WS 2014/15

Diskrete Strukturen

Kapitel 5: Algebraische Strukturen (Endliche Körper)

Hans-Joachim Bungartz

Lehrstuhl für wissenschaftliches Rechnen
Fakultät für Informatik
Technische Universität München

http://www5.in.tum.de/wiki/index.php/Diskrete_Strukturen_-_Winter_14

- Algebraische Strukturen
  - Grundlagen
  - Gruppen
  - Endliche Körper

- Ringe und Körper:

  Definition: Eine Algebra $\langle S, \oplus, \odot \rangle$ mit zweistelligen Operatoren $\oplus$ und $\odot$ heißt Ring, falls gilt:

  (1) $\langle S, \oplus \rangle$ ist eine abelsche Gruppe.

  (2) $\langle S, \odot \rangle$ ist ein Monoid.

  (3) Die Distributivgesetze gelten:

  - $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$,
  - $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$.

- Ringe und Körper:

  Definition: Eine Algebra $\langle S, \oplus, \odot \rangle$ mit zweistelligen Operatoren $\oplus$ und $\odot$ heißt Körper, falls

  (1) $\langle S, \oplus \rangle$ ist eine abelsche Gruppe mit neutralem Element **0**.

  (2) $\langle S \setminus \{\mathbf{0}\}, \odot \rangle$ ist eine abelsche Gruppe.

  (3) Das Linksdistributivgesetz gilt:

  $$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

  (das Rechtsdistributivgesetz folgt aus den übrigen Eigenschaften.)

- Ringe und Körper:

  Beispiele:

  - $\langle \mathbb{Z}, +, * \rangle$ ist Ring.
  - $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist Ring für alle $n \geq 1$.
  - $\langle \mathbb{Q}, +, * \rangle$ und $\langle \mathbb{R}, +, * \rangle$ sind Körper.
  - $\langle \mathbb{Z}_3, +_3, *_3 \rangle$ ist Körper.

- Ringe und Körper:

  Beispiel: Ein Körper mit vier Elementen.

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\otimes$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

- Zahlenkörper:

  Satz: Für alle $n \geq 2$:

  $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist ein Körper gdw. n ist eine Primzahl.

  Beweis: Für alle $n \geq 2$ erfüllt $\langle \mathbb{Z}_n, +_n, *_n \rangle$ alle Eigenschaften eines Körpers bis auf die Existenz von multiplikativen Inversen in $\langle \mathbb{Z}_n \setminus \{0\}, *_n \rangle$.

  Diese existieren g.d.w. n eine Primzahl ist.

- Polynomkörper:
  - Die Elemente des Körpers sind nicht mehr Zahlen, sondern Polynome.
  - Wir erweitern die Begriffe Summe, Produkt, Division, Rest, Modulo und Primzahl auf Polynome.
  - Wir führen dann einen zweiten Satz über die Existenz endlicher Körper ein.

- Polynome:

  Definition: Sei $\langle K, +, \cdot \rangle$ ein (kommutativer) Ring. Ein Polynom über K in der Variablen x ist ein Ausdruck der Gestalt

  $$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0,$$

  wobei $n \in \mathbb{N}_0$, $a_i \in K$ und $a_n \neq 0$.

  Der Grad des Polynoms ist n und seine Koeffizienten sind $a_0, \ldots, a_n$.

  $K[x]$ bezeichnet die Menge der Polynome über dem Ring K in der Variablen x.

- Polynome:

  Definition: Ein Polynom

  $$p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$$

  induziert eine Funktion $f_p: K \to K$ definiert durch

  $$f_p(b) = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \cdots + a_1 \cdot b + a_0$$

  für alle $b \in K$.

  Zwei Polynome sind gleich, wenn sie den gleichen Grad und die gleichen Koeffizienten haben.

  (Zu beachten: Verschiedene Polynome können dieselbe Funktion induzieren.)

- Polynome:
  - In praktischen Anwendungen gilt $K = \mathbb{Z}$ oder $\mathrm{K} = \mathbb{Z}_n$.
  - $p(x) = 0$ hat Grad $-\infty$.
  - Formal kann das Polynom

$$p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$$

auch mit der Folge $(a_0, \ldots, a_n)$ gleichgesetzt werden.

- Operationen auf Polynomen:
  - Seien zwei Polynome gegeben:

$$a(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$b(x) = b_n x^n + \cdots + b_1 x + b_0.$$

  - Die Summe $(a + b)(x)$ ist das Polynom

$$(a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

  - Die Differenz $(a - b)(x)$ ist das Polynom

$$(a_n - b_n)x^n + \cdots + (a_1 - b_1)x + (a_0 - b_0),$$

    wobei $-b_i$ das inverse Element von b_i bezüglich der Summe (im Ring K) darstellt.

- Operationen auf Polynomen:

  Beispiele mit $\mathbb{Z}$ als Ring:

  Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$a(x) + b(x) = x^2 + x + 7,$$
$$a(x) - b(x) = x^2 - 7x + 3.$$

  Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 5$ ergibt sich

$$a(x) + b(x) = 6,$$
$$a(x) - b(x) = 2x^3 - 4.$$

- Operationen auf Polynomen:

  Beispiele mit $\mathbb{Z}_6$ als Ring:

  Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$a(x) + b(x) = x^2 + x + 1,$$
$$a(x) - b(x) = x^2 + 5x + 3.$$

  Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 5$ ergibt sich

$$a(x) + b(x) = 0,$$
$$a(x) - b(x) = 2x^3 + 2.$$

- Operationen auf Polynomen:

  Das Produkt zweier Polynome

$$a(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$b(x) = b_m x^m + \cdots + b_1 x + b_0$$

  erhält man durch Ausmultiplizieren und anschließendes Sortieren und Zusammenfassen der Koeffizienten, also

$$(a \cdot b)(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \cdots$$
$$= \sum_{i=0}^{m+n} \sum_{j=0}^{i} a_j b_{i-j} x^i .$$

- Operationen auf Polynomen:

  Beispiel mit $\mathbb{Z}_6$ als Ring:

  Für $a(x) = x^2 + 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$(a \cdot b)(x) = (1 \cdot 4)x^3 + (1 \cdot 2 + 3 \cdot 4)x^2 + (3 \cdot 2 + 5 \cdot 4)x + 5 \cdot 2$$
$$= 4x^3 + 2x^2 + 2x + 4.$$

- Polynomgrad bei diesen Operationen:
  - Beispiel auf dem Ring $K = \mathbb{Z}_4$:
    $a(x) = 2x + 1,\ b(x) = 2x + 2.$
    $a(x) + b(x) = 3,\ a(x) \cdot b(x) = 2x + 2.$
  - Summe von Polynomen:
    $$\mathrm{grad}\big(a(x) + b(x)\big) \leq \max\{\mathrm{grad}\big(a(x)\big), \mathrm{grad}\big(b(x)\big)\}.$$
  - Produkt von Polynomen:
    $\mathrm{grad}\big(a(x) \cdot b(x)\big) \leq \mathrm{grad}\big(a(x)\big) + \mathrm{grad}\big(b(x)\big)$.
    Für Polynome auf Körpern gilt hier „=“.

- Operationen auf Polynomen:

  Die Polynomdivision ist analog zur Division mit Rest bei ganzen Zahlen.

  – Auch hier wird fortgesetzt jeweils der höchste Anteil des verbleibenden Polynoms eliminiert.

  Für gegebene Polynome a, b $(b \neq 0)$ mit Koeffizienten aus einem Ring wird hierbei die Gleichung

$$a(x) = q(x) \cdot b(x) + r(x)$$

  gelöst, wobei $\text{grad}(r) < \text{grad}(b)$.

- Operationen auf Polynomen:

  Beispiel:

$$
\begin{array}{rl}
2x^4 + x^3 + & x + 3 \;\text{ div }\; x^2 + x - 1 = 2x^2 - x + 3 \\
\underline{-\,(2x^4 + 2x^3 - 2x^2)} & \\
-\,x^3 + 2x^2 + & x + 3 \\
\underline{-\,(-\,x^3 - x^2 + x)} & \\
3x^2 + & 3 \\
\underline{-\,(3x^2 + 3x - 3)} & \\
-\,3x + 6 &
\end{array}
$$

- Operationen auf Polynomen:

  Satz: Zu je zwei Polynomen $a(x)$ und $b(x)$ (mit invertierbarem Leitkoeffizienten b_m) gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, sodass $a(x) = q(x) \cdot b(x) + r(x)$

  und $r = 0$ oder $\text{grad}(r) < \text{grad}(b)$.

  Beispiel:

  Im vorhergehenden Schema war das

  $$2x^4 + x^3 + x + 3$$
  $$= (2 - x + 3)(x^2 + x - 1) + (-3x + 6).$$

- Operationen auf Polynomen:

  Beweis: Gilt $\text{grad}(a) < \text{grad}(b)$, setze $q = 0$ und $r = a$. Sei also $\text{grad}(a) \geq \text{grad}(b)$.

  Induktion über $\text{grad}(a)$:

  Basis: $\text{grad}(a) = 0$. Aus $\text{grad}(a) \geq \text{grad}(b)$ folgt $a(x) = a_0$ und $b(x) = b_0$ mit invertierbarem b_0 (insbesondere $b_0 \neq 0$).

  Wir können daher $q(x) = a_0/b_0$ und $r(x) = 0$ setzen.

- Operationen auf Polynomen:

  Beweis (Fort.):

  Schritt: $\text{grad}(a) = n > 0$. Sei $\text{grad}(b) = m$, $m \leq n$, und

  $a(x) = a_n x^n + \cdots + a_1 x + a_0, \quad a_n \neq 0;$

  $b(x) = b_m x^m + \cdots + b_1 x + b_0, \quad b_m$ invertierbar.

  Wir setzen

$$c(x) = a(x) - \left(\frac{a_n}{b_m}\right) x^{n-m} \cdot b(x).$$

  Dann gilt $\text{grad}(c) < \text{grad}(a)$.

- Operationen auf Polynomen:

  Beweis (Fort.):

  Nach Induktionsannahme gibt es $q'(x)$ und $r'(x)$ mit $c(x) = q'(x) \cdot b(x) + r'(x)$ und $r'(x) = 0$ oder $\text{grad}(r') < \text{grad}(b)$.

  Es gilt

$$\begin{aligned} a(x) &= (a_n/b_m)x^{n-m} \cdot\ b(x) + q'(x) \cdot b(x) + r'(x) \\ &= \left((a_n/b_m)x^{n-m} + q'(x)\right) \cdot b(x) + r'(x) \\ &=:\ q(x) \cdot b(x) + r(x)\,. \end{aligned}$$

- Operationen auf Polynomen:

  Beweis (Fort.): Zur Eindeutigkeit:

  Seien q, r, q', r' mit $q \cdot b + r = a = q' \cdot b + r'$.

  Es folgt $(q - q') \cdot b = (r - r')$.

  Wenn $q \neq q'$, dann gilt:

  - $\text{grad}\big((q - q') \cdot b\big) \geq \text{grad}(b)$;
  - $\text{grad}(r - r') \leq \max\{\text{grad}(r), \text{grad}(r')\} < \text{grad}(b)$.

  Widerspruch! Also gilt $q = q'$ und daher $r = r'$. □

- Teilbarkeit und Modulorechnung auf Polynomen:
  Definition:
  - $a(x)$ teilt $b(x)$, wenn es ein Polynom $q(x) \in K[x]$ gibt, sodass
    $$b(x) = q(x) \cdot a(x).$$
  - $a(x)$ ist kongruent zu $b(x)$ modulo $\pi(x)$, bezeichnet durch $a(x) \equiv b(x) \bmod \pi(x)$, wenn $a(x) - b(x)$ durch $\pi(x)$ teilbar ist.

- Teilbarkeit und Modulorechnung auf Polynomen:

  Beispiel: Sei $K = \mathbb{Z}_3$ und $\pi(x) = x^2 + 1$.

  Die möglichen Reste der Division durch $\pi(x)$ sind die Polynome mit Koeffizienten in $\mathbb{Z}_3$ vom Grad 0 oder 1. Es gibt genau 9 davon:

  $$\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

  Es gilt z.B. $x^3 + 1 \equiv (2x + 1) \bmod \pi(x)$.

- Teilbarkeit und Modulorechnung auf Polynomen:

  Die Kongruenzrelation $\equiv$ teilt $K[x]$ in Äquivalenzklassen:

  $K[x]_{\pi(x)} := \{f(x) \in K[x] \mid \mathrm{grad}(f) < \mathrm{grad}(\pi)\}$.

  Wenn K endlich ist, dann ist $K[x]_{\pi(x)}$ auch endlich. Es gilt dann:

$$f(x) +_{\pi(x)} g(x) := \big(f(x) + g(x)\big) \bmod \pi(x),$$
$$f(x) \cdot_{\pi(x)} g(x) := \big(f(x) \cdot g(x)\big) \bmod \pi(x).$$

- Polynomkörper:

  Es gilt: $\langle \mathbb{Z}_n, +_n, *_n \rangle$ ist Körper $\Leftrightarrow$ n ist Primzahl.

  Wann ist $\langle K[x]_{\pi(x)}, +_{\pi(x)}, *_{\pi(x)} \rangle$ ein Körper?

  Satz (ohne Beweis): Ist K ein endlicher Körper und $\pi(x)$ ein Polynom in $K[x]$. Dann gilt:

  $\langle K[x]_{\pi(x)}, +_{\pi(x)}, *_{\pi(x)} \rangle$ ist Körper

  $\Leftrightarrow$

  $\pi(x)$ ist irreduzibel.

- Polynomkörper:
  Definition: Ein Polynom $\pi(x) \in K[x]$ mit $\pi(x) \neq 0$ heißt irreduzibel, falls für alle $f(x)$, $g(x) \in K[x]$ gilt: Wenn $\pi(x) = f(x) \cdot g(x)$, dann $\mathrm{grad}(f) = 0$ oder $\mathrm{grad}(g) = 0$.

- Polynomkörper:

  Beispiel 1: Sei $K = \mathbb{Z}_2$ und $\pi(x) = x^2 + x + 1$.

  $\mathbb{Z}_2[x]_{\pi(x)}$ besteht aus allen Polynomen in $\mathbb{Z}_2[x]$ mit Grad 0 oder 1: $\mathbb{Z}_2[x]_{\pi(x)} = \{0, 1, x, x+1\}$.

  Die Verknüpfungstabellen sehen wie folgt aus:

$+_{\pi(x)}$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$*_{\pi(n)}$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

- Polynomkörper:

  Beispiel 2: Sei $K = \mathbb{Z}_2$ und $\pi(x) = x^2 + 1$.

  $\mathbb{Z}_2[x]_{\pi(x)}$ besteht aus allen Polynomen in $\mathbb{Z}_2[x]$ mit Grad 0 oder 1: $\mathbb{Z}_2[x]_{\pi(x)} = \{0, 1, x, x+1\}$.

  Die Verknüpfungstabellen sehen wie folgt aus:

$+_{\pi(x)}$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$*_{\pi(n)}$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

- Polynomkörper:
  Der Grund, warum $\mathbb{Z}_2[x]_{\pi(x)}$ für $\pi(x) = x^2 + 1$ die Körpereigenschaften nicht erfüllt, ist der folgende:
  $\pi(x)$ ist reduzibel über $K = \mathbb{Z}_2$, d.h. $\pi(x)$ lässt sich als Produkt zweier Polynome vom Grad größer gleich 1 über $\mathbb{Z}_2$ schreiben:
  $$\pi(x) = x^2 + 1 = (x + 1) \cdot (x + 1).$$
  Dies ist für $x^2 + x + 1$ jedoch nicht der Fall.

- Polynomkörper:

  Satz: Sei K ein Körper mit n Elementen, und sei $g(x) \in K[x]$, $d = \text{grad}(g) \geq 1$.

  Dann besitzt $K[x]_g$ genau n^d Elemente.

  Satz: Zu jeder Primzahl p und zu jeder natürlichen Zahl $k \geq 1$ gibt es einen endlichen Körper mit p^k Elementen; dieser wird mit $GF(p^k)$ bezeichnet.
  Notation: GF = Galois Field, nach Evariste Galois (1811–1832).

Praktische Anwendungen in der Informatik:

- Arithmetische Operationen im Rechner basieren auf diskreten und endlichen Zahlsystemen.
- Algebraische Kurven und algebraische Geometrie
- Kryptographie und Codierungstheorie
- Computeralgebra-Systeme