Script generated by TTT

Title: Mayr: 2012 ds (22.11.2012)

Date: Thu Nov 22 10:14:52 CET 2012

Duration: 92:21 min

Pages: 38

WS 2012/13

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2012WS/ds/

Wintersemester 2012

Inhaltsverzeichnis

Kapitel III Ringe und Körper

1. Definitionen und Beispiele

Definition 117
Eine Algebra $A = (S, \oplus, \odot, 0, 1)$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heißt ein Ring, falls

R1. $(S, \oplus, 0)$ eine abelsche Gruppe mit neutralem Element $0 \in S$ ist,

R2. $(S, \odot, 1)$ ein Monoid mit neutralem Element $1 \in S$ ist und

R3. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ für alle $a, b, c \in S$,
$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$ für alle $a, b, c \in S$,
(man sagt: $\oplus$ und $\odot$ sind distributiv).

Definition 118

Eine Algebra $A = (S, \oplus, \odot, 0, 1)$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heißt Körper (engl. field), falls

K1. $(S, \oplus, 0)$ eine abelsche Gruppe mit neutralem Element $0 \in S$ ist,

K2. $(S \setminus \{0\}, \odot, 1)$ eine abelsche Gruppe mit neutralem Element $1 \in S$ ist und

K3. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ für alle $a, b, c \in S$.

Beispiele 119

- Die Algebra der ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ ist ein kommutativer Ring.
- Für $n \in \mathbb{N}$, $n > 1$, ist die Algebra der Restklassen bzgl. Division durch n, also $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ ein kommutativer Ring.
- Die Menge der $n \times n$-Matrizen $(n \geq 1)$ mit Einträgen aus $\mathbb{Z}$ ist ein im Allgemeinen nicht kommutativer Ring.

Beispiele 119

- Die Algebra der ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ ist ein kommutativer Ring.
- Für $n \in \mathbb{N}$, $n > 1$, ist die Algebra der Restklassen bzgl. Division durch n, also $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ ein kommutativer Ring.
- Die Menge der $n \times n$-Matrizen $(n \geq 1)$ mit Einträgen aus $\mathbb{Z}$ ist ein im Allgemeinen nicht kommutativer Ring.

Beispiele 120

- $\mathbb{Q}$ (die Menge der rationalen Zahlen) ist ein Körper.
- Ebenso $\mathbb{R}$ und $\mathbb{C}$.
- Die Restklassenalgebra $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ ist für alle n, die prim sind, ein Körper.

2. Eigenschaften von Körpern

Satz 121
In jedem Körper K gilt:

$$a \cdot 0 = 0 \cdot a = 0 \qquad \text{für alle } a \in K\,.$$

Beweis:
Es sei a ein beliebiges Element aus K. Dann folgt aus den Axiomen:

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + a \cdot 0 - a \cdot 0 = a \cdot (0+0) - a \cdot 0 \\ &= a \cdot 0 - a \cdot 0 = 0\,. \end{aligned}$$

□

Bemerkung: Satz 121 gilt sogar in Ringen.

Definition 122
Sei R kommutativ. Ein $a \in R$, $a \neq 0$, heißt Nullteiler, falls es ein $b \in R$ gibt, $b \neq 0$, so dass $ab = 0$.

Satz 123
In jedem Körper K gilt für alle $a, b \in K$:

$$ab = 0 \quad \Longrightarrow \quad a = 0 \quad \text{oder} \quad b = 0\,.$$

(Man sagt: Körper sind nullteilerfrei.)

Beweis:
Angenommen $ab = 0$. Falls $a \neq 0$, so existiert ein multiplikatives Inverses a^{-1} von a.
Unter Verwendung von Satz 121 folgt damit:

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0\,.$$

□

2.1 Größter gemeinsamer Teiler (ggT)

Definition 124

- Seien $a, b \in \mathbb{N}$. Dann heißt $d \in \mathbb{N}$ der größte gemeinsame Teiler ($\mathrm{ggT}(a,b)$), falls gilt:
  1. $d|a$ und $d|b$;
  2. falls $d' \in \mathbb{N}$, $d'|a$ und $d'|b$, dann gilt $d'|d$.
- Sind $a_1, \ldots, a_n \in \mathbb{N}$, $n \geq 3$, dann definieren wir

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

2.1 Größter gemeinsamer Teiler (ggT)

Definition 124

- Seien $a, b \in \mathbb{N}$. Dann heißt $d \in \mathbb{N}$ der größte gemeinsame Teiler ($\mathrm{ggT}(a,b)$), falls gilt:
  1. $d|a$ und $d|b$;
  2. falls $d' \in \mathbb{N}$, $d'|a$ und $d'|b$, dann gilt $d'|d$.
- Sind $a_1, \ldots, a_n \in \mathbb{N}$, $n \geq 3$, dann definieren wir

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

Satz 125

Seien $a, b \in \mathbb{N}$. Dann gibt es $c, d \in \mathbb{Z}$, so dass

$$c \cdot a + d \cdot b = \mathrm{ggT}(a, b)\,.$$

2.1 Größter gemeinsamer Teiler (ggT)

Definition 124

- Seien $a, b \in \mathbb{N}$. Dann heißt $d \in \mathbb{N}$ der größte gemeinsame Teiler ($\mathrm{ggT}(a, b)$), falls gilt:
  1. $d|a$ und $d|b$;
  2. falls $d' \in \mathbb{N}$, $d'|a$ und $d'|b$, dann gilt $d'|d$.
- Sind $a_1, \ldots, a_n \in \mathbb{N}$, $n \geq 3$, dann definieren wir

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

Satz 125

Seien $a, b \in \mathbb{N}$. Dann gibt es $c, d \in \mathbb{Z}$, so dass

$$c \cdot a + d \cdot b = \mathrm{ggT}(a, b)\,.$$

Beweis:

Sei o.B.d.A. $a > b$. Der Euklidische Algorithmus (fortgesetzte ganzzahlige Division mit Rest) (Euklid von Alexandria, ca. 325–265 v. Chr.) liefert eine Folge

$$\begin{aligned}
r_0 &:= a = q_2 \cdot b + r_2 && \text{, mit } 0 < r_2 < b, q_2, r_2 \in \mathbb{N}_0 \\
r_1 &:= b = q_3 \cdot r_2 + r_3 && \text{, mit } 0 < r_3 < r_2, q_3, r_3 \in \mathbb{N}_0 \\
r_2 &= q_4 \cdot r_3 + r_4 && \text{, mit } 0 < r_4 < r_3, q_4, r_4 \in \mathbb{N}_0 \\
&\vdots \\
r_{m-3} &= q_{m-1} \cdot r_{m-2} + r_{m-1} && \text{, mit } 0 < r_{m-1} < r_{m-2} \qquad (*) \\
r_{m-2} &= q_m \cdot r_{m-1} + r_m && \text{, mit } 0 = r_m < r_{m-1}
\end{aligned}$$

Dann gilt $r_{m-1}|a$ und $r_{m-1}|b$ sowie $\mathrm{ggT}(a, b)|r_{m-1}$.

Also $r_{m-1} = \mathrm{ggT}(a, b)$.

Rückwärtiges iteratives Ersetzen von $r_{m-2}, r_{m-3}, \ldots$ in Gleichung (*) entsprechend den vorhergehenden Gleichungen liefert die gewünschte Darstellung. □

Beweis:
Sei o.B.d.A. $a > b$. Der Euklidische Algorithmus (fortgesetzte ganzzahlige Division mit Rest) (Euklid von Alexandria, ca. 325–265 v. Chr.) liefert eine Folge

$$\begin{aligned}
r_0 := a &= q_2 \cdot b + r_2 && \text{, mit } 0 < r_2 < b, q_2, r_2 \in \mathbb{N}_0 \\
r_1 := b &= q_3 \cdot r_2 + r_3 && \text{, mit } 0 < r_3 < r_2, q_3, r_3 \in \mathbb{N}_0 \\
r_2 &= q_4 \cdot r_3 + r_4 && \text{, mit } 0 < r_4 < r_3, q_4, r_4 \in \mathbb{N}_0 \\
&\vdots \\
r_{m-3} &= q_{m-1} \cdot r_{m-2} + r_{m-1} && \text{, mit } 0 < r_{m-1} < r_{m-2} \qquad (*) \\
r_{m-2} &= q_m \cdot r_{m-1} + r_m && \text{, mit } 0 = r_m < r_{m-1}
\end{aligned}$$

Dann gilt $r_{m-1} | a$ und $r_{m-1} | b$ sowie $\mathrm{ggT}(a,b) | r_{m-1}$.
Also $r_{m-1} = \mathrm{ggT}(a,b)$.
Rückwärtiges iteratives Ersetzen von $r_{m-2}, r_{m-3}, \ldots$ in Gleichung (*) entsprechend den vorhergehenden Gleichungen liefert die gewünschte Darstellung. □

Satz 126
Bezeichnet man mit $+_n$ und $\cdot_n$ die Addition bzw. Multiplikation modulo n, so gilt:

$$(\mathbb{Z}_n, +_n, \cdot_n) \text{ ist ein Körper} \quad \Longleftrightarrow \quad n \text{ ist Primzahl}.$$

Satz 126
Bezeichnet man mit $+_n$ und $\cdot_n$ die Addition bzw. Multiplikation modulo n, so gilt:

$$(\mathbb{Z}_n, +_n, \cdot_n) \text{ ist ein Körper} \quad \Longleftrightarrow \quad n \text{ ist Primzahl}.$$

Beweis:
Die Axiome K1 und K3 sind durch die Addition und Multiplikation modulo n offensichtlich erfüllt. Wir haben bereits gesehen, dass a modulo n genau dann ein multiplikatives Inverses hat, wenn a und n teilerfremd sind, also

$$\mathrm{ggT}(a,n) = 1\,.$$

Falls n prim ist, gilt dies für alle a, $1 \le a < n$.
Umgekehrt kann $ggT(a,n) = 1$ für alle a, $1 \le a < n$ nur gelten, falls n prim ist. □

Beweis:
Die Axiome K1 und K3 sind durch die Addition und Multiplikation modulo n offensichtlich erfüllt. Wir haben bereits gesehen, dass a modulo n genau dann ein multiplikatives Inverses hat, wenn a und n teilerfremd sind, also

$$\mathrm{ggT}(a,n) = 1\,.$$

Falls n prim ist, gilt dies für alle a, $1 \le a < n$.

2.2 Multiplikative Gruppe endlicher Körper

Satz 127
In jedem endlichen Körper K ist die multiplikative Gruppe $K^* = K \setminus \{0\}$ zyklisch, d.h. es gibt ein Element $g \in K^*$ mit $K^* = \{1, g, g^2, \ldots, g^{|K|-2}\}$.

Beweis:
Es gilt: $\mathrm{ord}(a) < \infty$ für alle $a \in K^*$. Sei a ein Element in K^* mit maximaler Ordnung:

$$\max\{\mathrm{ord}(b) \mid b \in K^*\} = \mathrm{ord}(a)\,.$$

Es ist zu zeigen, dass $\mathrm{ord}(a) = |K| - 1$. Dazu betrachten wir das Polynom $x^{\mathrm{ord}(a)} - 1$, das Grad $\mathrm{ord}(a)$ hat.

2.2 Multiplikative Gruppe endlicher Körper

Satz 127

In jedem endlichen Körper K ist die multiplikative Gruppe $K^* = K \setminus \{0\}$ zyklisch, d.h. es gibt ein Element $g \in K^*$ mit $K^* = \{1, g, g^2, \ldots, g^{|K|-2}\}$.

Beweis:

Es gilt: $\mathrm{ord}(a) < \infty$ für alle $a \in K^*$. Sei a ein Element in K^* mit maximaler Ordnung:

$$\max\{\mathrm{ord}(b) \mid b \in K^*\} = \mathrm{ord}(a) .$$

Es ist zu zeigen, dass $\mathrm{ord}(a) = |K| - 1$. Dazu betrachten wir das Polynom $x^{\mathrm{ord}(a)} - 1$, das Grad $\mathrm{ord}(a)$ hat.

Für jedes $b \in K^*$ gilt, dass $\mathrm{ord}(b) \mid \mathrm{ord}(a)$ (da sonst ab größere Ordnung als a hätte). Also ist jedes Element von K^* eine Nullstelle des obigen Polynoms. Da ein Polynom vom Grad k höchstens k verschiedene Nullstellen haben kann (warum? Siehe dazu später Satz ??), folgt daraus $\mathrm{ord}(a) \geq |K^*| = |K| - 1$. □

2.3 Primitive Elemente

Definition 128

Sei K ein endlicher Körper. Ein Element a, das die multiplikative Gruppe $K^* = K \setminus \{0\}$ erzeugt, nennt man primitives Element.

Beispiel 129

In $\mathbb{Z}_5^*$ sind sowohl 2 als auch 3 primitive Elemente:

$$\begin{array}{ll} 2^0 = 1 & 3^0 = 1 \\ 2^1 = 2 & 3^1 = 3 \\ 2^2 = 4 & 3^2 = 4 \\ 2^3 = 3 & 3^3 = 2 \\ (2^4 = 1) & 3^4 = 1) \end{array}$$

Bemerkung: $(\mathbb{Z}_4, +_4, \cdot_4, 0, 1)$ ist kein Körper!

Beispiel 130

Setzt man $K = \{0, 1, a, b\}$ und definiert eine Addition und Multiplikation wie folgt:

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

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

so bildet $(K, \oplus, \odot, 0, 1)$ einen Körper (Übung!).

Bemerkung: $(\mathbb{Z}_4, +_4, \cdot_4, 0, 1)$ ist kein Körper!

Beispiel 130

Setzt man $K = \{0, 1, a, b\}$ und definiert eine Addition und Multiplikation wie folgt:

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

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

so bildet $(K, \oplus, \odot, 0, 1)$ einen Körper (Übung!).

3. Polynome

3.1 Definition und Grundlagen

Definition 131
Sei R ein (kommutativer) Ring. Ein Polynom über R in der Variablen x ist eine Funktion p der Form

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

wobei $n \in \mathbb{N}_0$, $a_i \in R$ und $a_n \neq 0$.
n heißt der Grad des Polynoms, $a_0, \ldots, a_n$ seine Koeffizienten.
Die Funktion p ordnet jedem Wert $x_0 \in R$ den Wert $p(x_0) \in R$ zu, ist also eine Funktion von R nach R.
$R[x]$ bezeichnet die Menge der Polynome über dem Ring R in der Variablen x.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel 132

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

3.2 Rechnen mit Polynomen

Berechnung des Funktionswertes
Um den Wert eines Polynoms an einer bestimmten Stelle $x_0 \in R$ zu bestimmen, verwendet man am besten das sogenannte Hornerschema:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ &= ((\ldots(((a_n x + a_{n-1})x + a_{n-2})x + \ldots.)x + a_1)x + a_0. \end{aligned}$$

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel 132

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

3.2 Rechnen mit Polynomen

Berechnung des Funktionswertes
Um den Wert eines Polynoms an einer bestimmten Stelle $x_0 \in R$ zu bestimmen, verwendet man am besten das sogenannte Hornerschema:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ &= ((\ldots(((a_n x + a_{n-1})x + a_{n-2})x + \ldots.)x + a_1)x + a_0. \end{aligned}$$

Hat man die Koeffizienten in einem Array $a[0..n]$ abgespeichert, kann man den Funktionswert $p(x_0)$ daher wie folgt berechnen:

```
begin
  p ← a[n]
  for i = n-1 downto 0 do
    p ← p · x_0 + a[i]
  end
  return(p)
end
```

Beobachtung:
Für die Auswertung eines Polynoms vom Grad n genügen damit $O(n)$ Multiplikationen und Additionen.

Addition
Die Summe zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ ist (sei o.B.d.A. $m \leq n$) definiert durch

$$(a + b)(x) = c_n x^n + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = a_i + b_i \,.$$

Bemerkungen:

Beispiel 133

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich $(a+b)(x) = x^2 + x + 7$. Hier gilt $\mathrm{grad}(a+b) = 2 = \mathrm{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen $(a+b)(x) = 2$ und somit $\mathrm{grad}(a+b) = 0 < 3 = \max\{\mathrm{grad}(a), \mathrm{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\leq n$ lässt sich in $O(n)$ arithmetischen Schritten berechnen.

Beispiel 133

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich $(a+b)(x) = x^2 + x + 7$. Hier gilt $\mathrm{grad}(a+b) = 2 = \mathrm{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen $(a+b)(x) = 2$ und somit $\mathrm{grad}(a+b) = 0 < 3 = \max\{\mathrm{grad}(a), \mathrm{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\leq n$ lässt sich in $O(n)$ arithmetischen Schritten berechnen.

Diskrete Strukturen
©Ernst W. Mayr
206/215

Multiplikation

Das Produkt zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ erhält man durch Ausmultiplizieren und anschliessendes Sortieren und Zusammenfassen der Koeffizienten. Also

$$(a \cdot b)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Für den Grad des Produktpolynoms gilt

$$\mathrm{grad}(a \cdot b) = \mathrm{grad}(a) + \mathrm{grad}(b)\,,$$

falls R nullteilerfrei sowie $a \neq 0 \neq b$ ist, ansonsten

$$\mathrm{grad}(a \cdot b) \leq \mathrm{grad}(a) + \mathrm{grad}(b)\,.$$

Beispiel 134

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

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + \\ &\qquad ((-3) \cdot 2 + 5 \cdot 4)x + 5 \cdot 2 \\ &= 4x^3 - 10x^2 + 14x + 10\,.\end{aligned}$$

Man sagt auch, dass die Koeffizienten

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

des Produktpolynoms durch Faltung der Koeffizientenfolgen von $a(x)$ und $b(x)$ entstehen.

Beobachtung:
Das Produkt zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Es gibt dafür aber auch schnellere Algorithmen!

Division
Für diesen Abschnitt setzen wir voraus, dass der Koeffizientenring ein Körper ist.
Betrachte das Schema

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

Beobachtung:
Das Produkt zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Es gibt dafür aber auch schnellere Algorithmen!