

- Agenda:
- ✓ Polynomringe
  - ✓ Restklassenringe
  - ✓ Körper
  - ✓ Restklassenkörper
  - ✓ Körper komplexer Zahlen (nach der Analyse behandelt).

## 2.2.2. Polynomring in einer Unbestimmten

Sei  $R$  ein Ring und  $x$  eine Unbestimmte  
(d.h. ein Symbol bzw. eine formale Variable)

Als  $R[x]$  bezeichnen wir die Menge aller  
der Ausdrücke der Form

$$f = \sum_{i=0}^{\infty} c_i x^i$$

bei denen die Werte  $c_i$  ( $i \in \mathbb{N}_0$ ) zu  $R$  gehören  
und  $\{i \in \mathbb{N}_0 : c_i \neq 0\}$  eine endliche Menge ist.

Bsp

$$f = x^2 - 3x + 2 \in \mathbb{Z}[x]$$

$$c_0 = 2 \in \mathbb{Z}$$

$$c_1 = -3 \in \mathbb{Z}$$

$$c_2 = 1 \in \mathbb{Z}$$

$$c_3 = c_4 = c_5 = \dots = 0$$

$$\{i \in \mathbb{N}_0 : c_i \neq 0\} = \{0, 1, 2\}$$

$\deg(f) = \max \{i \in \mathbb{N}_0 : c_i \neq 0\}$  heißt Grad von  $f$

$x^i$  heißt Monom vom Grad  $i$

$c_i \cdot x^i$  mit  $c_i \neq 0$  der Term vom Grad  $i$ .

$c_i$  heißt der Koeffizient vom Monom/Term

$x^i$  bzw.  $c_i \cdot x^i$

Das Polynom, dessen alle Koeffizienten gleich Null sind,  
heißt das Nullpolynom, dieses Polynom hat Grad  $-\infty$ .

$R$  wird als Teilmenge von  $R[x]$  aufgefasst, insb. Elemente von  $R$  los ohne Polynome vom Grad 0. Auf  $R[x]$  werden + und  $\cdot$  wie folgt eingeführt:

$$\sum_{i=0}^{\infty} c_i x^i + \sum_{i=0}^{\infty} d_i x^i := \sum_{i=0}^{\infty} (c_i + d_i) x^i$$

$$\left( \sum_{i=0}^{\infty} c_i x^i \right) \cdot \left( \sum_{j=0}^{\infty} d_j x^j \right) := \sum_{i+j \in \mathbb{N}_0} c_i d_j x^{i+j}$$

$$= \sum_{k=0}^{\infty} \left( \sum_{i=0}^k c_i d_{k-i} \right) x^k$$

Die Gleichheit von Polynomen ist durch Koeffizientenvergleich definiert.

**Proposition** Für einen Ring  $R$  ist  $(R[x], +, \cdot)$  ebenfalls ein Ring.

**Bemerkung** Polynome aus  $R[x]$  lassen sich auswerten, indem man für  $x$  ein festes Objekt einsetzt, z.B. ein Element aus  $R$  oder ein anderes Polynom oder weitere Objekte.

**Bsp.**  $f(x) = x^2 - 3x + 2$

$$\begin{aligned} f(x-1) &= (x-1)^2 - 3(x-1) + 2 \\ &= x^2 - 2x + 1 - 3x + 3 + 2 \\ &= x^2 - 5x + 6 \end{aligned}$$

$$\begin{aligned} f(x+1) &= (x+1)^2 - 3(x+1) + 2 \\ &= x^2 + 2x + 1 - 3x - 3 + 2 \\ &= x^2 - x = x \cdot (x-1) \end{aligned}$$

$$\Rightarrow f(x) = f((x-1)+1) = (x-1)(x-1-1) \\ = (x-1) \cdot (x-2)$$

**Def** Ist  $R$  Ring,  $a \in R$  und  $f \in R[x]$   
so heißt  $a$  Nullstelle von  $f$ , wenn  
 $f(a) = 0$  ist.

**Bsp** Sei  $u(t)$  Funktion in der Zeit  $t$ ,  
(beliebig oft differenzierbar) und sei  
 $\frac{d}{dt}$  die Ableitung nach der Zeit.

Wir können das Polynom

$$f(x) = x^2 - 3x + 2 \text{ und } \frac{d}{dt} \text{ auswerten:}$$

$$f\left(\frac{d}{dt}\right) = \left(\frac{d}{dt}\right)^2 - 3 \cdot \left(\frac{d}{dt}\right) + 2 \cdot id \quad \leftarrow \begin{array}{l} \text{Differenzial-} \\ \text{operator} \\ \text{der man} \\ \text{zu Funktionen} \\ \text{anwenden kann.} \end{array}$$

$$f\left(\frac{d}{dt}\right)u = \left(\frac{d}{dt}\right)^2 u - 3 \frac{d}{dt} u + 2u = u'' - 3u' + 2u$$

$$f\left(\frac{d}{dt}\right) = \left(\frac{d}{dt} - id\right) \cdot \left(\frac{d}{dt} - 2 \cdot id\right)$$

$$\left(\frac{d}{dt} - 2id\right)u = u' - 2u$$

$$\begin{aligned} \left(\frac{d}{dt} - id\right) \left(\frac{d}{dt} - 2id\right)u &= \left(\frac{d}{dt} - id\right)(u' - 2u) \\ &= (u' - 2u)' - (u' - 2u) \\ &= u'' - 2u' - u' + 2u \\ &= u'' - 3u' + 2u \end{aligned}$$

**Proposition** Sei  $R$  Ring und  $f \in R[x]$  fkt.

Sei  $a \in R$  Nullstelle von  $f$ . Dann lässt sich  $f$  in eindeutiger Weise als

$$f(x) = (x-a) \cdot g(x) \text{ mit } g \in R[x].$$

**Beweis:** Ist  $a$  Nullstelle von  $f(x)$  so ist  
 $0$  eine Nullstelle von  $f(x+a) \in R[x]$

D.h.  $f(x+a) = c_0 + c_1 x + c_2 x^2 + \dots$ ,  
wobei  $c_0 = 0$  ist.

D.h.  $f(x+a) = c_1 x + c_2 x^2 + \dots$   
=  $x \cdot (c_1 + c_2 x + c_3 x^2 + \dots)$   
=  $x \cdot h(x)$  mit

$$h(x) = c_1 + c_2 x + c_3 x^2 + \dots$$

Durch Einsetzen von  $x-a$  an der Stelle von  $x$  in der Gleichung  $f(x+a) = x \cdot h(x)$  erhalten wir  $f(x) = (x-a) \cdot h(x-a)$ , sodass wir  $g(x) = h(x-a)$  festlegen können.

Wir zeigen nun die Eindeutigkeit von  $g(x)$ .

Seien  $g, \tilde{g} \in R[x]$  Polynome mit

$$f(x) = (x-a) \cdot g(x) = (x-a) \cdot \tilde{g}(x).$$

Das Einsetzen von  $x+a$  an der Stelle von  $x$  ergibt

$$x \cdot g(x+a) = x \cdot \tilde{g}(x+a)$$

Seien  $g(x+a) = s_0 + s_1 x + s_2 x^2 + \dots$   
 $\tilde{g}(x+a) = \tilde{s}_0 + \tilde{s}_1 x + \tilde{s}_2 x^2 + \dots$

 $\Rightarrow s_0 \cdot x + s_1 x^2 + s_2 x^3 + \dots = \tilde{s}_0 \cdot x + \tilde{s}_1 x^2 + \tilde{s}_2 x^3 + \dots$ 
 $\Rightarrow s_0 = \tilde{s}_0, s_1 = \tilde{s}_1, s_2 = \tilde{s}_2, \dots$ 
 $\Rightarrow g(x+a) = \tilde{g}(x+a)$ 

Das Einsetzen von  $x-a$  an der Stelle von  $x$  ergibt  $g(x) = \tilde{g}(x)$ .  $\square$

**Bemerkung** Wir können das  $g$  mit

$f(x) = (x-a) \cdot g(x)$  finden, indem wir das Polynom  $g(x)$  teilen (mit Rest).

**Bsp**  $f = x^3 - 5x^2 + 7x - 2$

$$a = 2$$

$$x^3 - 5x^2 + 7x - 2 : x-2 = x^2 - 3x + 1$$

$$\begin{array}{r} x^3 - 5x^2 + 7x - 2 \\ - (x^3 - 2x^2) \\ \hline -3x^2 + 7x - 2 \\ - (-3x^2 + 6x) \\ \hline x - 2 \\ - (x - 2) \\ \hline 0 \end{array} \Rightarrow$$

$$f(x) = (x-2) \cdot (x^2 - 3x + 1).$$

### 2.2.3. Restklassenregel

Neben der Addition in  $\mathbb{Z}_m$ , die bereits eingeführt worden ist, wird nun in  $\mathbb{Z}_m$  auch eine Multiplikation eingeführt.

Proposition. Sei  $m \in \mathbb{N}$  und seien

$a, b \in \mathbb{Z}_m$  Restklassen. Dann existiert eine eindeutige Restklasse  $c \in \mathbb{Z}_m$  derart, dass  $a \cdot b \in c$  für alle Vertreter  $a \in A$  und  $b \in B$  gilt.

Beweis: Man setzt  $c = [a \cdot b]_m$  und zeigt, dass  $c$  nicht von der von  $a \in A$  und  $b \in B$  abhängig ist. D.h. wenn man die Vertreter anders wählen würde, würde sich  $c$  nicht ändern. Details: Übungsaufgabe. □

$$(\mathbb{Z}_m, +, \cdot)$$