

13. Vorlesung

- Rückblick: Übersicht zu Ringen R
- Standardbeispiel: Polynomringe $R[x]$
- Polynomringe $K[x]$ (K Körper) sind EUKLIDISCHE RINGE
 - Gibt es einen größten gemeinsamen Teiler von Elementen a, b eines Ringes?
 - Kann man in Ringen den EUKLIDISCHEN Algorithmus anwenden?
- Anwendung: Zyklische Polynomcodes

Übersicht zu Ringen

	Ring	\cdot komm.	Einsel. 1 existiert	keine Nullteiler	a^{-1} ex. für alle $a \neq 0$
Ring	×				
komm. Ring	×	×			
Integritätsring	×	×	×	×	
Körper	×	×	×	×	×

- Integritätsring \mathbb{Z} :
Nur $1, -1$ besitzen multiplikative Inverse.
- Integritätsring $\mathbb{Z}[i]$:
Nur $1, -1, i, -i$ besitzen multiplikative Inverse.
- Integritätsring \mathbb{Z}_p (p prim):
Jedes Element $a \neq 0$ besitzt ein multiplikatives Inverses.

Polynome über Ringen

Sei $(R, +, \cdot)$ ein Ring.

- $R[x]$ bezeichnet die Menge aller Polynome in der Unbestimmten x mit Koeffizienten aus R :

$$R[x] := \underbrace{\{a_0 + a_1x + \cdots + a_mx^m + \dots \mid a_i \in R \text{ für alle } i\}}_{\text{endlich viele Summanden}}$$

- Addition von Polynomen

$$\begin{aligned} a(x) \oplus b(x) &= (a_0 + a_1x + \cdots + a_mx^m) \oplus (b_0 + b_1x + \cdots + b_mx^m) \\ &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m \end{aligned}$$

- Multiplikation von Polynomen

$$\begin{aligned} a(x) \odot b(x) &= (a_0 + a_1x + \cdots + a_mx^m) \odot (b_0 + b_1x + \cdots + b_mx^m) \\ &= (a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1)x + \cdots + \left(\sum_{i=0}^k a_i \cdot b_{k-i} \right) x^k + \dots \end{aligned}$$

Polynomringe

- Sei $(R, +, \cdot)$ ein Ring. Dann ist $(R[x], \oplus, \odot)$ ein Ring.
- Sei $(R, +, \cdot)$ ein Integritätsring.
Dann ist $(R[x], \oplus, \odot)$ ein Integritätsring.

Polynomringe $K[x]$ über einem Körper K sind spezielle Integritätsringe, nämlich

EUKLIDISCHE RINGE.

Im Weiteren benutzen wir dann aber nicht die Definition solcher Ringe, sondern eine (einfacher verständliche) Charakterisierung (als Ringe, in denen man jeden größten gemeinsamen Teiler $\text{ggT}(a, b)$ mit $(a, b) \neq (0, 0)$ mit Hilfe des EUKLIDISCHEN Algorithmus berechnen kann).

Größter gemeinsamer Teiler

- Ein Element d eines Integritätsringes R heißt ein größter gemeinsamer Teiler (ggT) von Elementen $a_1, a_2, \dots, a_n \in R$
(Schreibweise: $\text{ggT}(a_1, a_2, \dots, a_n) \cong d$),
wenn gilt:
 - (1) $d|a_1, d|a_2, \dots, d|a_n$
 - (2) Aus $t|a_i$ ($i = 1, 2, \dots, n$) folgt $t|d$ für alle $t \in R$.
- Es gilt $\text{ggT}(a_1, a_2, \dots, a_n) = \text{ggT}(\text{ggT}(a_1, a_2, \dots, a_{n-1}), a_n)$.
- Zu je zwei Elementen a_1, a_2 mit $(a_1, a_2) \neq (0, 0)$ eines EUKLIDISCHEN Ringes R existiert ein größter gemeinsamer Teiler und jeder größte gemeinsame Teiler von a_1 und a_2 lässt sich als Linearkombination von a_1 und a_2 mit Koeffizienten aus R darstellen.

Polynomringe über Körpern

- Polynomdivision:

Sei $K[x]$ ein Polynomring über einem Körper K .

Sind $a(x)$ und $b(x)$ Polynome aus $K[x]$ mit $a(x) \neq 0$, dann gibt es eindeutig bestimmte Polynome $q(x), r(x) \in K[x]$ mit $b(x) = q(x)a(x) + r(x)$ und $r(x) = 0$ oder $\text{Grad}(r(x)) < \text{Grad}(a(x))$.

- Sei $K[x]$ ein Polynomring über einem Körper K .
Dann ist $K[x]$ ein EUKLIDISCHER Ring.
- Den größten gemeinsamen Teiler zweier Polynome kann man mit dem EUKLIDISCHEN Algorithmus berechnen.

Zyklische Polynomcodes

- $K[x]_n = \underbrace{\{a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} \mid a_i \in K \text{ für } i = 0, \dots, n-1\}}_{a(x)}$

bezeichnet die Menge aller Polynome in der Unbestimmten x vom Grad $< n$ mit Koeffizienten aus K , wobei K ein endlicher Körper ist.

- Codewörter aus $K^n \iff$ Codewörter aus $K[x]_n$
 $c_0c_1 \dots c_{n-1} \iff c(x) := c_0 + c_1x + \dots + c_{n-1}x^{n-1}$
 $c_{n-1}c_0c_1 \dots c_{n-2} \iff \underbrace{c_{n-1} + c_0x + c_1x^2 + \dots + c_{n-2}x^{n-1}}_{= x \cdot c(x) \pmod{x^n - 1}}$

- Ein (n, k) -Linearcode \mathcal{C} über einem Körper K ist genau dann zyklisch, wenn für alle $c(x) \in \mathcal{C}$ gilt:

$$c(x) \in \mathcal{C} \quad \Rightarrow \quad x \cdot c(x) \pmod{x^n - 1} \in \mathcal{C}$$

Bezeichnung: \mathcal{C} wird zyklischer Polynomcode genannt.