x + 1$

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

$4x^2 + 4x + 4$

↳ Hier können wir nicht mehr weitermachen. Somit ist dies unser Rest.

Nebenrechnungen:

$3x^3 \cdot 4x^2 = 2x^5$

$3x^3 \cdot 3x = 4x^4$

$3x^3 \cdot 1 = 3x^3$

Es gilt $2x^5 + 3x^4 + 2x^3 + 4x + 1 = (3x^3 + x^2 + 4x + 2)(4x^2 + 3x + 1) + 4x^2 + 4x + 4$.

Aufgabe

Um zu bestimmen, ob $x^3 + 2x^2 + x + 2$ durch $2x + 1$ teilbar ist, führen wir eine Polynomdivision durch:

$$(x^3 + 2x^2 + x + 2) : (2x + 1) = 2x^2 + 2$$

$-(x^3 + 2x^2)$

$0 + x + 2$

$-(x + 2)$

0

Somit ist $x^3 + 2x^2 + x + 2$ durch $2x + 1$ teilbar.

Irreduzible Polynome

Definition 5.28. A polynomial $a(x) \in F[x]$ with degree at least 1 is called *irreducible* if it is divisible only by constant polynomials and by constant multiples of $a(x)$.

- Polynome von Grad 1: immer irreduzibel
- Polynome von Grad 2&3: irreduzibel genau dann wenn keine Nullstellen (Korollar 5.30)
- Polynome von Grad 4:
  - Polynom hat Nullstelle: nicht irreduzibel
  - Polynom hat keine Nullstelle: irreduzibel wenn nicht teilbar durch alle irreduziblen Polynome von Grad 2
- ...

Aufgabe

Sind die folgenden Polynome über $GF(2)$ irreduzibel?

- $a(x) = x + 1$
- $b(x) = x^2 + 1$
- $c(x) = x^4 + x + 1$

Irreduzible Polynome

$a(x) = x + 1$: irreduzibel (Polynome mit Grad 1 sind immer reduzibel)

$b(x) = x^2 + 1$:

Wir suchen nach Nullstellen:

$b(0) = 1$

$b(1) = 0$

Somit ist 1 eine Nullstelle. Somit ist $x^2 + x$ durch $(x-1) \equiv_2 (x+1)$ teilbar und somit nicht irreduzibel.

$c(x) = x^4 + x + 1$

Wir suchen nach Nullstellen:

$c(0) = 1$

$c(1) = 1 + 1 + 1 \equiv_2 1$

$c(x)$ hat also keine Nullstellen. Wir müssen nun prüfen, ob $c(x) = p(x)q(x)$ für zwei irreduzible Polynome p, q vom Grad 2 gilt.
Mit Grad 2 gibt es nur ein irreduzibles Polynom über $GF(2)$: $x^2 + x + 1$

$$
\begin{array}{l}
x^4 + \quad x + 1 : x^2 + x + 1 = x^2 + x \\
\underline{-(x^4 + x^3 + x^2)} \\
\quad x^3 + x^2 + x \\
\quad \underline{-(x^3 + x^2 + x)} \\
\qquad\quad 0 + 1
\end{array}
$$

Somit ist $x^4 + x + 1$ nicht durch $x^2 + x + 1$ teilbar.
Daraus folgt, dass $c(x)$ irreduzibel ist.

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

$F[x]_{m(x)} = \{a(x) \in F[x] | \deg(a(x)) < \deg(m(x))\}$ ist ein Ring.

F ist ein Körper, $m(x)$ ist ein Polynom über F

Theorem 5.37: $F[x]_{m(x)}$ ist ein Körper $\Leftrightarrow$ $m(x)$ ist irreduzibel

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

Beispiel: $\mathbb{Z}_3[x]_{2x^2+x+1}$ ($\mathbb{Z}_3$ ist ein Körper, da 3 prim)

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

Rechnen in $\mathbb{Z}_5[x]_{2x^2+3x+1}$:

Addition: immer mod 5

$$(3x+1)+(3x+4) = 6x+5 \equiv_5 x$$

Multiplikation: immer mod $2x^2+3x+1$ und mod 5:

$$(3x+1)(3x+4) = 4x^2+2x+3x+4 \equiv_5 4x^2+4 \equiv_{2x^2+3x+1} 4x^2+4-2(2x^2+3x+1) \equiv_{2x^2+3x+1} -6x+2 \equiv_{2x^2+3x+1} 4x+2$$

$$(2x+2)(x+1) \equiv_{2x^2+3x+1} 2x^2+4x+2 \equiv_{2x^2+3x+1} x+1$$

Aufgabe

10.5 Extension Fields ($\star$) ***(8 Points)***

Let $F = \mathbb{Z}_5[x]_{x^2+4x+1}$.

a) Prove that F is a field.

b) Prove that $F^* = \langle x + 3 \rangle$. Show your work.

c) Write $a(y) = (2x+3)y^2 + (2x+1)y + 1 \in F[y]$ as a product of irreducible polynomials.
Hint: $2x + 1 \equiv_{x^2+4x+1} 2(x + 3)$ in $\mathbb{Z}_5[x]$.

Aufgabe

a) Wir müssen zeigen, dass $m(x) = x^2+4x+1$ irreduzibel ist. Dafür suchen wir nach Nullstellen.

$m(0) = 1$

$m(1) = 1+4+1 \equiv_5 1$

$m(2) = 4+3+1 \equiv_5 3$

$m(3) = 4+2+1 \equiv_5 2$

$m(4) = 1+1+1 \equiv_5 3$

$m(x)$ hat also keine Nullstellen. Nach Kor. 5.30 ist $m(x)$ also irreduzibel und somit ist $\mathbb{Z}_5[x]_{x^2+4x+1}$ nach Theorem 5.37 ein Körper.

b) Wir müssen zeigen, dass $x+3$ ein Generator von F^* ist. Nach Lemma 5.34. gilt $|F| = 5^2 = 25$. Da $F^* = F \setminus \{0\}$, gilt $|F^*| = 25-1 = 24$. Somit $ord(x+3) \in \{1,2,3,4,6,8,12,24\}$, da die Ordnung jedes Elements die Gruppenordnung teilen muss.
Wir müssen zeigen, dass $ord(x+3) = 24$.

$x+3 \equiv_{x^2+4x+1} x+3$

$(x+3)^2 = x^2+6x+9 \equiv_{x^2+4x+1} 2x+8 \equiv_5 2x+3$

$(x+3)^3 = (2x+3)(x+3) = 2x^2+9x+9 \equiv_{x^2+4x+1} x+7 \equiv_5 x+2$

$(x+3)^4 = (x+2)(x+3) = x^2+5x+6 \equiv_{x^2+4x+1} x+5 \equiv_5 x$

$(x+3)^6 = ((x+3)^3)^2 = (x+2)^2 = x^2+4x+4 \equiv_{x^2+4x+1} 3$

$(x+3)^8 = ((x+3)^4)^2 = x^2 \equiv_{x^2+4x+1} x+4$

$(x+3)^{12} = (3)^2 = 9 \equiv_5 4$

Da $ord(x+3) \notin \{1,2,3,4,6,8,12\}$, muss gelten $ord(x+3) = 24$. Somit ist $x+3$ ein Generator von F^* und es gilt $F^* = \langle x+3 \rangle$

c) Wir betrachten nun $\mathbb{Z}_5[x]_{x^2+4x+1}[y]$

$a(y) \equiv_{x^2+4x+1} \overbrace{(2x+3)}^{a^2} y^2 + 2\overbrace{(x+3)}^{a} y + \overbrace{1}^{1}$ → Binomische Formel: $(ay+b)^2 = a^2y^2 + 2aby + b$

bzw. $(ay+1)^2 = a^2y^2 + 2ay + 1$

$(x+3)^2 = x^2 + 6x + 9 \equiv_{x^2+4x+1} 2x + 8 \equiv_5 2x + 3$

Somit gilt $a(y) = ((x+3)y+1)^2$, $(x+3)y+1$ ist irreduzibel, da es Grad 1 hat.

Nullteiler und Einheiten in $F[x]_{m(x)}$

- Nullteiler: Alle Elemente, die einen gemeinsamen Faktor mit m(x) haben
- Einheiten: Alle Elemente, die keinen gemeinsamen Faktor mit m(x) haben

$F[x]_{n(x)}[y]$

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

$a(y) = (x+1)y^3 + xy^2 + y + (x+1)$

Nullstellen bestimmen:

$a(0) = x+1$

$a(1) = (x+1) + x + 1 + x + 1 \equiv_2 x+1$

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

Somit ist x eine Nullstelle.

Aufgabe

Finde alle Nullteiler und Einheiten in $GF(5)[x]_{2x^2+x}$.

Einheiten und Nullteiler

Wir faktorisieren erst $2x^2+x$. In diesem Fall ist das einfach $2x^2+x = x\cdot(2x+1)$.
Nun sind die Nullteiler alle Elemente, die einen gemeinsamen Faktor mit $2x^2+x$ haben, also x oder $(2x+1)$. Da wir nur Polynome von Grad 1 in $GF(5)[x]_{2x^2+x}$ haben, sind dies die konstanten Vielfachen.

Vielfache von x:
- x
- $2x$
- $3x$
- $4x$

Vielfache von $2x+1$:
- $2x+1$
- $2(2x+1) = 4x+2$
- $3(2x+1) \equiv_5 x+3$
- $4(2x+1) \equiv_5 3x+4$

Also sind alle Nullteiler $N = \{x, 2x, 3x, 4x, 2x+1, 4x+2, x+3, 3x+4\}$.
Da wir in einem endlichen Ring sind, sind die Einheiten alle restlichen Elemente bis auf die Null:
$E = GF(5)[x]_{2x^2+x} \setminus (N \cup \{0\})$

Aufgabe

Finde die multiplikative Inverse von $3x + 1$ in $GF(5)_{2x^2+x}$.

Aufgabe

Da wir nur Polynome vom Grad 1 haben, suchen wir ein $ax+b$ mit $a,b \in GF(5)$, sodass

$$(ax+b)\cdot(3x+1) \equiv_{2x^2+x} 1$$

$$\Leftrightarrow \quad 3ax^2 + ax + 3bx + b \equiv_{2x^2+x} 1$$

$$\Leftrightarrow \quad 3ax^2 + (a+3b)x + b - 4a\cdot(2x^2+x) \equiv_{2x^2+x} 1$$

$$\Leftrightarrow \quad (a+3b)x + b - 4ax \equiv_5 (2a+3b)x + b \equiv_{2x^2+x} 1$$

Wir machen nun ein Koeffizientenvergleich:

$$2a + 3b \equiv_5 0$$
$$b = 1$$

$$2a + 3 \equiv_5 0$$

$$\Leftrightarrow \quad 2a \equiv_5 -3 \equiv_5 2$$
$$a = 1$$

Somit ist unsere multiplikative Inverse $x+1$. Wir können dies überprüfen:

$$(x+1)(3x+1) = 3x^2 + 4x + 1 \equiv_{2x^2+x} 3x^2 + 4x + 1 + 2x^2 + x \equiv_5 1 \quad \checkmark$$