WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

11-14-2004

Kapitel 4. Ringe und Körper

Definition

Eine Algebra $A = \langle S, \oplus, \odot \rangle$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heißt ein Ring, falls

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

R2. $\langle S, \odot \rangle$ 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).

Kapitel 4. Ringe und Körper

Definition

Eine Algebra $A = \langle S, \oplus, \odot \rangle$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heißt ein Ring, falls

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

R2. $\langle S, \odot \rangle$ 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).

Kapitel 4. Ringe und Körper

Definition

Eine Algebra $A = \langle S, \oplus, \odot \rangle$ mit zwei zweistelligen Operatoren $\oplus$ und $\odot$ heißt ein Ring, falls

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

R2. $\langle S, \odot \rangle$ 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

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

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

K2. $\langle S \setminus \{0\}, \odot \rangle$ 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 $a, b, c \in S$.

Definition

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

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

K2. $\langle S \setminus \{0\}, \odot \rangle$ 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 $a, b, c \in S$.

Definition

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

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

K2. $\langle S \setminus \{0\}, \odot \rangle$ 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

- Die Algebra der ganzen Zahlen $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ ist ein kommutativer Ring.
- Für $n \in \mathbb{N}$, $n > 1$, ist die Algebra der Restklassen bzgl. Division durch n, also $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$ 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

- Die Algebra der ganzen Zahlen $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ ist ein kommutativer Ring.
- Für $n \in \mathbb{N}$, $n > 1$, ist die Algebra der Restklassen bzgl. Division durch n, also $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$ 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

- Die Algebra der ganzen Zahlen $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ ist ein kommutativer Ring.
- Für $n \in \mathbb{N}$, $n > 1$, ist die Algebra der Restklassen bzgl. Division durch n, also $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$ 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:

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

Beispiele:

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

Beispiele:

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

Satz

1 In jedem Körper K gilt:

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

Beweis.

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

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + 0 = a \cdot 0 + (a + (-a)) = ((a \cdot 0) + a) + (-a) \\ &= (a \cdot (0 + 1)) + (-a) = (a \cdot 1) + (-a) = a + (-a) \\ &= 0 \,. \end{aligned}$$

□

Satz

1 In jedem Körper K gilt:

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

Beweis.

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

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + 0 = a \cdot 0 + (a + (-a)) = ((a \cdot 0) + a) + (-a) \\ &= (a \cdot (0 + 1)) + (-a) = (a \cdot 1) + (-a) = a + (-a) \\ &= 0 \,. \end{aligned}$$

□

Satz

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

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

(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 1 folgt damit:

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

Satz

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

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

(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 1 folgt damit:

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

□

Satz

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

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

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, $1 \leq a < n$.
Umgekehrt kann $\mathrm{ggT}(a, n) = 1$ für alle a, $1 \leq a < n$ nur gelten, falls n prim ist. □

Satz

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

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

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, $1 \leq a < n$.

Umgekehrt kann $\mathrm{ggT}(a, n) = 1$ für alle a, $1 \leq a < n$ nur gelten, falls n prim ist. □

Satz

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

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

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, $1 \leq a < n$.
Umgekehrt kann $\mathrm{ggT}(a, n) = 1$ für alle a, $1 \leq a < n$ nur gelten, falls n prim ist. □

Multiplikative Gruppe endlicher Körper

Satz

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

*B*eweis:
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 viele verschiedene Nullstellen haben kann (warum?), folgt daraus $\mathrm{ord}(a) \geq |K^*| = |K| - 1$.
q. e. d.

Multiplikative Gruppe endlicher Körper

Satz

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

*B*eweis:
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 viele verschiedene Nullstellen haben kann (warum?), folgt daraus $\mathrm{ord}(a) \geq |K^*| = |K| - 1$.

q. e. d.

Multiplikative Gruppe endlicher Körper

Satz

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

*B*eweis:
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 viele verschiedene Nullstellen haben kann (warum?), folgt daraus $\mathrm{ord}(a) \geq |K^*| = |K| - 1$.
q. e. d.

Primitive Elemente

Definition

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

Beispiel

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

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

Primitive Elemente

Definition

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

Beispiel

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

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

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

Beispiel

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 $\langle K, \oplus, \odot, 0, 1 \rangle$ einen Körper (Übung!).

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

Beispiel

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 $\langle K, \oplus, \odot, 0, 1 \rangle$ einen Körper (Übung!).