Diskrete Mathematik

Inhalte 8. Vorlesungswoche

Sebastian Iwanowski
FH Wedel

Referenzen zum Nacharbeiten:

Lang 7 (teilweise),
letzter Absatz von Beutelspacher 3.7 (für $\mathbb{Z}_n^*$)
irgendein Buch aus der Bibliothek (Signatur 2.2 oder ähnlich)
mit den Themen Gruppen, Ringe, Körper, Polynome

4. Zahlentheorie

4.5 Algebraische Strukturen

Definition der Struktur einer Gruppe:

Sei G eine nichtleere Menge und $\oplus$ eine Verknüpfung zwischen den Elementen von G.
Dann heißt die Struktur $(G, \oplus)$ eine **abelsche Gruppe**, wenn folgende Eigenschaften erfüllt sind:

1) $\forall\ a,b \in G: a \oplus b \in G$ — ***innere Verknüpfung***

2) $\forall\ a,b,c \in G: (a \oplus b) \oplus c = a \oplus (b \oplus c)$ — ***Assoziativgesetz***

3) $\exists\ e \in G\ \forall\ a \in G: e \oplus a = a \oplus e = a$ — ***Neutrales Element***

4) $\forall\ a \in G\ \exists\ a^{-1} \in G: a^{-1} \oplus a = a \oplus a^{-1} = e$ — ***Inverses Element***

5) $\forall\ a,b \in G: a \oplus b = b \oplus a$ — ***Kommutativgesetz***

nur Eigenschaft 1):	Gruppoid
nur Eigenschaft 1), 2):	Halbgruppe
nur Eigenschaft 1), 2), 3), 4):	Gruppe

4. Zahlentheorie

4.5 Algebraische Strukturen

Beispiele für unendliche Gruppen bzw. Halbgruppen:

1) $(\mathbb{N},+)$
2) $(\mathbb{Z},+)$
3) $(\mathbb{Z},\cdot)$
4) $(\mathbb{Q},+)$
5) $(\mathbb{Q},\cdot)$
6) $(\mathbb{Q} \setminus \{0\},\cdot)$
7) $(\mathbb{Q}^+,\cdot)$
8) $(\mathbb{R} \setminus \{0\},\cdot)$
9) $(\mathbb{R} \setminus \{0\},+)$
10) $(\{f: \mathbb{R}\to\mathbb{R}\},+)$
11) $(\{f: \mathbb{R}\to\mathbb{R}\},\cdot)$
12) $(\{f: \mathbb{R} \setminus \{0\} \to\mathbb{R} \setminus \{0\}\},\cdot)$
13) $(\{f: \mathbb{R}^+ \to\mathbb{R}^+\},\cdot)$
14) $(\{f: \mathbb{R} \to\mathbb{R}\},\circ)$
15) $(\{f: \mathbb{R} \to\mathbb{R}$, f bijektiv$\},\circ)$
16) $(\{f: \mathbb{R} \to\mathbb{R}$, f differenzierbar$\},\circ)$
17) $(\{f: \mathbb{R} \to\mathbb{R}$, f bijektiv und differenzierbar$\},\circ)$
18) $(\{f: \mathbb{R} \to\mathbb{R}$, f linear$\},\circ)$
19) $(\{f: \mathbb{R} \to\mathbb{R}$, f linear$\},+)$
20) $(\{f: \mathbb{R} \to\mathbb{R}$, f Polynomfunktion$\},+)$

4. Zahlentheorie

4.5 Algebraische Strukturen

Beispiele für endliche Gruppen bzw. Halbgruppen:

1) $(\mathbb{Z}_n,+)$ *(zyklische Gruppe mit additiver Verknüpfung)*

2) $(\mathbb{Z}_n,\cdot)$

3) $(\mathbb{Z}_n \setminus \{[0]_n\},\cdot)$

4) $(\mathbb{Z}_n^*,\cdot)$ *(multiplikative Gruppe der zu n teilerfremden Restklassen,* ***prime Restklassengruppe mod n****))*

5) Symmetriegruppe eines gleichseitigen Dreiecks

6) $(\{x,\frac{1}{x},1-x,\frac{x-1}{x},\frac{1}{1-x},\frac{x}{1-x}\},\circ)$ (Hintereinanderschaltung der Funktionen)

7) $(\mathbb{Z}_n \times \mathbb{Z}_n,+)$ *(2-dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*

8) $((\mathbb{Z}_n)^r,+)$ *(r-dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*

4. Zahlentheorie

4.5 Algebraische Strukturen

Wann gelten zwei Gruppen als gleich?

Definition: Zwei Gruppen $(G,\oplus)$ und $(H,\odot)$ gelten als gleich (isomorph), wenn es zwischen ihnen eine bijektive Abbildung $I: G \to H$ gibt, welche die Verküpfungsstruktur erhält:

$$\forall\, a,b \in G: I(a \oplus b) = I(a) \odot I(b)$$

$$\forall\, a,b \in H: I^{-1}(a \odot b) = I^{-1}(a) \oplus I^{-1}(b)$$

I wird *Isomorphismus* genannt.

Charakteristische Elemente endlicher Gruppen:

Ordnung einer Gruppe

Ordnung eines Elements

Erzeugnis eines Elements (einer Menge von Elementen)

Satz: Jede endliche Gruppe wird durch endlich viele Elemente erzeugt.

Bemerkung: Auch unendliche Gruppen können durch endlich viele Elemente erzeugt werden (aber niemals durch ein einzelnes).

4. Zahlentheorie

4.5 Algebraische Strukturen

Definition der Struktur eines Körpers:

Sei K eine nichtleere Menge und $\oplus$, $\odot$ Verknüpfungen zwischen den Elementen von G.
Dann heißt die Struktur (K, $\oplus$, $\odot$) ein **Körper**, wenn folgende Eigenschaften erfüllt sind:

1) (K, $\oplus$) ist abelsche Gruppe mit neutralem Element e_0

2) (K, $\odot$) ist Halbgruppe

3) $\forall\ a,b,c \in K: (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$
$c \odot (a \oplus b) = (c \odot a) \oplus (c \odot b)$ ***Distributivgesetze***

4) $\exists\ e_1 \in K\ \forall\ a \in K: e_1 \odot a = a \odot e_1 = a$ ***Neutrales Element***

5) $\forall\ a \in K \setminus \{e_0\}\ \exists\ a^{-1} \in K \setminus \{e_0\}: a^{-1} \odot a = a \odot a^{-1} = e_1$ ***Inverses Element***

6) $\forall\ a,b \in K: a \odot b = b \odot a$ ***Kommutativgesetz***

nur Eigenschaft 1), 2), 3): Halbring
nur Eigenschaft 1), 2), 3), 4), 6): Ring
nur Eigenschaft 1), 2), 3), 4), 5): Schiefkörper

4. Zahlentheorie

4.5 Algebraische Strukturen

Beispiele von unendlichen Körpern, Ringen, etc.:

1) $(\mathbb{Z},+,\cdot)$
2) $(\mathbb{Q},+,\cdot)$
3) $(\mathbb{R} \setminus \{0\},+,\cdot)$
4) $(\{f: \mathbb{R}\to\mathbb{R}\},+,\cdot)$
5) $(\{f: \mathbb{R}\to\mathbb{R}$, f bijektiv$\},+,\circ)$
6) $(\{f: \mathbb{R}\to\mathbb{R}$, f bijektiv$\},\circ,+)$
7) $(\{f: \mathbb{R}\to\mathbb{R}$, f linear$\},+,\cdot)$
8) $(\{f: \mathbb{R}\to\mathbb{R}$, f Polynomfunktion$\},+,\cdot)$

4. Zahlentheorie

4.5 Algebraische Strukturen

Endliche Körper:

1) $(\mathbb{Z}_p,+,\cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r,+,\cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Satz (Galois, 1811-1832): ***Das sind alle!***

Endliche Körper gibt es nur mit p^r Elementen (p Primzahl, r natürliche Zahl).
Jeder endliche Körper ist bis auf Isomorphie gleich zu den oben genannten.
Der Körper mit q Elementen wird GF (q) genannt (GF = Galoisfeld)

Wie sieht die multiplikative Verknüpfung für r > 1 aus ?

Die multiplikative Gruppe des Körpers $((\mathbb{Z}_p)^r,+,\cdot)$ ist isomorph zu $(\mathbb{Z}_{p^r-1},+)$.

In welcher Reihenfolge muss man die Elemente für die multiplikative Verknüpfung anordnen, damit das Distributivgesetz erfüllt ist?

➔ Konstruktionsanleitung mit Hilfe von Polynomen

4. Zahlentheorie

4.5 Algebraische Strukturen

Definition Polynom für einen beliebigen Körper K:

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

Hierbei steht x für eine Variable mit Definitionsbereich K, a_i für eine beliebige Konstante aus K und x^i bedeutet die i-fache Hintereinanderschaltung der multiplikativen Verknüpfung angewendet auf das Körperelement x.
Ein Polynom ist durch die Angabe des Tupels $(a_n,a_{n-1},...,a_1,a_0)$ eindeutig charakterisiert.

Das größte n mit $a_n \neq 0$ wird als *Grad des Polynoms* bezeichnet.
Die Menge der Polynome über einem Körper K wird mit K[x] bezeichnet.

Satz:

(K[x],+,·) bildet einen Ring.

4. Zahlentheorie

4.5 Algebraische Strukturen

Polynomdivision mit Rest:

Seien f[x], g[x] Polynome.
Dann gibt es Polynome q[x], r[x] mit Grad (r[x]) < Grad (g[x]):

$$f[x] = q[x] \cdot g[x] + r[x]$$

Die Polynome q[x], r[x] werden analog zum schriftlichen Divisionsverfahren von Zahlen gebildet. (Euklidischer Algorithmus).
Analog zur Definition bei Zahlen wird das Restpolynom r[x] auch f[x] mod g[x] genannt.

Definitionen:

Eine ***Nullstelle*** zu einem gegebenen Polynom ist ein Wert des Körpers K, dessen Einsetzung in das Polynom den Wert 0 ergibt.

Ein ***irreduzibles Polynom*** über einem Körper K
ist ein Polynom ohne Nullstellen in K.

4. Zahlentheorie

4.5 Algebraische Strukturen

Konstruktionsanleitung für GF (q) mit $q = p^r$ (p Primzahl, r natürliche Zahl):

1) Bestimme die Additions- und Multiplikationstabellen von GF (p):
   Der Körper ist isomorph zum Restklassenkörper $(\mathbb{Z}_p,+,\cdot)$.

2) Identifiziere die Elemente aus GF (q) mit den p^r verschiedenen Polynomen über $(\mathbb{Z}_p,+,\cdot)$ mit Grad < r

3) Bilde die Additionstabelle wie bei Polynomen üblich.
   (Anmerkung: Die entstehende Gruppe ist isomorph zu $((\mathbb{Z}_p)^r,+)$)

4) Wähle ein irreduzibles Polynom g[x] über GF (p) mit Grad r.
   Bilde die Multiplikationstabelle wie bei Polynomen üblich,
   aber *rechne modulo g[x]*, um jeweils Polynome mit Grad < r zu erzeugen.
   (Anmerkung: Die entstehende Gruppe ist isomorph zu $(\mathbb{Z}_{q-1},+)$)

4. Zahlentheorie

4.5 Algebraische Strukturen

Beispiel: GF (9) $9 = 3^3$ (p =3, r=3)

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

·	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	2	5	8	1	4	7
4	0	4	8	5	6	1	7	2	3
5	0	5	7	8	1	3	4	6	2
6	0	6	3	1	7	4	2	8	5
7	0	7	5	4	2	6	8	3	1
8	0	8	4	7	3	2	5	1	6