





## ÖNSÖZ

İlk defa Cantor tarafından düzenli biçimde ele alınan küme kavramı ve kümeler arasında tanımlanan işlemlerin özellikleri üzerine kurulan kümeler teorisi matematikte yeni bir çağır açmıştır. Özellikle 19. yüzyıl matematikçilerinin çabaları ile; küme teorisine dayalı cebirsal yapılar tanımlanıp klasik matematikte sadece sayılarla yapılan cebir çalışmaları birtakım aksiyom ve sembolik gösterimlerle yeniden yapılandırılmış (genelleştirilmiş) ve bugünkü anlamıyla cebir alanı oluşturulmuştur.

Geliştirilen bu yeni matematik dalına modern cebir, soyut cebir gibi isimler verilmektedir. Son yüzyılda matematiğin bu alanı, daha önce çözümü mümkün olmayan birçok matematik probleminin çözümünü sağladığı gibi matematiğin diğer alanları ile matematiğe yakın birçok bilime de ivme kazandırmıştır. (istatistik, olasılık, fizik vb.)

Bu kitap, yukarıda önemi vurgulanan cebir alanında temel bilgilerden oluşan bir çalışmadır. Kitap, soyut matematik bilgilerinin kısa bir özeti ve cebirin üç temel yapısı olan grup, halka ve cisim yapılarının tanıtım ve özelliklerini içermektedir.

Kitap, özellikle Eğitim Fakültelerinin İlköğretim Matematik Öğretmenliği Programında okutulmakta olan Cebire Giriş dersi için yardımcı ders kitabı olarak hazırlanmakla beraber; Fen Fakültelerinin Soyut Cebir I dersi için de bir başvuru kitabı olabilir.

Kitapta sırası ile Ön Bilgiler, Gruplar, Halkalar, Tamlık Bölgeleri ve Cisimler adı altında beş bölüm bulunmaktadır. Bu bölümlerde bazı önerme ve teoremler-hacmi fazla büyütmek için-ispatsız verilmiş, az sayıda özel cebirsal yapılara ise (abel gruplar, simetrik gruplar, sonlu cisimler vb.) yer verilmemiştir. Okuyucular, bu konularda temel referans kaynaklara başvurulabilir.

Bana sabır gösteren Aileme, kitabın yazılım ve basım aşamasında yardımlarını esirgemeyen Doç. Dr. Metin ORBAY'a ve Pegem A Yayıncılık Ailesine teşekkürlerimi sunarım.

2008, Amasya

Dr. M. Hikmet Develi

Değerli Eşim  
Ayşe Nur DEVELİ için,

## İÇİNDEKİLER

Semboller-Gösterimler

Kitap Hakkında

### I ÖN BİLGİLER

Önergeler

Küme Cebri

İkili Bağıntılar

Fonksiyonlar

İkili İşlemler

Tam Sayılarda Aritmetik

Modüler Aritmetik

### II GRUPLAR

Grup Tanımları ve Örnekleri

Alt Gruplar

Devirli Gruplar ve Devirli Alt Gruplar

Normal Alt Gruplar ve Bölüm Grupları

Grup Homomorfizmaları

### III HALKALAR

Halka Tanımları ve Örnekleri

Alt Halkalar, İdealler ve Bölüm Halkaları

Halka Homomorfizmaları

### IV TAMLIK BÖLGELERİ

Halkalarda Aritmetik

Gauss Tamlık Halkası

### V CİSİMLER

Cismin yapısı, Özellikleri ve Örnekleri

Asal ve Maksimal İdealler

Vektör Uzayları

Cisim Genişlemeleri

Kaynaklar

İndeks





## I. BÖLÜM

# ÖN BİLGİLER

*Bu bölümde; soyut matematik kitaplarında geniş biçimde yer alan önermeler, kümeler, bağıntı, fonksiyon, ikili işlem, tam sayılarda aritmetik ve modüler aritmetik konularının cebirde sıkça kullanılan kısımları kısaca özetlenecektir.*

### 1.1 ÖNERMELER

Bu kısımda; önermenin tanımı, örnekleri, önermeler arasında tanımlanan belli başlı işlemler ve teorem tanımları ile bunların ispat yöntemleri üzerinde durulacaktır.

**Tanım 1.1.1:** Doğru veya yanlış kesin bir hüküm (yargı) içeren ifadelere (bildirim cümlelerine) basit önerme denir ve  $p, q, r, \dots$  ile gösterilir.

Basit bir önermenin içerdği hüküm doğru ise önermenin doğruluk değeri 1, yanlış ise önermenin doğruluk değeri 0 denir ve sıra ile  $p \equiv 1$  ve  $p \equiv 0$  şeklinde gösterilir.

**Örnek 1.1.1:**  $p$ : Doğal sayılar kümesi sonsuzdur

önermesi için  $p \equiv 1$

**Örnek 1.1.2:**  $q$ : 1, bir asal sayıdır

önermesi için  $q \equiv 0$

**Örnek 1.1.3:**  $r$ : Bütün kenarları eşit olan bir geometrik şeklin bütün iç açıları da eşittir

önermesi için  $r \equiv 0$  (?)



**Örnek 1.1.4:** t: Geceler, gündüzlerden daha uzundur bir önerme olmakla beraber doğruluk değeri değişkendir (?)

**Örnek 1.1.5:** Bir gün 24 saattir. Beşiktaş, bugün galip gelebilir. Bu gün size geleceğiz. Sizleri cezalandırayım mı? gibi durum veya eylem bildiren, kesin hüküm içermeyen veya soru yöneltten cümleler birer önerme değildirler.

**Tanım 1.1.2:** Doğruluk değeri öznesinin değişimine bağlı olarak değişen önermelere açık önerme denir.

**Örnek 1.1.6:** Örnek 1.1.4 teki önerme bir açık önermedir.

**Örnek 1.1.7:**  $p(x): x|x \in \mathbb{R} \wedge x^2 \leq 1$

önermesi bir açık önerme olup;

$$x \in \mathbb{R} \wedge |x| > 1; p(x) \equiv 0$$

$$x \in \mathbb{R} \wedge -1 \leq x \leq 1; p(x) \equiv 1 \text{ dir.}$$

**Tanım 1.1.3:** Doğruluk değerleri daima eşit olan önermelere denk önermeler denir ve  $p \equiv q$  şeklinde yazılır.

**Örnek 1.1.8:** p: Üçgenin iç açıları toplamı  $180^\circ$  dir

$$q: \forall x \in \mathbb{Z}; |x| \geq 0$$

önermeleri için  $p \equiv q$  dur.

**Tanım 1.1.4:** Bir p önermesinin doğruluk değerini 1 iken 0 veya 0 iken 1 yapacak şekilde bir hüküm değişikliği sonunda elde edilen yeni önermeye p önermesinin olumsuzu (veya tersi) denir ve  $\bar{p}$  (veya  $p'$ ) ile gösterilir.

**Örnek 1.1.9:** p : Karın rengi beyazdır.

$$\bar{p} : \text{Karın rengi siyahtır.}$$

**Tanım 1.1.5:** En az iki basit önermenin aşağıdaki bağlaçlardan en az birisi ile birleştirilmesi sonucunda elde edilen önermeye birleşik önerme denir.



$\wedge$ (ve),  $\vee$ (veya)  
 $\Rightarrow$ (ise),  $\Leftrightarrow$ (ancak ve ancak)

Yukarıdaki birleşik önermelerin doğruluk tablosu aşağıdaki gibidir.

| p | q | $p \wedge q$ | $p \vee q$ | $p \Rightarrow q$ | $q \Rightarrow p$ | $p \Leftrightarrow q$ |
|---|---|--------------|------------|-------------------|-------------------|-----------------------|
| 1 | 1 | 1            | 1          | 1                 | 1                 | 1                     |
| 1 | 0 | 0            | 1          | 0                 | 1                 | 0                     |
| 0 | 1 | 0            | 1          | 1                 | 0                 | 0                     |
| 0 | 0 | 0            | 0          | 1                 | 1                 | 1                     |

**Tablo 1.1.1**

**Not 1.1.1**  $p \Rightarrow q$  ifadesi; p, q'yu gerektirir

$p \Leftarrow q$  ifadesi; q için p yeterlidir

$p \Leftrightarrow q$  ifadesi; p ile q birbirini gerektirir anlamını taşır.

Ayrıca;  $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (p \Leftarrow q)$  dir. (?)

**Tanım 1.1.6:**  $p \Rightarrow q$  gerektirmesinde p'ye hipotez, q'ya hüküm denir.

**Tanım 1.1.7:** Hipotezinin doğruluk değeri 1 olan gerektirmeye teorem denir.

**Tanım 1.1.8:**  $p \Rightarrow q$  bir teorem olmak üzere;

$\bar{p} \Rightarrow \bar{q}$  önermesine teoremin tersi

$q \Rightarrow p$  önermesine teoremin karşıtı

$\bar{q} \Rightarrow \bar{p}$  önermesine teoremin karşıt tersi denir.

**Önerme 1.1.1:**  $(p \Rightarrow q) \equiv (\bar{q} \Rightarrow \bar{p})$

$\equiv (\bar{p} \vee q)$  denklikleri her p ve q için doğrudur. (?)

**Sonuç 1.1.1:**  $p \Rightarrow q$  şeklindeki bir teoremin ispatı bazen çok zor olabilir.

Böyle durumlarda teorem yerine karşıt tersini ispatlamak yeterli olur. (!)



**Not 1.1.2:** Bu kitapta, mevcut bilgilerle kolayca ispatlanacak gerektirmeler önerme, ispatı daha zor olan ve kendinden sonra gelen birçok önermeye referans teşkil eden gerektirmeler ise teorem olarak isimlendirilecektir.

**Tanım 1.1.9:** Bir birleşik önerme, kendisini oluşturan basit önermelerin tüm doğruluk değerleri için daima doğru oluyor ise bu önermeye uyuşma veya totoloji, daima yanlış oluyor ise çelişme denir.

**Örnek 1.1.10:**  $p \vee \bar{p}$  nin bir totoloji,  $p \wedge \bar{p}$  nin bir çelişki olduğu doğruluk tabloları yapılarak kolayca görülür.(?)

**Örnek 1.1.11:**  $(p \Rightarrow q) \Rightarrow (\bar{q} \Rightarrow \bar{p})$  önermesinin totoloji olduğunu gösterelim

| p | q | $\bar{p}$ | $\bar{q}$ | $p \Rightarrow q$ | $\bar{q} \Rightarrow \bar{p}$ | $(p \Rightarrow q) \Rightarrow (\bar{q} \Rightarrow \bar{p})$ |
|---|---|-----------|-----------|-------------------|-------------------------------|---------------------------------------------------------------|
| 1 | 1 | 0         | 0         | 1                 | 1                             | 1                                                             |
| 1 | 0 | 0         | 1         | 0                 | 0                             | 1                                                             |
| 0 | 1 | 1         | 0         | 1                 | 1                             | 1                                                             |
| 0 | 0 | 1         | 1         | 1                 | 1                             | 1                                                             |

**Tablo 1.1.2**

**Not 1.1.3:** Tablodan  $(p \Rightarrow q) \equiv (\bar{q} \Rightarrow \bar{p})$  olduğu görülmektedir (!)

**Önerme 1.1.2:** p, q, r... birer önerme olmak üzere aşağıdakiler doğrudur.

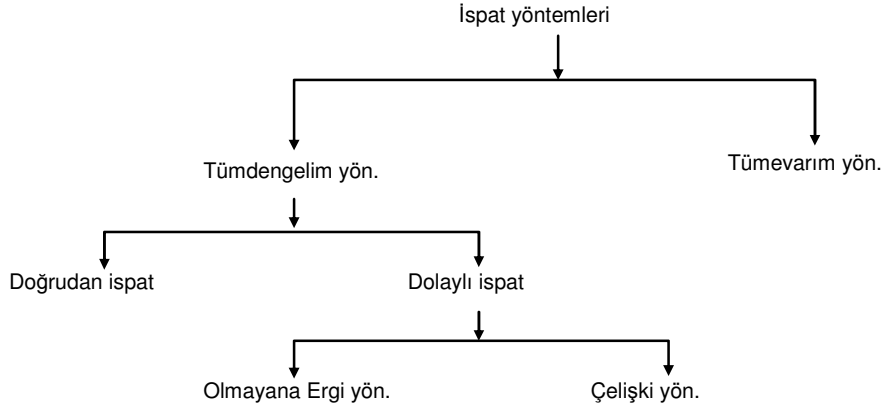
- a)  $p \vee p \equiv p$       ve       $p \wedge p \equiv p$       (tek kuvvet özelliği)
- b)  $p \vee 0 \equiv p$       ve       $p \wedge 0 \equiv 0$       (etkisiz ve yutan eleman özelliği)
- c)  $p \vee q \equiv q \vee p$       ve       $p \wedge q \equiv q \wedge p$       (değişme özelliği)
- d)  $p \vee (q \vee r) \equiv (p \vee q) \vee r$       ve       $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$       (birleşme özelliği)
- e)  $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$       ve       $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$       (dağılma özelliği)
- f)  $\overline{(p \vee q)} \equiv \bar{p} \wedge \bar{q}$       ve       $\overline{(p \wedge q)} \equiv \bar{p} \vee \bar{q}$       (De Morgan kuralları)

g)  $\overline{(\overline{p})} \equiv p$

h)  $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \equiv (p \Rightarrow r)$  (geçişme özelliği)

Cebirde teorem ispatları önemli bir yer tutar. Ayrıca matematiğin diğer alanlarındaki alışlagelmiş ispat yöntemleri dışında; matematiğe son yüzyıllarda girmiş olan değişik ispat yöntemlerine de sıkça başvurulur.

Şimdi belli başlı ispat yöntemlerini bir şema ile verip bunlardan özellikle cebirde kullanılan özel ispat yöntemlerinden Olmayana ergi, çelişki ve tümevarım yöntemleri ile ispata birer örnek verelim.



#### Örnek 1.1.12 (Olmayana ergi yöntemi):

Bu yöntem, özetle;  $(p \Rightarrow q) \equiv (\bar{q} \Rightarrow \bar{p})$  denkliğinden yararlanılarak;  $p \Rightarrow q$  teoremi yerine bunun karşıt tersi olan  $\bar{q} \Rightarrow \bar{p}$  teoremini ispatlama yoludur.

Şimdi; iki doğal sayının çarpımı bir çift doğal sayı ise; çarpanlardan en az birisi çift doğal sayıdır teoremini bu yöntemle ispatlayalım.

$p$ :  $a, b \in \mathbb{N}$  ve  $ab = c \in \mathbb{N}$  çift sayı

$q$ :  $a$  çift doğal sayı veya  $b$  çift doğal sayı

olmak üzere; teoremimiz  $p \Rightarrow q$  şeklindedir.

Bu durumda;

$\bar{p}$ :  $ab$  tek sayı

$\bar{q}$ :  $a$  tek ve  $b$  tek

olmak üzere  $\bar{q} \Rightarrow \bar{p}$  teoremini ispatlamak yeter. (?)



Gerçekten;

$$\begin{aligned} a = 2k + 1, b = 2t + 1 \ (k, t \in \mathbb{N}) &\Rightarrow ab = 4kt + 2(k + t) + 1 \\ &\Rightarrow ab = 2(2kt) + 2(k + t) + 1 \quad \text{bulunur.} \end{aligned}$$

$2kt = u$  ve  $k + t = v$  dersek  $u, v \in \mathbb{N}$  olmak üzere;

$$ab = 2(u + v) + 1 \quad \text{bulunur.} \quad \square$$

### Örnek 1.1.13 (Çelişki yöntemi):

Bu yöntem, özetle;  $(p \Rightarrow q) \equiv \bar{p} \vee q \equiv \overline{(p \wedge \bar{q})}$  denklighinden faydalanma yoludur.  $p \wedge \bar{q}$  nun bir çelişki olduğu gösterilirse bu sonuç,  $\overline{(p \wedge \bar{q})}$  nin dolayısı ile  $p \Rightarrow q$  nun bir totoloji olduğunu gösterir. (?)

Şimdi; tek iki doğal sayının çarpımı da tek sayıdır teoremini bu yöntemle ispatlayalım.

$$\begin{aligned} p : a, b \in \mathbb{N}; a \text{ tek} \wedge b \text{ tek} \\ q : ab \text{ tek} \end{aligned}$$

olmak üzere  $p \wedge \bar{q}$  önermesinin çelişki olduğunu göstermek yeter. (?)

Gerçekten;  $ab$  çift ise örnek 1.1.12 den  $a$  ve  $b$  den en az birisi çift olmak zorundadır. Bu ise  $p$  ile çelişir. Dolayısı ile  $p \wedge \bar{q}$  önermesi,  $p$  ve  $q$  nun bütün doğruluk değerleri için yanlıştır.  $\square$

**Not 1.1.4:**  $p \Leftrightarrow q$  şeklindeki teoremlerin ispatı ise  $p \Rightarrow q$  ve  $q \Rightarrow p$  teoremlerinin ispatlarının birleşimidir.

Bazı teoremlerin ispatında yukarda bahsedilen ispat yöntemleri ile sonuca ulaşmak oldukça zor olabilir. Özellikle değişkeni doğal sayı olan birtakım açık önermelerin ispatı için tümevarım yöntemi en uygun yoldur.

Doğal sayıların aksiyomatik inşasına dayanan bu yöntemi örneklemekten önce aşağıdaki tanımı ve önermeyi verelim.

**Tanım 1.1.10:** Aşağıdaki aksiyomları (kabulleri veya şartları) sağlayan  $\mathbb{N}$  kümesine doğal sayılar kümesi denir.

$$P_1 : 1 \in \mathbb{N}$$

$P_2 : \mathbb{N}$  den  $\mathbb{N} - \{1\}$  kümesine öyle birebir bir fonksiyon tanımlanabilir ki bu fonksiyon altında  $\forall n \in \mathbb{N}$  in görüntüsüne  $n$  nin ardışı denir ve bu eleman  $n^+$  ile gösterilir.

$P_3 : (\text{Tümevarım aksiyomu})$   $M, \mathbb{N}$  in 1i kapsayan bir alt kümesi olsun.  
 $n \in M$  olması  $n^+ \in M$  olmasını da gerektiriyor ise  $M = \mathbb{N}$  dir.

**Önerme 1.1.3 (Tümevarım prensibi):**  $\mathbb{N}$  doğal sayılar kümesi olmak üzere;

$$P(n) : \forall n \in \mathbb{N}; \begin{cases} \text{a) } n=1 \text{ için } P(1) \equiv 1 \\ \text{b) bir } n \in \mathbb{N} \text{ için } P(n) \equiv 1 \text{ olması } P(n^+) \equiv 1 \text{ olmasını} \end{cases}$$

gerektiriyor ise  $\forall n \in \mathbb{N}; P(n) \equiv 1$  dir.

**İspat:**  $P(n) \equiv 1$  şartını sağlayan  $n \in \mathbb{N}$  lerin kümesi  $M$  olsun.

$$1 \in M \text{ dir. } (?)$$

Ayrıca bir  $n \in M$  için  $n^+ \in M$  olacağından  $M = \mathbb{N}$  dir. (?)

**Örnek 1.1.14:**

$$P(n) : \forall n \in \mathbb{N}; \sum_{k=1}^n k = \frac{n(n+1)}{2} \text{ dir}$$

**İspat:**  $P(1) : \sum_{k=1}^1 k = 1 - \frac{1(1+1)}{2} \Rightarrow p(1) \equiv 1$  dir.

$$P(n) : \sum_{k=1}^n k = \frac{n(n+1)}{2} \Rightarrow p(n) \equiv 1 \text{ olsun.}$$

$$P(n+1) : \sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2} \Rightarrow p(n+1) \equiv 1 \text{ olduğu } P(n) \text{ in her iki}$$

yanına  $n+1$  eklemekle kolayca görülür. (?)

**Not 1.1.5:** Bazen bir  $P(n)$  açık önermesi  $n=1$  için doğru olmadığı gibi sonlu ilk  $s-1$  adımda yanlış  $s$ -yincide doğru olabilir. Bu durumda;  
 $P(s) \equiv 1$  ve bir  $n > s$  için  $P(n) \equiv 1$  iken  $P(n+1) \equiv 1$  olduğunu göstermek yeter.

$$P(n) : 2^n < n! \quad \text{önermesi bu durumda bir örnektir. } (?)$$



## 1.2 KÜME CEBRİ

Küme tanımları, kümelerde birleşim, kesişim, fark, kapsama gibi temel işlemler okuyucu tarafından iyi bilinmektedir. Bu kısımda sadece küme cebrinin önermelere dayalı gösterim ve ispatlarından kitabi ilgilendirenlere yer verilecektir.

**Tanım 1.2.1:** E evrensel küme, A bir küme olsun.

$$\bar{A} = \{a \in E \mid a \notin A\}$$

kümesine A'nın tümleyeni denir.

**Sonuç 1.2.1:**  $\bar{\bar{A}} = A$  dır (E / A = E - A, E nin A 'dan farkı)

**Sonuç 1.2.2:**  $a \in A$  olması p önermesi ise  $a \in \bar{A}$  ( $a \notin A$ ) olması  $\bar{p}$  önermesidir. (?)

**Önerme 1.2.1:** A ile B, E'nin iki alt kümesi ise, aşağıdakiler doğrudur.

- a)  $A \cup A = A$  ve  $\rightarrow A \cap A = A$  (tek kuvvet özelliği)
- b)  $A \cup \emptyset = A$  ve  $\rightarrow A \cap \emptyset = \emptyset$
- c)  $A \cup E = E$  ve  $\rightarrow A \cap E = A$
- d)  $A \cup B = B \cup A$  ve  $\rightarrow A \cap B = B \cap A$  (değişme özelliği)
- e)  $A \subset A \cup B, B \subset A \cup B \leftarrow$  ve  $\leftarrow A \cap B \subset A, A \cap B \subset B$
- f)  $A \subset B \Leftrightarrow A \cup B = B \leftarrow$  ve  $\leftarrow A \subset B \Leftrightarrow A \cap B = A$
- g)  $A = B \Leftrightarrow A \subset B \wedge B \subset A$

**Önerme 1.2.2:** Her A kümesi için aşağıdakiler doğrudur.

- a)  $A \cup \bar{A} = E$
- b)  $A \cap \bar{A} = \emptyset$
- c)  $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$
- d)  $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$

**İspat:** Örnek olması bakımından d) yi farklı iki yoldan ispatlayalım.

**a) Elemanlarla ispat:**

$$\begin{aligned}
a \in \overline{(A \cap B)} &\Leftrightarrow a \notin (A \cap B) \\
&\Leftrightarrow \overline{(a \in A \wedge a \in B)} \\
&\Leftrightarrow a \notin A \vee a \notin B \\
&\Leftrightarrow a \in \bar{A} \vee a \in \bar{B} \\
&\Leftrightarrow a \in (\bar{A} \cup \bar{B})
\end{aligned}$$

**b) Önermelerle ispat:**

$p : a \in A$  ve  $q : a \in B$  olsun.

$\bar{p} : a \notin A$  ve  $\bar{q} : a \notin B$  olur.

Bu durumda;  $\overline{p \wedge q} \equiv \bar{p} \vee \bar{q}$  denklğini göstermek yeter (?) □

**Önerme 1.2.3:** A, B, C herhangi üç küme olmak üzere; aşağıdakiler doğrudur.

a)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

( $\cup$  in  $\cap$  üzerine soldan dağılımı)

b)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

( $\cap$  in  $\cup$  üzerine soldan dağılımı)

**İspat:** b) yi önermeler cebri ile ispatlayalım.

$p : a \in A$ ,  $q : a \in B$  ve  $r : a \in C$

önermeleri olmak üzere; yukarıdaki eşitliği ispatlamak için

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

denklğini ispatlamak yeter. (Önerme 1.1.2, e)) □

**Tanım 1.2.2:** Bir A kümesinin bütün alt kümelerini (A ve  $\emptyset$  aşık alt kümeleri dahil) eleman olarak kabul eden ve bunlardan başka elemanı da bulunmayan kümeye (kümeler kümesine) A'nın kuvvet kümesi denir ve bu küme  $P(A)$  ile gösterilir.

**Not 1.2.1:** A sonlu bir küme ve eleman sayısı (mertebesi)  $o(A) = n$  ise  $o(P(A)) = 2^n$  olduğunu biliyoruz (!)