Algebra für Informationssystemtechniker

Prof. Dr. Ulrike Baumann

Fachrichtung Mathematik

Institut für Algebra

www.math.tu-dresden.de/∼baumann

Ulrike.Baumann@tu-dresden.de

02.07.2018

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?
- Rechnen im Ring $(K[x]/f(x), \oplus, \otimes)$
- Ergänzung: Anwendung bei zyklischen Polynomcodes

Übersicht zu Ringen

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

- 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:

$$R[x] := \{\underbrace{a_0 + a_1 x + \cdots + a_m x^m + \ldots}_{\text{endlich viele Summanden}} \mid a_i \in R \text{ für alle } i\}$$

- Addition von Polynomen

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

- Multiplikation von Polynomen

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

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 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 $a_1, a_2, \ldots, a_n \in R$ (Schreibweise: $\mathrm{ggT}(a_1, a_2, \ldots, a_n) \cong d$),
  wenn gilt:

  (1) $d|a_1,\ d|a_2,\ \ldots,\ d|a_n$

  (2) Aus $t|a_i$ $(i = 1, 2, \ldots, n)$ folgt $t|d$ für alle $t \in R$.

- Es gilt $\mathrm{ggT}(a_1, a_2, \ldots, a_n) = \mathrm{ggT}(\mathrm{ggT}(a_1, a_2, \ldots, a_{n-1}), a_n)$.

- 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.

- Man kann modulo eines Polynoms rechnen.

Konstruktion von Ringen

Ring der ganzen Zahlen	Polynomring über einem Körper K
$\mathbb{Z}$	$K[x]$
$\downarrow$ *Rechnen modulo n*	$\downarrow$ *Rechnen modulo* $p(x)$
$\mathbb{Z}_n$	$K[x]/p(x)$
Restklassenring modulo n	Polynomring modulo $p(x)$

Rechnen im Ring $(K[x]/f(x); \oplus, \otimes)$

Sei K ein endlicher Körper und $f(x) \in K[x]$ mit $\text{Grad}(f(x)) = n$.

$$\begin{aligned} K[x]/f(x) &:= \{r(x) \in K[x] \mid r(x) = 0 \text{ oder } \text{Grad}(r(x)) < n\} \\ &= \{r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} \mid r_i \in K \text{ für } i = 0, ..., n-1\} \end{aligned}$$

- Addition $\oplus$:

$$\begin{aligned} a(x) \oplus b(x) &= (a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) \oplus (b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}) \\ &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_{n-1} + b_{n-1}) x^{n-1} \end{aligned}$$

- Multiplikation $\otimes$:

$$\begin{aligned} a(x) \otimes b(x) &= a(x) \odot b(x) \pmod{f(x)} \\ &= \cdots + \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) x^k + \ldots \pmod{f(x)} \end{aligned}$$

Ergänzung: Zyklische Polynomcodes

- $K[x]_n = \{\underbrace{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}}_{a(x)} \mid a_i \in K \text{ für } i = 0, \ldots, n-1\}$

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

- $$\begin{aligned} \text{Codewörter aus } K^n \quad &\leftrightsquigarrow \quad \text{Codewörter aus } K[x]_n \\ c_0 c_1 \ldots c_{n-1} \quad &\leftrightsquigarrow \quad c(x) := c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \\ c_{n-1} c_0 c_1 \ldots c_{n-2} \quad &\leftrightsquigarrow \quad \underbrace{c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}}_{= x \cdot c(x) \pmod{x^n - 1}} \end{aligned}$$

- 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.