Ayrık Matematik

Cebirsel Yapılar

H. Turgut Uyar   Ayşegül Gençata Yayımlı   Emre Harmancı

2001-2012

Lisans

Konular

Cebirsel Yapı

- cebirsel yapı: $<$küme, işlemler, sabitler$>$
  - taşıyıcı küme
  - işlemler: ikili, tekli
  - sabitler: etkisiz, yutucu

İşlem

- her işlem bir fonksiyon
- ikili işlem:
  $\circ : S \times S \rightarrow T$
- tekli işlem:
  $\Delta : S \rightarrow T$
- kapalı: $T \subseteq S$

Kapalı İşlem Örnekleri

Örnek

- çıkarma işlemi $\mathbb{Z}$ kümesinde kapalı
- çıkarma işlemi $\mathbb{Z}^+$ kümesinde kapalı değil

İkili İşlem Özellikleri

Tanım
değişme:
$\forall a, b \in S \ a \circ b = b \circ a$

Tanım
birleşme:
$\forall a, b, c \in S \ (a \circ b) \circ c = a \circ (b \circ c)$

İkili İşlem Örneği

Örnek
$\circ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$a \circ b = a + b - 3ab$

- değişme:
  $a \circ b = a + b - 3ab = b + a - 3ba = b \circ a$
- birleşme:

$$\begin{aligned} (a \circ b) \circ c &= (a + b - 3ab) + c - 3(a + b - 3ab)c \\ &= a + b - 3ab + c - 3ac - 3bc + 9abc \\ &= a + b + c - 3ab - 3ac - 3bc + 9abc \\ &= a + (b + c - 3bc) - 3a(b + c - 3bc) \\ &= a \circ (b \circ c) \end{aligned}$$

Sabitler

Tanım
etkisiz eleman:
$x \circ 1 = 1 \circ x = x$

- soldan etkisiz: $1_l \circ x = x$
- sağdan etkisiz: $x \circ 1_r = x$

Tanım
yutucu eleman:
$x \circ 0 = 0 \circ x = 0$

- soldan yutucu: $0_l \circ x = 0$
- sağdan yutucu: $x \circ 0_r = 0$

Sabit Örnekleri

Örnek

- $< \mathbb{N}, max >$ için etkisiz eleman 0
- $< \mathbb{N}, min >$ için yutucu eleman 0
- $< \mathbb{Z}^+, min >$ için yutucu eleman 1

Örnek

$\circ$	a	b	c
a	a	b	b
b	a	b	c
c	a	b	a

- b soldan etkisiz
- a ve b sağdan yutucu

Sabitler

Teorem
$\exists 1_l \wedge \exists 1_r \Rightarrow 1_l = 1_r$

Tanıt.
$1_l \circ 1_r = 1_l = 1_r$ □

Teorem
$\exists 0_l \wedge \exists 0_r \Rightarrow 0_l = 0_r$

Tanıt.
$0_l \circ 0_r = 0_l = 0_r$ □

Evrik

- $x \circ y = 1$ ise:
  - x elemanı y elemanının *sol evriği*
  - y elemanı x elemanının *sağ evriği*
- $x \circ y = y \circ x = 1$ ise x ile y evrik

Evrik

Teorem

$\circ$ işlemi birleşme özelliği taşıyorsa:

$w \circ x = x \circ y = 1 \Rightarrow w = y$

Tanıt.

$$\begin{aligned} w &= w \circ 1 \\ &= w \circ (x \circ y) \\ &= (w \circ x) \circ y \\ &= 1 \circ y \\ &= y \end{aligned} \qquad \square$$

Cebir Ailesi

- cebir ailesi: cebirsel yapı, aksiyomlar
  - değişme, birleşme
  - evrik elemanlar

Cebir Ailesi Örnekleri

Örnek

- aksiyomlar:
  - $x \circ y = y \circ x$
  - $(x \circ y) \circ z = x \circ (y \circ z)$
  - $x \circ 1 = x$
- bu aksiyomları sağlayan yapılar:
  - $< \mathbb{Z}, +, 0 >$
  - $< \mathbb{Z}, \cdot, 1 >$
  - $< \mathcal{P}(S), \cup, \emptyset >$

Altcebir

Tanım

altcebir:

$A =< S, \circ, \Delta, k > \ \wedge A' =< S', \circ', \Delta', k' >$ olsun

- A' cebrinin A cebrinin bir altcebri olması için:
  - $S' \subseteq S$
  - $\forall a, b \in S' \ a \circ' b = a \circ b \in S'$
  - $\forall a \in S' \ \Delta' a = \Delta a \in S'$
  - $k' = k$

Altcebir Örnekleri

Örnek

- $< \mathbb{Z}^+, +, 0 >$ cebri, $< \mathbb{Z}, +, 0 >$ cebrinin bir altcebridir.
- $< \mathbb{N}, -, 0 >$ cebri, $< \mathbb{Z}, -, 0 >$ cebrinin bir altcebri değildir.

Yarıgruplar

Tanım

yarıgrup: $< S, \circ >$

- $\forall a, b, c \in S \ (a \circ b) \circ c = a \circ (b \circ c)$

Yarıgrup Örnekleri

Örnek

$< \Sigma^+, \& >$

- Σ: alfabe, Σ^+: en az 1 uzunluklu katarlar
- &: katar bitiştirme işlemi

Monoidler

Tanım

monoid: $< S, \circ, 1 >$

- $\forall a, b, c \in S\ (a \circ b) \circ c = a \circ (b \circ c)$
- $\forall a \in S\ a \circ 1 = 1 \circ a = a$

Monoid Örnekleri

Örnek

$< \Sigma^*, \&, \epsilon >$

- Σ: alfabe, Σ^*: herhangi uzunluklu katarlar
- &: katar bitiştirme işlemi
- ϵ: boş katar

Grup

Tanım

grup: $< S, \circ, 1 >$

- $\forall a, b, c \in S\ (a \circ b) \circ c = a \circ (b \circ c)$
- $\forall a \in S\ a \circ 1 = 1 \circ a = a$
- $\forall a \in S\ \exists a^{-1} \in S\ \ a \circ a^{-1} = a^{-1} \circ a = 1$
- *Abel grubu*: $\forall a, b \in S\ a \circ b = b \circ a$

Grup Örnekleri

Örnek

- $< \mathbb{Z}, +, 0 >$ bir gruptur.
- $< \mathbb{Q}, \cdot, 1 >$ bir grup değildir.
- $< \mathbb{Q} - \{0\}, \cdot, 1 >$ bir gruptur.

Grup Örneği: Permutasyon Bileşkesi

- permutasyon: küme içi bijektif bir fonksiyon
- gösterilim:
$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ p(a_1) & p(a_2) & \dots & p(a_n) \end{pmatrix}$$

Permutasyon Örnekleri

Örnek

$A = \{1, 2, 3\}$

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Grup Örneği: Permutasyon Bileşkesi

- permutasyon bileşkesi birleşme özelliği gösterir
- birim permutasyon: 1_A

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

- bir küme üzerindeki permutasyonların kümesi,
  permutasyon bileşkesi işlemi
  ve birim permutasyon bir grup oluşturur

Grup Örneği: Permutasyon Bileşkesi

Örnek ($\{1, 2, 3, 4\}$ kümesindeki permutasyonlar)

A	1_A	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}
1	1	1	1	1	1	1	2	2	2	2	2	2
2	2	2	3	3	4	4	1	1	3	3	4	4
3	3	4	2	4	2	3	3	4	1	4	1	3
4	4	3	4	2	3	2	4	3	4	1	3	1

	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}	p_{17}	p_{18}	p_{19}	p_{20}	p_{21}	p_{22}	p_{23}
1	3	3	3	3	3	3	4	4	4	4	4	4
2	1	1	2	2	4	4	1	1	2	2	3	3
3	2	4	1	4	1	2	2	3	1	3	1	2
4	4	2	4	1	2	1	3	2	3	1	2	1

Grup Örneği: Permutasyon Bileşkesi

Örnek

- $p_8 \diamond p_{12} = p_{12} \diamond p_8 = 1_A$:
  $p_{12} = p_8^{-1}$, $p_8 = p_{12}^{-1}$
- $p_{14} \diamond p_{14} = 1_A$:
  $p_{14} = p_{14}^{-1}$
- $G_1 =< \{1_A, p_1, \dots, p_{23}\}, \diamond, 1_A >$ bir gruptur

Grup Örneği: Permutasyon Bileşkesi

Örnek

$\diamond$	1_A	p_2	p_6	p_8	p_{12}	p_{14}
1_A	1_A	p_2	p_6	p_8	p_{12}	p_{14}
p_2	p_2	1_A	p_8	p_6	p_{14}	p_{12}
p_6	p_6	p_{12}	1_A	p_{14}	p_2	p_8
p_8	p_8	p_{14}	p_2	p_{12}	1_A	p_6
p_{12}	p_{12}	p_6	p_{14}	1_A	p_8	p_2
p_{14}	p_{14}	p_8	p_{12}	p_2	p_6	1_A

- $< \{1_A, p_2, p_6, p_8, p_{12}, p_{14}\}, \diamond, 1_A > \; G_1$'in bir altgrubudur

Sağdan ve Soldan Kaldırma

Teorem

$a \circ c = b \circ c \Rightarrow a = b$

$c \circ a = c \circ b \Rightarrow a = b$

Tanıt.

$$\begin{array}{rrcl} & a \circ c & = & b \circ c \\ \Rightarrow & (a \circ c) \circ c^{-1} & = & (b \circ c) \circ c^{-1} \\ \Rightarrow & a \circ (c \circ c^{-1}) & = & b \circ (c \circ c^{-1}) \\ \Rightarrow & a \circ 1 & = & b \circ 1 \\ \Rightarrow & a & = & b \end{array}$$

□

Grupların Temel Teoremi

Teorem

$a \circ x = b$ denkleminin tek çözümü: $x = a^{-1} \circ b$.

Tanıt.

$$\begin{array}{rrcl} & a \circ c & = & b \\ \Rightarrow & a^{-1} \circ (a \circ c) & = & a^{-1} \circ b \\ \Rightarrow & 1 \circ c & = & a^{-1} \circ b \\ \Rightarrow & c & = & a^{-1} \circ b \end{array}$$

$\square$

Halka

Tanım

halka: $< S, +, \cdot, 0 >$

- $\forall a, b, c \in S \ (a + b) + c = a + (b + c)$
- $\forall a \in S \ a + 0 = 0 + a = a$
- $\forall a \in S \ \exists(-a) \in S \ a + (-a) = (-a) + a = 0$
- $\forall a, b \in S \ a + b = b + a$
- $\forall a, b, c \in S \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\forall a, b, c \in S$
  - $a \cdot (b + c) = a \cdot b + a \cdot c$
  - $(b + c) \cdot a = b \cdot a + c \cdot a$

Alan

Tanım

alan: $< S, +, \cdot, 0, 1 >$

- bütün halka özellikleri
- $\forall a, b \in S \ a \cdot b = b \cdot a$
- $\forall a \in S \ a \cdot 1 = 1 \cdot a = a$
- $\forall a \in S \ \exists a^{-1} \in S \ a \cdot a^{-1} = a^{-1} \cdot a = 1$

Kaynaklar

Grimaldi

- Chapter 5: Relations and Functions
  - 5.4. Special Functions
- Chapter 16: Groups, Coding Theory, and Polya's Method of Enumeration
  - 16.1. Definitions, Examples, and Elementary Properties
- Chapter 14: Rings and Modular Arithmetic
  - 14.1. The Ring Structure: Definition and Examples

Kısmi Sıralı Küme

Tanım

kısmi sıra bağıntısı:

- yansımalı
- ters bakışlı
- geçişli

- *kısmi sıralı küme* (poset):
  elemanları üzerinde kısmi sıra bağıntısı tanımlanmış küme

Kısmi Sıra Örnekleri

Örnek (kümeler kümesi, $\subseteq$)

- $A \subseteq A$
- $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$
- $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

Kısmi Sıra Örnekleri

Örnek ($\mathbb{Z}$, $\leq$)

- $x \leq x$
- $x \leq y \wedge y \leq x \Rightarrow x = y$
- $x \leq y \wedge y \leq z \Rightarrow x \leq z$

Kısmi Sıra Örnekleri

Örnek ($\mathbb{Z}^+$, $|$)

- $x|x$
- $x|y \wedge y|x \Rightarrow x = y$
- $x|y \wedge y|z \Rightarrow x|z$

Karşılaştırılabilirlik

- $a \preceq b$: *a b'nin önündedir*
- $a \preceq b \vee b \preceq a$: *a ile b karşılaştırılabilir*
- çizgisel sıra:
  her eleman çifti karşılaştırılabiliyor

Karşılaştırılabilirlik Örnekleri

Örnek

- $\mathbb{Z}^+, |$: 3 ile 5 karşılaştırılamaz
- $\mathbb{Z}, \leq$: çizgisel sıra

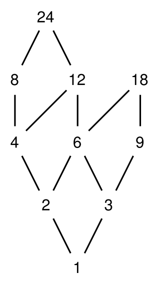
Hasse Çizenekleri

- $a \ll b$: *a b'nin hemen önündedir*
  $\neg\exists x \; a \preceq x \preceq b$
- Hasse çizeneği:
  - $a \ll b$ ise a ile b arasına çizgi
  - önde olan eleman aşağıya

Hasse Çizeneği Örnekleri

Örnek

$\{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$
$|$ bağıntısı

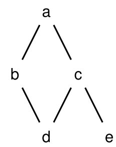


Tutarlı Sayılama

- tutarlı sayılama:
  $f : S \rightarrow \mathbb{N}$
  $a \preceq b \Rightarrow f(a) \leq f(b)$
- birden fazla tutarlı sayılama olabilir

Tutarlı Sayılama Örnekleri

Örnek



- $\{a \longmapsto 5, b \longmapsto 3, c \longmapsto 4, d \longmapsto 1, e \longmapsto 2\}$
- $\{a \longmapsto 5, b \longmapsto 4, c \longmapsto 3, d \longmapsto 2, e \longmapsto 1\}$

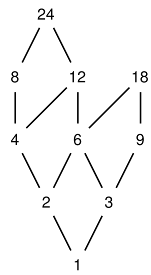
En Büyük - En Küçük Eleman

Tanım
en büyük eleman: max
$\forall x \in S \ max \preceq x \Rightarrow x = max$

Tanım
en küçük eleman: min
$\forall x \in S \ x \preceq min \Rightarrow x = min$

En Büyük - En Küçük Eleman Örnekleri

Örnek



max : 18, 24
min : 1

Sınırlar

Tanım
$A \subseteq S$

A'nın üstsınırı M:
$\forall x \in A \ x \preceq M$

$M(A)$: A'nın üstsınırları kümesi

A'nın en küçük üstsınırı $sup(A)$:
$\forall M \in M(A) \ sup(A) \preceq M$

Tanım
$A \subseteq S$

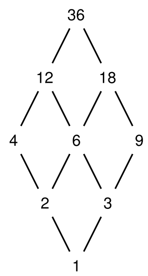
A'nın altsınırı m:
$\forall x \in A \ m \preceq x$

$m(A)$: A'nın altsınırları kümesi

A'nın en büyük altsınırı $inf(A)$:
$\forall m \in m(A) \ m \preceq inf(A)$

Sınır Örneği

Örnek (36'nın bölenleri)



inf = en büyük ortak bölen
sup = en küçük ortak kat

Kafes

Tanım
kafes: $< L, \wedge, \vee >$
$\wedge$: karşılaşma, $\vee$: bütünleşme

- $a \wedge b = b \wedge a$
  $a \vee b = b \vee a$
- $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
  $(a \vee b) \vee c = a \vee (b \vee c)$
- $a \wedge (a \vee b) = a$
  $a \vee (a \wedge b) = a$

Kısmi Sıralı Küme - Kafes İlişkisi

- P bir kısmi sıralı küme ise $< P, inf, sup >$ bir kafestir.
  - $a \wedge b = inf(a, b)$
  - $a \vee b = sup(a, b)$
- Her kafes bu tanımların geçerli olduğu bir kısmi sıralı kümedir.

Dualite

Tanım
dual:
$\wedge$ yerine $\vee$, $\vee$ yerine $\wedge$

Teorem (Dualite Teoremi)
Kafeslerde her teoremin duali de teoremdir.

Kafes Teoremleri

Teorem
$a \wedge a = a$

Tanıt.
$a \wedge a = a \wedge (a \vee (a \wedge b))$ □

Kafes Teoremleri

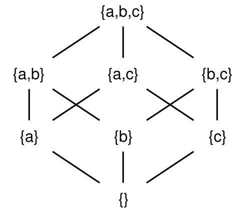
Teorem
$a \preceq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$

Kafes Örnekleri

Örnek

$< \mathcal{P}\{a, b, c\}, \cap, \cup >$

$\subseteq$ bağıntısı



Sınırlı Kafesler

Tanım
L kafesinin altsınırı: 0
$\forall x \in L \; 0 \preceq x$

Tanım
L kafesinin üstsınırı: I
$\forall x \in L \; x \preceq I$

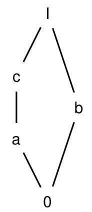
Teorem
Sonlu her kafes sınırlıdır.

Kafeslerde Dağılma

- *dağılma özellikli kafes*:
  - $\forall a, b, c \in L \; a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
  - $\forall a, b, c \in L \; a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Karşı Örnekler

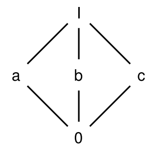
Örnek



$a \vee (b \wedge c) = a \vee 0 = a$
$(a \vee b) \wedge (a \vee c) = I \wedge c = c$

Karşı Örnekler

Örnek



$a \vee (b \wedge c) = a \vee 0 = a$
$(a \vee b) \wedge (a \vee c) = I \wedge I = I$

Kafeslerde Dağılma

Teorem
Bir kafes yalnız ve ancak bu iki yapıdan birine izomorfik bir altkafes içeriyorsa dağılma özelliği göstermez.

Bütünleşmeyle İndirgeme

Tanım
bütünleşmeyle indirgenemez eleman:
$a = x \vee y \Rightarrow a = x$ veya $a = y$

- *atom*: altsınırın hemen ardından gelen, bütünleşmeyle indirgenemez eleman

Bütünleşmeyle İndirgeme Örneği

Örnek (bölünebilirlik bağıntısı)

- asal sayılar ve 1 bütünleşmeyle indirgenemez
- 1 altsınır, asal sayılar atom

Bütünleşmeyle İndirgeme

Teorem

Bütünleşmeyle indirgenebilir bütün elemanlar, bütünleşmeyle indirgenemez elemanların bütünleşmesi şeklinde yazılabilir.

Tümleyen

Tanım

a ile x tümleyen:

$a \wedge x = 0$ ve $a \vee x = I$

Tümlemeli Kafesler

Teorem

Sınırlı, dağılma özellikli bir kafeste tümleyen varsa tektir.

Tanıt.

$a \wedge x = 0, a \vee x = I$, $a \wedge y = 0, a \vee y = I$

$$\begin{aligned} x &= x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = I \wedge (x \vee y) \\ &= x \vee y = y \vee x = I \wedge (y \vee x) \\ &= (y \vee a) \wedge (y \vee x) = y \vee (a \wedge x) = y \vee 0 = y \end{aligned}$$

$\square$

Boole Cebri

Tanım

Boole cebri:

$< B, +, \cdot, \overline{x}, 1, 0 >$

$$\begin{array}{ll} a + b = b + a & a \cdot b = b \cdot a \\ (a + b) + c = a + (b + c) & (a \cdot b) \cdot c = a \cdot (b \cdot c) \\ a + 0 = a & a \cdot 1 = a \\ a + \overline{a} = 1 & a \cdot \overline{a} = 0 \end{array}$$

Boole Cebri - Kafes İlişkisi

Tanım

Bir Boole cebri sonlu, dağılma özellikli,
her elemanın tümleyeninin olduğu bir kafestir.

Dualite

Tanım

dual:

$+$ yerine $\cdot$, $\cdot$ yerine $+$
0 yerine 1, 1 yerine 0

Örnek

$(1 + a) \cdot (b + 0) = b$
teoreminin duali:
$(0 \cdot a) + (b \cdot 1) = b$

Boole Cebri Örnekleri

Örnek

$B = \{0, 1\}, + = \vee, \cdot = \wedge$

Örnek

$B = \{$ 70'in bölenleri $\}$, $+ = okek, \cdot = obeb$

Boole Cebri Teoremleri

$a + a = a$	$a \cdot a = a$
$a + 1 = 1$	$a \cdot 0 = 0$
$a + (a \cdot b) = a$	$a \cdot (a + b) = a$
$(a + b) + c = a + (b + c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
$\overline{\overline{a}} = a$	
$\overline{a + b} = \overline{a} \cdot \overline{b}$	$\overline{a \cdot b} = \overline{a} + \overline{b}$

Kaynaklar

Okunacak: Grimaldi

- Chapter 7: Relations: The Second Time Around
  - 7.3. Partial Orders: Hasse Diagrams
- Chapter 15: Boolean Algebra and Switching Functions
  - 15.4. The Structure of a Boolean Algebra