Dr. Strauber Györgyi – Sóti Lászlóné

Számítástudomány alapjai I.

Tartalomjegyzék

Bevezetés ... 3
1. Halmazok, halmazműveletek ... 4
2. Ítéletek, ítéletkalkulus ... 10
3. Relációk, függvények ... 16
4. A számfogalom bővítése ... 25
A természetes számok bevezetése ... 25
A számfogalom bővítése ... 26
5. Halmazok számossága ... 30
6. Algebrai struktúrák ... 34
7. Boole algebra ... 37
8. Kódelmélet ... 41
Információ, információs csatorna ... 41
Kódolás, dekódolás ... 42
Optimális kódok ... 43
Hibajavító kódolás ... 44
Irodalom ... 49

Bevezetés

A Számítástudomány alapjai I. tantárgy a számítástechnika matematikai alapjaiba nyújt betekintést.
Az előadás két nagy témakört ölel fel.
Az első témakör megismerteti a hallgatót a halmazok, ítéletek, relációk, függvények alapvető fogalmaival, tételeivel. Betekintést ad a számelmélet alapjaiba, definiálja a különböző algebrai struktúrákat, azon belül részletesebben foglalkozik a Boole-algebrákkal. Röviden érinti a kódelmélet, azon belül a zajmentes- és zajos csatornák, az optimális- és hibajavító kódolás alapelemeit.
A második témakör a vektoralgebra, lineáris algebra, lineáris egyenletrendszerek témaköre.

Jelen jegyzet az 1. témakör anyagát öleli fel (a 2. témakörrel külön jegyzet foglalkozik). Minden fejezet tartalmazza az alapvető fogalmak definiálását, a tárgyhoz kapcsolódó legfontosabb tételek kimondását, néhol bizonyítását. Az elméleti anyagot példákkal illusztrálja.
A jegyzethez külön kötetben példatár is kapcsolódik.

1. Halmazok, halmazműveletek

Ebben a fejezetben halmazokkal és a rajtuk értelmezett műveletekkel foglalkozunk.

A halmaz fogalma: Halmaznak nevezzük egy adott tulajdonság alapján összegyűjtött dolgok, fogalmak, objektumok összességét. A halmazba sorolt dolgokat, fogalmakat, objektumokat a halmaz elemeinek nevezzük.
A halmaz fogalmát ennél pontosabban nem definiáljuk, más matematikai objektumokkal nem írjuk le, **definiálatlan alapfogalom**ként fogadjuk el.

Megjegyzés: Fontos, hogy a halmaz elemei egyértelműen meghatározzák a halmazt, ugyanúgy, mint az a tulajdonság, amely alapján a halmazelemeket kiválasztottuk.

Jelölés: $X = \{ x \mid T(x)\}$, ahol

X a halmaz, amely azon x elemekből áll, melyekre érvényes a T(x) tulajdonság.

A halmazelemek jelölése: $x \in X$.

Példa: $X = \{x \mid x>0$ és x racionális szám$\}$,

azaz X halmaz a pozitív racionális számok halmaza.

Megjegyzés: Véges számú elemet tartalmazó halmazok megadhatók elemeik felsorolásával is.

Példa: $Y = \{1,2,3\}$.

Definíció: Két halmaz akkor és csak akkor **egyenlő**, ha azonosak az elemeik.

Megjegyzés: A fenti definíció azt jelenti, hogy a halmazelemek tulajdonságait többféleképpen is megfogalmazhatjuk, az elemeket többféleképpen is leírhatjuk, ez nem befolyásolja a halmazok egyezőségét.

Példa: $X := \{x \mid (x+1)*(x-1) = 0$ és x racionális szám $\}$,

$Y := \{-1, 1\}$.

Ekkor X = Y, azaz a két halmaz egyenlő.

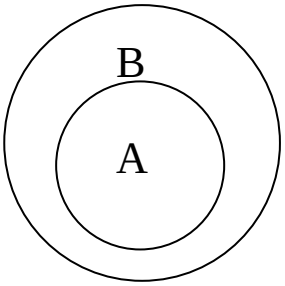
Definíció: **Üres halmaz** az a halmaz, amelynek nincs eleme.

Jelölés: Ø.

Definíció: Az A halmaz a B halmaznak **részhalmaza,** ha A minden eleme egyben B eleme is.

Jelölés: $A \subseteq B$

Ábrázolás (Venn-diagrammal, ld. 1.1 ábra):

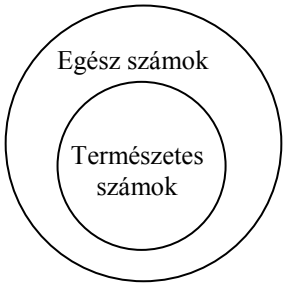


1.1.ábra

Definíció: Az A halmaz a B **valódi részhalmaza**, ha $A \subseteq B$ és A nem egyenlő B-vel, azaz B-nek létezik olyan eleme, amely A-nak nem eleme.

Jelölés: $A \subset B$

Példa:



1.2. ábra

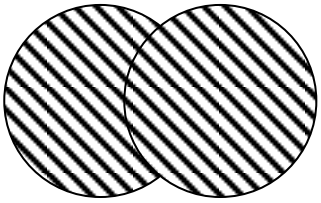
A továbbiakban a halmazokon értelmezett műveleteket és azok tulajdonságait tekintjük át. A halmazok műveletei: unió, metszet, különbség, szimmetrikus differencia, komplementer-képzés.

Definíció: A és B halmazok **egyesítése(uniója)** azon elemek összessége, melyek A és B halmazok legalább egyikének elemei.

Jelölés: $A \cup B$

Megjegyzés: A fentiek alapján $A \cup B = \{x \mid x \in A \text{ vagy } x \in B\}$.

Ábrázolás (Venn-diagrammal, ld. 1.3. ábra):



1.3. ábra

Az unió művelet tulajdonságai:

$A \cup B = B \cup A$, azaz az unió művelete **kommutatív** művelet.

$A \cup (B \cup C) = (A \cup B) \cup C$, azaz az unió művelete **asszociatív** művelet.

$A \cup A = A$,

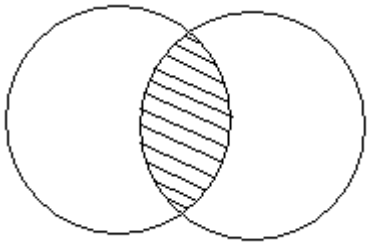
$A \cup \emptyset = A$ azaz az üres halmaz **nullelem**ként viselkedik (hasonlóan a 0 számhoz a valós számok között).

Definíció: Az A és B halmazok **metszete** azon elemek összessége, melyek A és B halmazok mindegyeikének elemei.

Jelölés: $A \cap B$

Megjegyzés: Azaz $A \cap B = \{x \mid x \in A \text{ és } x \in B\}$.

Ábrázolás (Venn-diagrammal, ld. 1.4. ábra):



1.4. ábra

A metszet művelet tulajdonságai:

$A \cap B = B \cap A$ azaz a metszet művelet **kommutatív** művelet.

$A \cap (B \cap C) = (A \cap B) \cap C$ azaz a metszet művelet **asszociatív** művelet.

$A \cap A = A$,

$A \cap \emptyset = \emptyset$.

Definíció: A és B **diszjunkt halmazok**, ha metszetük az üres halmaz.

A halmazok metszetére és uniójára vonatkozóan igazak a **disztributív törvények:**
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Megjegyzés: Látható, hogy a fenti azonosságokban a metszet és az unió szerepe felcserélhető (a második azonosságban az első azonosság metszet művelete helyére unió, az unió művelet helyére metszet műveletet írtunk), azaz a metszet és az unió **duális** műveletek.

Megjegyzés: Az unió és a metszetképzés kiterjesztése több halmazra:

Legyen A_γ halmazok sokasága, ahol γ tetszőleges Γ halmazbeli elem (γ-t indexnek, Γ -t pedig indexhalmaznak nevezzük). Ekkor

az A_γ halmazok **egyesítése** azon elemek összessége, melyek legalább egy A_γ halmaznak elemei, azaz

$$\bigcup_{\gamma \in \Gamma} A_\gamma = \{ x \mid \text{létezik olyan } A_\gamma \text{ halmaz, amelyre } x \in A_\gamma \},$$ és

Az A_γ halmazok **metszete** azon elemek összessége, melyek minden A_γ halmaznak elemei, azaz

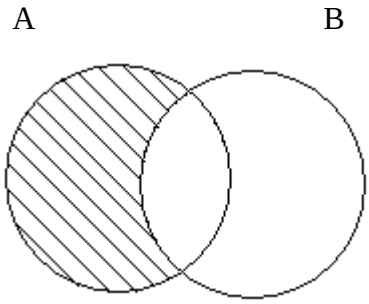
$$\bigcap_{\gamma \in \Gamma} A_\gamma = \{ x \mid x \in A_\gamma \text{ minden } \gamma \in \Gamma \text{ esetén} \}.$$

Definíció: Az A és B halmazok **különbség**e, az A halmaz azon elemeinek összessége, melyek nem elemei B-nek.

Jelölés: $A \setminus B$

Megjegyzés: Azaz $A \setminus B = \{x \mid x \in A \text{ és } x \notin B\}$

Ábrázolás (Venn-diagrammal, ld. 1.5. ábra):



1.5. ábra

A különbség művelet tulajdonságai:

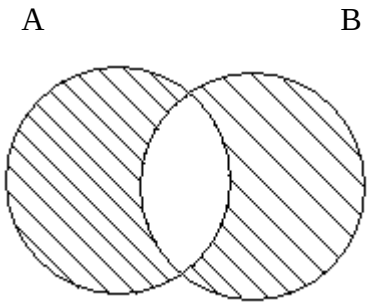
$A \setminus \emptyset = A$,
$\emptyset \setminus A = \emptyset$,
$A \setminus A = \emptyset$,
$(A \setminus B) \cap (B \setminus A) = \emptyset$,
$(A \setminus B) \cup B = A \cup B$.

Definíció: Az A és B halmazok **szimmetrikus differenciája** azon elemek összessége, melyek A és B halmazok közül pontosan az egyiknek elemei.

Jelölés: $A \circ B$

Megjegyzés: Azaz A o B = { x | x ∈ A ∪ B és x ∉ A ∩ B}

Ábrázolás (Venn-diagrammal, ld. 1.6. ábra):



1.6. ábra

A szimmetrikus differencia művelet tulajdonságai:

A o A =Ø,

A o Ø = A,

A o B = B o A azaz a szimmetrikus differencia művelet **kommutatív** művelet,

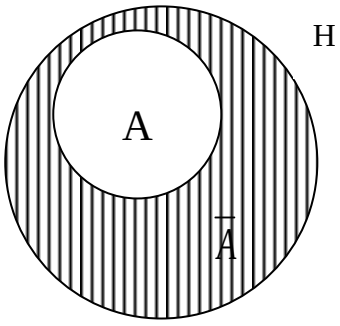
A o B = (A \ B) ∪ (B \ A).

Definíció: Legyen H tetszőleges halmaz, és legyen A ⊆ H (H-t **alaphalmaz**nak nevezzük). Ekkor A halmaz H halmazra vonatkoztatott **komplementer halmaza** a H azon elemeinek összessége, melyek nem elemei A-nak.

Jelölés: $\overline{A}$

Megjegyzés: Azaz $\overline{A}$ = {x | x ∈ H és x ∉ A}, vagyis x ∈ H \ A.

Ábrázolás (Venn-diagrammal, ld. 1.7. ábra):



1.7. ábra

A komplementer művelet tulajdonságai:

$A \cup \overline{A} = H$,

$A \cap \overline{A} = Ø$,

$\overline{\overline{A}} = A$,

$\overline{H} = Ø$,

$\overline{Ø} = H$.

Érvényesek a **De Morgan azonosság**ok:

$\overline{A \cup B} = \overline{A} \cap \overline{B}$ valamint

$\overline{A \cap B} = \overline{A} \cup \overline{B}$.

2. Ítéletek, ítéletkalkulus

Definíció: Az ítélet olyan kijelentés, melyről egyértelműen eldönthető, hogy igaz-e vagy hamis, és számunkra csupán ez a tulajdonsága érdekes.

Definíció: Az igaz vagy hamis tulajdonságokat **logikai értékek**nek nevezzük.

Jelölés:

↑	vagy	**i**	vagy	**igaz**	vagy	**T(rue)**	vagy	**1**
↓	vagy	**h**	vagy	**hamis**	vagy	**F(alse)**	vagy	**0**

Megjegyzés: Az ítéletek jelölésére latin betűket használunk és **ítéletváltozó**knak vagy **logikai változó**knak is nevezzük.

Definíció: **Elemi ítélet** (egyszerű ítélet) az olyan ítélet, mely nem bontható fel egyszerűbb ítéletekre.

Definíció: A nem elemi ítéleteket **összetett ítélet**nek nevezzük.

Definíció: Azokat az elemi ítéleteket, melyekből az összetett ítélet felépül, **az ítélet komponensei**nek nevezzük.

Példa.:

Esik az eső. → elemi ítélet

Esik az eső és süt a nap → összetett ítélet

⇓ ⇓

Komponensek

Definíció: **Ítéletművelet** (logikai művelet) az olyan művelet, melyet ítéleteken végrehajtva ismét ítéleteket kapunk eredményül, és a kapott ítélet logikai értékét a komponensek logikai értékei, valamint a végrehajtott műveletek egyértelműen meghatározzák.

Definíció: A logikának az az ága, mely az elemi ítéletek logikai értékét más ítéletek logikai értékétől függetlennek tekinti, az **ítéletkalkulus** (kijelentéskalkulus).

Definíció: Az ítéletműveletekkel összekapcsolt logikai változókat az ítéletkalkulus egy **formulá**jának nevezzük.

Definíció: Az ítéletkalkulus egy formuláját **kiértékel**jük, ha változói helyébe konkrét logikai értékeket helyettesítve meghatározzuk a formula logikai értékét.

Definíció: Az ítéletkalkulus két formulája **egyenértékű**, ha a bennük szereplő változók logikai értékeinek összes lehetséges helyettesítése esetén értékelésük azonos eredményre vezet.

A továbbiakban a legfontosabb ítéletműveleteket foglaljuk össze.

Definíció: Az **A** ítélet **negációja** az az ítélet, melynek logikai értéke akkor és csak akkor igaz, ha **A** értéke hamis.

Jelölése: $\neg \mathbf{A}$

Az ítéletműveleteket igazságtábla segítségével definiáljuk, melyben megadjuk művelet végeredményét, a műveletekben szereplő változók logikai értékeinek összes lehetséges helyettesítése esetén.

A negáció művelet igazságtáblája:

A	↑	↓
$\neg$**A**	↓	↑

A negáció művelet tulajdonságai:

$\neg\uparrow = \downarrow$,
$\neg\downarrow = \uparrow$,
$\neg(\neg A) = A$.

Definíció: Az **A** és **B** ítéletek **diszjunkció**ja az az ítélet, melynek értéke akkor és csak akkor hamis, ha mindkét komponensének értéke hamis.

Jelölése: $\mathbf{A} \vee \mathbf{B}$ (megengedő vagy)

Igazságtáblája:

A \ **B**	↑	↓
↑	↑	↑
↓	↑	↓

A diszjunkció művelet tulajdonságai:

$A \vee B = B \vee A$ azaz a diszjunkció művelet **kommutatív** művelet.
$(A \vee B) \vee C = A \vee (B \vee C)$ azaz a diszjunkció művelet **asszociatív** művelet.
$A \vee \downarrow = A$,
$A \vee \uparrow = \uparrow$,
$A \vee (\neg A) = \uparrow$,
$A \vee A = A$.

Definíció: A **kizáró vagy** művelettel összekapcsolt két ítéletből nyert összetett ítélet értéke akkor és csak akkor igaz, ha a komponensek értékének pontosan egyike igaz.

Jelölése: $\mathbf{A \bar{\vee} B}$

Igazságtáblája:

A \ B	↑	↓
↑	↓	↑
↓	↑	↓

Definíció: Az **A** és **B** ítéletek **konjunkció**ja az az ítélet, melynek értéke akkor és csak akkor igaz, ha mindkét komponensének értéke igaz.

Jelölése: $\mathbf{A \wedge B}$

Igazságtáblája:

A \ B	↑	↓
↑	↑	↓
↓	↓	↓

A konjunkció művelet tulajdonságai:

$A \wedge B = B \wedge A$ azaz a konjunkció művelet **kommutatív** művelet.
$(A \wedge B) \wedge C = A \wedge (B \wedge C)$ azaz a konjunkció művelet **asszociatív** művelet.
$A \wedge A = A$,
$A \wedge (\neg A) = \downarrow$,
$A \wedge \uparrow = A$,
$A \wedge \downarrow = \downarrow$.

Az ítéletek diszjunkciójára és konjunkciójára vonatkozóan igazak a **disztributív törvények:**

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C),$$
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C).$$

Megjegyzés: A negáció, a diszjunkció és a konjunkció műveletekkel minden további művelet kifejezhető. A logikai műveletek azon halmazát, melyek elemeivel bármely logikai kifejezés felírható, **funkcionálisan teljes** művelethalmaznak nevezzük.

Definíció: **A** előtagú és **B** utótagú **implikáció** az az ítélet, mely akkor és csak akkor hamis, ha előtagja igaz és utótagja hamis.

Jelölése: $\mathbf{A \rightarrow B}$

Igazságtáblája:

A \ B	↑	↓
↑	↑	↓
↓	↑	↑

Az implikáció művelet tulajdonságai:

$A \rightarrow B = (\neg A) \vee B$, azaz az implikáció művelete kifejezhető a negáció és a diszjunkció műveletekkel.

$A \rightarrow B = \neg(A \vee (\neg B))$,
$(\neg A) \rightarrow B = A \vee B$,
$\neg(A \rightarrow (\neg B)) = A \wedge B$.

Definíció: **A** és **B** **ekvivalenciá**ja az az ítélet, mely akkor és csak akkor igaz, ha komponensei logikai értékei egyenlőek.

Jelölése: $\mathbf{A \leftrightarrow B}$

Igazságtáblája:

A \ B	↑	↓
↑	↑	↓
↓	↓	↑

Az ekvivalencia művelet tulajdonságai:

$A \leftrightarrow B = B \leftrightarrow A$ azaz az ekvivalencia művelet **kommutatív** művelet.
$(A \leftrightarrow B) \leftrightarrow C = A \leftrightarrow (B \leftrightarrow C)$ azaz az ekvivalencia művelet **asszociatív** művelet.
$A \leftrightarrow B = (A \rightarrow B) \wedge (B \rightarrow A) = ((\neg A) \vee B) \wedge ((\neg B) \vee A)$,
azaz az ekvivalencia művelete kifejezhető a negáció, a konjunkció és a diszjunkció műveletekkel.
$A \leftrightarrow B = ((\neg A) \rightarrow B) \wedge ((\neg B) \rightarrow A)$.

Definíció: Az ítéletkalkulus egy formulája **tautológia** (azonosan igaz állítás), ha a formula logika értéke minden kiértékelés esetén igaz.

Példa.: $A \vee (\neg A) = \uparrow$,
$A \vee \uparrow = \uparrow$,
$(A \rightarrow \neg A) \rightarrow \neg A = \uparrow$.

Megjegyzés: Képezzük két formula ekvivalenciáját. Ha a kapott formula tautológia, akkor az eredeti két formula egyenértékű egymással.

Definíció: Az ítéletkalkulus egy formulája **ellentmondás** (azonosan hamis állítás), ha a formula logikai értéke minden kiértékelés esetén hamis.

Példa.: $A \wedge (\neg A) = \downarrow$,
$A \wedge \downarrow = \downarrow$,
$(\neg A \wedge B) \wedge A = \downarrow$.

Definíció: Az ítéletkalkulus egy $\mathbf{F_1}$ formulájának **következménye** egy $\mathbf{F_2}$ formula, ha nem lehet a formulákat úgy értékelni, hogy $\mathbf{F_1}$ értéke igaz, és $\mathbf{F_2}$ értéke hamis legyen.

Megjegyzés: Azt, hogy $\mathbf{F_1}$ formulának következménye-e $\mathbf{F_2}$ formula, eldönthetjük úgy, hogy megvizsgáljuk, az $\mathbf{F_1} \rightarrow \mathbf{F_2}$ implikáció tautológia-e.

Definíció: Az $\mathbf{F_{n+1}}$ formula az $\mathbf{F_1}$, $\mathbf{F_2}$, …, $\mathbf{F_n}$ ($n \geq 1$) formulák **következménye**, ha minden olyan értékelésük esetén, melyre $\mathbf{F_1}$, …, $\mathbf{F_n}$ értéke igaz, az $\mathbf{F_{n+1}}$ értéke is igaz.
Ebben az esetben $\mathbf{F_1}$, …, $\mathbf{F_n}$ -t **premisszá**nak (feltételnek), $\mathbf{F_{n+1}}$ -et **konklúzió**nak (következménynek) nevezzük.

Megjegyzés: $\mathbf{F_{n+1}}$ akkor és csak akkor következménye $\mathbf{F_1}$, $\mathbf{F_2}$, …, $\mathbf{F_n}$-nek, ha
$(\mathbf{F_1} \wedge \mathbf{F_2} \wedge \ldots \wedge \mathbf{F_n}) \rightarrow \mathbf{F_{n+1}}$ formula tautológia.

Definíció: Az $\mathbf{A_1}$, $\mathbf{A_2}$, …, $\mathbf{A_n}$ logikai változóknak és negáltjaiknak a konjunkcióját **elemi szorzat**oknak, diszjunkcióját **elemi összeg**eknek nevezzük.

Példa.: A, $\neg A$, $A \wedge \neg B$, $A \wedge B \wedge \neg B$ → elemi szorzatok,
A, $\neg A$, $A \vee \neg B$, $A \vee B \vee \neg B$ → elemi összegek.

Definíció: Azt a logikai kifejezést, mely elemi szorzatok összegéből (diszjunkciójából) áll, **diszjunktív normálforma**nak nevezzük.

Példa.: $(A \wedge \neg B) \vee (B \wedge C) \vee (\neg B \wedge C)$.

Megjegyzés: Minden logikai kifejezés felírható diszjunktív normálforma alakban.

Definíció: Az elemi összegek szorzatából (konjunkciójából) álló kifejezést **konjunktív normálforma**nak nevezzük.

Példa.: $(A \vee \neg B) \wedge (B \vee C) \wedge (\neg B \vee C)$.

Megjegyzés: Minden logikai kifejezés felírható konjunktív normálforma alakban.

Definíció: Az $\mathbf{A_1}$, …,$\mathbf{A_n}$ logikai változók azon elemi szorzatait, melyekben minden változó szerepel, de egyidejűleg nem tartalmazzák a változót és annak negáltját, **teljes (primitív) elemi szorzat**oknak nevezzük.

Példa.: A és B logikai változók esetén primitív elemi szorzatok a következők: $A \wedge B$, $A \wedge \neg B$, $\neg A \wedge B$, $\neg A \wedge \neg B$.

Definíció: Az $\mathbf{A_1}$,…, $\mathbf{A_n}$ logikai változók azon elemi összegeit, melyekben minden változó szerepel, de egyidejűleg nem tartalmazzák a változót és annak negáltját, **teljes (primitív) elemi összeg**eknek nevezzük.

Példa.: A és B logikai változók esetén primitív elemi összegek a következők:
$A \vee B$, $A \vee \neg B$, $\neg A \vee B$, $\neg A \vee \neg B$.

Definíció: Azokat a logikai kifejezéseket, melyek primitív elemi szorzatok összegeiből (diszjunkciójából) állnak, **perfekt (teljes) diszjunktív normálformá**nak nevezzük.

Megjegyzés: Minden logikai kifejezés felírható perfekt diszjunktív normálforma alakban.

Példa.: $A \rightarrow B = (A \wedge B) \vee (\neg A \wedge B) \vee (\neg A \wedge \neg B)$.

Definíció: A primitív elemi összegek konjunkciójából álló logikai kifejezéseket **perfekt (teljes) konjunktív normálformá**knak nevezzük.

Példa.: $(A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B) \wedge (\neg A \vee \neg B)$.

Megjegyzés: Minden logikai kifejezés felírható perfekt konjunktív normálforma alakban.

3. Relációk, függvények

Definíció: A D_1, D_2, …, D_n halmazok ($n \geq 2$) **direkt szorzatának (Descartes szorzatának)** nevezzük azon $(d_1, \ldots, d_n)$ alakú, rendezett n-esek halmazát, ahol $d_1 \in D_1$, $d_2 \in D_2$, …, $d_n \in D_n$ összfüggések mindegyike teljesül.

Jelölés: $D_1 \times D_2 \times \ldots \times D_n = \{(d_1, \ldots, d_n) \mid d_1 \in D_1 \wedge \ldots \wedge d_n \in D_n\}$

Megjegyzés: Ha $D_1 = D_2 = \ldots = D_n =: D$, akkor a jelölés: D^n, azaz a D halmaz n-edik hatványa.

Példa.: Legyen n:=2 $D_1 = D_2 := \boldsymbol{Z}$, ahol $\boldsymbol{Z}$ az egész számok halmaza.
Ekkor $D_1 \times D_2 = \boldsymbol{Z} \times \boldsymbol{Z} = \boldsymbol{Z}^2$ a rendezett egész számpárok összessége.

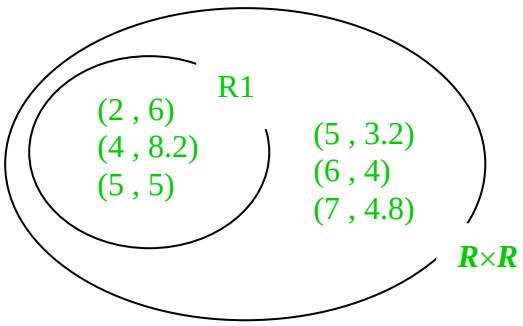
Definíció: Legyenek D_1 és D_2 tetszőleges halmazok. A $D_1 \times D_2$ direkt szorzat tetszőleges jól meghatározott részhalmazát **binér reláció**nak nevezzük.

Jelölés: $R \subseteq D_1 \times D_2$.

Definíció: Legyenek D_1, D_2, …, D_n tetszőleges halmazok.
A $D_1 \times D_2 \times \ldots \times D_n$ direkt szorzat részhalmazait $\{D_1, D_2, \ldots, D_n\}$ - beli n-változós relációknak nevezzük.

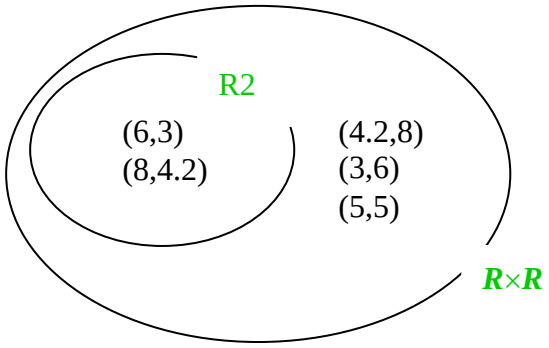
Definíció: Ha $D_1 = \ldots = D_n$, akkor **homogén reláció**ról beszélünk.

Példa 1: **R1** := $\{(a,b) \mid a \leq b\} \subseteq \boldsymbol{R} \times \boldsymbol{R}$, ahol $\boldsymbol{R}$ a valós számok halmaza.
Azaz R1 a valós számpároknak az a részhalmaza, ahol a számpár első eleme kisebb vagy egyenlő, mint a második.
Tehát pl. a (2 , 6) számpár eleme az R1 relációnak, amit így is jelölhetünk:
(2 , 6) ∈ R1, vagy 2 R1 6. A 3.1. ábra szemlélteti a valós számpárok azon részhalmazát, melyet az R1 reláció kijelöl.



3.1. ábra

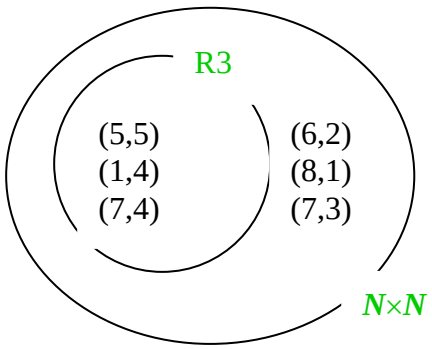
Példa 2: **R2** := {(a,b)| a > b} $\subseteq$ $\boldsymbol{R}\times\boldsymbol{R}$, ahol $\boldsymbol{R}$ a valós számok halmaza.
Azaz R2 a valós számpároknak az a részhalmaza, ahol a számpár első eleme nagyobb, mint a második.
A 3.2. ábra szemlélteti a valós számpárok azon részhalmazát, melyet az R2 reláció kijelöl.



3.2. ábra

Példa 3: **Definíció: a** kongruens **b**-vel modulo 3, ha 3-mal osztva **a** és **b** ugyanazt a maradékot adja.
Jelölés: a ≡ b (mod 3).
Példa: 1 ≡ 4 (mod 3), 5 ≡ 14 (mod 3).

R3 := {(a,b)| a ≡ b (mod 3)} $\subseteq \boldsymbol{N}\times\boldsymbol{N}$, ahol $\boldsymbol{N}$ a természetes számok halmaza.
Azaz R3 a természetes számpároknak az a részhalmaza, ahol a számpár első és második eleme kongruens egymással, modulo 3.
A 3.3. ábra szemlélteti a valós számpárok azon részhalmazát, melyet az R3 reláció kijelöl.



3.3. ábra

A továbbiakban a relációk legfontosabb tulajdonságaival foglalkozunk.

Definíció: Az $R \subseteq D \times D$ binér reláció **reflexív**, ha **a**R**a** (vagy más jelöléssel (**a**,**a**) $\in$ R) minden **a**$\in$D esetén. Azaz minden D- beli **a** –ra **a** önmagával relációban van, az (**a**,**a**) pár eleme a reláció által kijelölt részhalmaznak.

Definíció: Az $R \subseteq D \times D$ reláció **szimmetrikus**, ha minden **a**, **b** $\in$ D esetén **a**R**b** akkor és csak akkor, ha **b**R**a**, azaz az (**a**,**b**) pár pontosan akkor eleme a reláció által kijelölt részhalmaznak, ha a (**b**,**a**) pár is az.

Definíció: Az $R \subseteq D \times D$ reláció **tranzitív**, ha minden **a**, **b**, **c** $\in$ D esetén ha **a**R**b** és **b**R**c**, akkor **a**R**c**, azaz minden olyan esetben, ha fennáll az (**a**,**b**) $\in$ R reláció, valamint a (**b**,**c**) $\in$ R reláció, akkor kötelezően teljesülnie kell az (**a**,**c**) $\in$ R relációnak is.

Definíció: Az $R \subseteq D \times D$ reláció **antiszimmetrikus**, ha minden olyan **a**, **b** $\in$ D esetén, melyre az **a**R**b** reláció és a **b**R**a** reláció is fennáll, teljesül, hogy **a** = **b**. Azaz csak **a** = **b** esetben lehet az (**a**,**b**) pár és a (**b**,**a**) pár mindegyike eleme a reláció által kijelölt részhalmaznak.

Megjegyzés: A fenti definícióból látható, hogy - az egyenlőség relación kívül – ha egy reláció szimmetrikus, akkor nem lehet antiszimmetrikus.

Definíció: Az $R \subseteq D \times D$ reláció **dichotom**, ha minden **a, b** $\in$D esetén, ahol **a** $\neq$ **b,** vagy az **a**R**b** vagy a **b**R**a** reláció teljesül. A vagy itt **kizáró vagy** műveletet jelent, azaz az egyik reláció mindenképpen teljesül és mindenképpen csak egy reláció teljesül a kettő közül.

Megjegyzés: A fenti definícióból látható, hogy ha egy reláció szimmetrikus, akkor nem lehet dichotom.

Példa1: A fenti **R1** reláció **(** $\leq$)

reflexív,	ugyanis **a** $\leq$ **a** minden valós szám esetén.
nem szimmetrikus,	ugyanis abból, hogy **a** $\leq$ **b,** nem következik, hogy **b** $\leq$ **a** minden **a**, **b** valós szám esetén.
tranzitív,	ugyanis **a** $\leq$ **b** és **b** $\leq$ **c** esetén **a** $\leq$ **c** minden valós szám esetén teljesül.
antiszimmetrikus,	ugyanis ha **a** $\leq$ **b** és **b** $\leq$ **a,** akkor **a** = **b**.
dichotom,	ugyanis minden valós **a** $\neq$ **b** szám esetén vagy **a** $\leq$ **b,** vagy **b** $\leq$ **a** teljesül.

Példa2: A fenti **R3** reláció **(** $\equiv$, mod (3))

reflexív,	ugyanis **a** $\equiv$ **a** minden valós szám esetén (3-mal osztva ugyanazt a maradékot adja)
szimmetrikus,	ugyanis abból, hogy **a** $\equiv$ **b,** következik, hogy **b** $\equiv$ **a** minden **a**, **b** valós szám esetén.
tranzitív,	ugyanis **a** $\equiv$ **b** és **b** $\equiv$ **c** esetén **a** $\equiv$ **c** minden valós szám esetén teljesül.

nem antiszimmetrikus, ugyanis abból, hogy **a** ≡ **b** (és a szimmetria miatt így **b** ≡ **a),** nem következik, hogy **a** = **b**. (Ld. még azt a megjegyzést, hogy szimmetrikus reláció – az egyenlőség reláció kivételével – nem antiszimmetrikus.

nem dichotom, ugyanis szimmetrikus reláció nem lehet dichotom.

Példa3: Legyen **R4** a következő: **R4**={(a,b) | $a^2 + b^2 \leq 1$} ⊆ ***R***×***R*** (tehát azon valós számpárok tartozzanak a relációba, ahol a tagok négyzetösszege ≤ 1.) Ekkor **R4**

nem reflexív, ugyanis pl. nem igaz, hogy $2^2 + 2^2 \leq 1$.

szimmetrikus, ugyanis abból, hogy $\mathbf{a}^2 + \mathbf{b}^2 \leq 1$**,** következik, hogy $\mathbf{b}^2 + \mathbf{a}^2 \leq 1$ minden **a**, **b** valós szám esetén.

nem tranzitív: ugyanis pl. $0{,}9^{\,2} + 0{,}1^{\,2} \leq 1$ és $0{,}1^{\,2} + 0{,}8^{\,2} \leq 1$, de nem igaz, hogy $0{,}9^{\,2} + 0{,}8^{\,2} \leq 1$.

nem antiszimmetrikus, mivel szimmetrikus.

nem dichotom, mivel szimmetrikus.

Definíció: Ha egy reláció reflexív, szimmetrikus, és tranzitív, akkor **ekvivalencia-relációnak** nevezzük.

Példa: Az **R3** kongruenciareláció ekvivalenciareláció.

Definíció: Ha egy R reláció ekvivalenciareláció a D×D Descartes-szorzat halmazon, akkor **a**R**b** esetén azt is mondhatjuk, hogy **a ekvivalens b**-vel.

Tétel: Ha egy R ⊆ D × D reláció ekvivalencireláció, akkor D egymástól diszjunkt részhalmazoknak (Q_i , ahol i = 1, 2, …) az uniójára bomlik. Ezek a részhalmazok az R reláció **ekvivalencia-osztályai**. Azaz:

1.) $Q_1 \cup \ldots \cup Q_i \cup \ldots = D$,
2.) $Q_i \cap Q_j = \varnothing$, ha $i \neq j$,
3.) **a**, **b** ∈ D akkor és csak akkor tartozik ugyanabba a Q_i ekvivalenciaosztályba, ha az **a**R**b** reláció fennáll, azaz **a** ekvivalens **b**-vel.

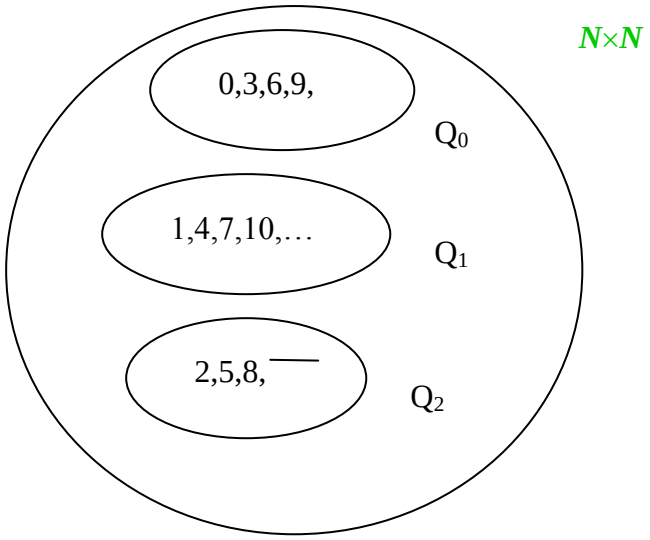
Példa: Az **R3** := {(a,b)| a ≡ b (mod 3)} ⊆ ***N***×***N*** kongruencia-reláció esetén

N = $Q_0 \cup Q_1 \cup Q_2$, ahol

- Q_0 azon természetes számok halmaza, melyek 0-t adnak maradékul 3-mal osztva,
- Q_1 azon természetes számok halmaza, melyek 1-et adnak maradékul 3-mal osztva,

- Q_2 azon természetes számok halmaza, melyek 2-t adnak maradékul 3-mal osztva.

Az ekvivalencia-osztályokat az alábbi 3.4. ábra szemlélteti:



3.4. ábra

Definíció: Ha R reflexív, antiszimmetrikus és tranzitív, akkor R **parciális rendezési** reláció vagy **részben rendezési** reláció.

Példa1: A részhalmaz-képzés ($\subseteq$) a halmazok esetén parciális rendezési reláció.

Példa2: Legyen a vizsgált reláció az oszthatósági kapcsolat a természetes számok halmazán, azaz **R** := { (**a**,**b**) | **a** osztója **b**-nek } $\subseteq N \times N$.
Ekkor belátható, hogy **R** parciális rendezési reláció.

Definíció: Ha R parciális rendezésű reláció és R dichotom, akkor R **teljes rendezési** reláció.

Példa: Az **R1** reláció **(** $\leq$) a valós számok halmazán teljes rendezési reláció.

Definíció: Legyen az $R \subseteq D \times D$ reláció egy parciális rendezési reláció. Ekkor azt mondjuk, hogy D **parciálisan rendezett halmaz** az R relációra vonatkozólag.

Definíció: Legyen az $R \subseteq D \times D$ reláció egy teljes rendezési reláció. Ekkor azt mondjuk, hogy D **teljesen rendezett halmaz** az R relációra vonatkozólag.

Definíció: A parciálisan rendezett D halmaz két eleme (**a** és **b**) **összehasonlítható**, ha az **a**R**b** vagy a **b**R**a** relációk valamelyike teljesül.

Definíció: Az R parciális rendezési relációval rendezett D halmaz **m** eleme **minimális elem**, ha nem létezik olyan **x** ∈ D elem, amely **x** elem **m**-től különböző (**x** ≠ **m**) és amelyre az **x**R**m** reláció fennállna.

Definíció: Az R parciális rendezési relációval rendezett D halmaz **M** eleme **maximális elem**, ha nem létezik olyan **x** ∈ D elem, amely **x** elem **M**-től különböző (**x** ≠ **M**) és amelyre az **M**R**x** reláció fennállna.

Példa1: Legyen R a fent vizsgált oszthatósági reláció a természetes számok halmazán.
Ekkor a minimális elem: **m** = 1,
maximális elem: nincs.

Példa2: Legyen R szintén az oszthatósági reláció, de most az 1-nél nagyobb természetes számok halmazán értelmezve, azaz
R := { (**a**,**b**) | **a** osztója **b**-nek } ⊆ $N_1 \times N_1$, ahol N_1 az 1-nél nagyobb természetes számok halmaza.
Ekkor minimális elem: minden prímszám,
maximális elem: nincs.

Példa3: Legyen R továbbra is az oszthatósági reláció, de most az egész számok halmazán (**Z**) értelmezve.
Ekkor minimális elem: nincs,
maximális elem: nincs.

Tétel: Egy teljesen rendezett halmaznak legfeljebb egy minimális (maximális) eleme lehet.

Megjegyzés: A tétel csak az egyértelműséget biztosítja, a létezést nem.

Definíció: Egy teljesen rendezett halmaz **jól rendezett**, ha minden nem üres részhalmazának van minimális eleme.

Definíció: Az R ⊆ $D_1 \times D_2$ bináris reláció **inverze** az $R^{-1} \subseteq D_2 \times D_1$ bináris reláció, ha minden (**a**,**b**) ∈ $D_1 \times D_2$ esetén **a**R**b** reláció akkor és csak akkor teljesül, ha a **b**R^{-1}**a** reláció is teljesül.

Példa1: A valós számok halmazán értelmezett ≤ reláció inverze a valós számok halmazán értelmezett ≥ reláció.

Példa2: Legyen D_1:= {1, 3, 5, 7} és legyen D_2:= {2, 3, 4, 5}.
Tartalmazza az **R** ⊆ $D_1 \times D_2$ reláció az alábbi 3 számpárt:
R := { (**1**, **5**), (**3**, **2**), (**7**, **5**)} ⊆ $D_1 \times D_2$.
Ekkor az **R** reláció $\mathbf{R^{-1}}$ inverze a következő:
$\mathbf{R^{-1}}$ = { (**5**, **1**), (**2**, **3**), (**5**, **7**)} ⊆ $D_2 \times D_1$.

Definíció: Az R ⊆ $D_1 \times D_2$ bináris reláció egy **a**∈D_1 elemre vonatkozó **metszet**ének nevezzük a D_2 halmaz azon **b** elemeinek összességét, amelyekre az **a**R**b** reláció teljesül.

Jelölés: R(a)

Megjegyzés: Azaz: $R(\mathbf{a}) = \{\mathbf{b} \mid \mathbf{b} \in D_2 \text{ és } \mathbf{aRb}\}$ minden $\mathbf{a} \in D_1$ esetén.

Példa1: Legyen $D_1 := D_2 := \boldsymbol{R}$ (ahol $\boldsymbol{R}$ a valós számok halmaza) és legyen a vizsgált reláció a következő:

$\mathbf{R1} = \{(a,b) \mid a = b^2\} \subseteq \boldsymbol{R} \times \boldsymbol{R}$.

Ekkor $R1(4) = \{+2,-2\}$, $R1(0) = \{0\}$, $R1(-4) = \emptyset$.

Példa2: Legyen $D_1 := D_2 := \boldsymbol{R}$ (ahol $\boldsymbol{R}$ a valós számok halmaza) és legyen a vizsgált reláció a következő:

$\mathbf{R2} = \{(a,b) \mid a^2 = b\} \subseteq \boldsymbol{R} \times \boldsymbol{R}$.

Ekkor $R1(4) = \{16\}$, $R1(0) = \{0\}$, $R1(-4) = \{16\}$.

Definíció: Az $R \subseteq D_1 \times D_2$ bináris relációt a D_1 halmazon értelmezett **függvény**nek nevezzük, ha $R(a)$ metszet egyelemű minden $a \in D_1$ esetén.

Példa1: A fent definiált $\mathbf{R1} = \{(a,b) \mid a = b^2\} \subseteq \boldsymbol{R} \times \boldsymbol{R}$ reláció nem függvény.

Ha **R1** relációt az $\boldsymbol{R}^+ \times \boldsymbol{R}^+$ Descartes-szorzaton definiáljuk, ahol $\boldsymbol{R}^+$ a pozitív valós számok halmaza, akkor az **R1** reláció függvény.

Példa2: A fent definiált $\mathbf{R2} = \{(a,b) \mid a^2 = b\} \subseteq \boldsymbol{R} \times \boldsymbol{R}$ reláció függvény.

Definíció: A függvény definíciójában szereplő D_1 halmaz a függvény **értelmezési tartomány**a.

Definíció: Az értelmezési tartomány összes elemére vonatkoztatott metszetek összessége, azaz $\bigcup_{a \in D_1} R(a) \subseteq D_2$ a függvény **értékkészlet**e.

Jelölés: $f: D_1 \to D_2$ függvény, ahol az R relációt a függvények esetében szokásosabb f (g,h,…p,q) betűkkel jelöljük.

Definíció: Az $f: D_1 \to D_2$ függvény esetén a D_1 halmaz tetszőleges $a \in D_1$ eleméhez tartozó $R(a) = b \in D_2$ elemet az a elem **képé**nek nevezzük.

Definíció: Az f: $D_1 \to D_2$ függvény **szurjektív**, ha D_2 minden eleme képelem, azaz minden $\bigcup_{a \in D_1} R(a) = D_2$.

Példa: Az $f(x)=x^2$ függvény szurjektív, ha f: $\boldsymbol{R} \to \boldsymbol{R}^{+,0}$ (ahol $\boldsymbol{R}^{+,0}$ a nemnegatív valós számok halmaza), de nem szurjektív, ha f: $\boldsymbol{R} \to \boldsymbol{R}$. (Ld. 3.5. ábra)

szurjektív nem szurjektív

3.5. ábra

Definíció: Az f: $D_1 \to D_2$ függvény **injektív**, ha D_1 különböző elemeinek különböző képek felelnek meg.

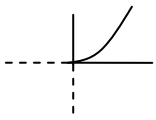
Példa: $f(x)=x^2$ függvény injektív, ha f: $\boldsymbol{R}^{+,0} \to \boldsymbol{R}$, de nem injektív, ha f: $\boldsymbol{R} \to \boldsymbol{R}$. (Ld. 3.6. ábra)

injektív nem injektív

3.6. ábra

Definíció: Az f: $D_1 \to D_2$ függvény **bijektív**, ha injektív és szurjektív.

Példa: Az $f(x)=x^2$ bijektív, ha f: $\boldsymbol{R}^{+,0} \to \boldsymbol{R}^{+,0}$. (Ld. 3.7. ábra)



bijektív

3.7. ábra

Tétel: Az f^-: $D_1 \to D_2$ függvény (reláció értelmében vett) inverze ($f^{-(-1)}$: $D_2 \to D_1$) akkor és csak akkor függvény, ha f bijektív.

Definíció: Az olyan függvényt, melynek értelmezési tartománya egy $I \neq \varnothing$ halmaz, értékkészlete pedig a logikai értékek halmaza ($\{\uparrow, \downarrow\}$), **logikai függvénynek** nevezzük.

Példa: Legyen I := ***N.***
$f_1(x) :=$ ↑, ha x prímszám, ↓ különben.
$f_2(x) :=$ ↑, ha x páros, ↓ különben.

Ekkor $f_3(x) = f_1(x) \wedge f_2(x)$ szintén logikai függvény, melyre
$f_3(x) :=$ ↑, ha x = 2, ↓ különben.

Definíció: Az **univerzális kvantifikáció** műveletét egy I halmazon értelmezett f (a) logikai függvényre a $\forall$ a f (a) a $\in$ I szimbólummal jelöljük és a művelet eredményét a következő módon definiáljuk:

$\forall$ a f (a) = ↑, ha f (a) = ↑ minden a $\in$ I, ↓ különben.

Definíció: Az **egzisztenciális kvantifikáció** műveletét egy I halmazon értelmezett f (a) logikai függvényre a $\exists$ a f (a) a $\in$ I szimbólummal jelöljük és a művelet eredményét a következő módon definiáljuk:

$\exists$ a f (a) = ↑, ha létezik olyan a $\in$ I , melyre f (a) = ↑ , ↓ különben.

Példa: Legyen I := **N.**
Ekkor $\forall x\,(x > 5) =$ ↓ és
$\exists x\,(x > 5) =$ ↓,

Definíció: Legyen ***A*** egy tetszőleges halmaz , és legyen f: $\boldsymbol{A \times A \to A}$ függvény. Ekkor f függvény egy **kétváltozós belső műveletet** értelmez az ***A*** halmazban.

Példa: Legyen ***A*** := ***R*** (a valós számok halmaza).
f (**a**, **b**) := **a** + **b** = **c** $\in$ ***R*** egy kétváltozós belső művelet a valós számok halmazán.
f (**a**, **b**) := **a** * **b** = **c** $\in$ ***R*** szintén kétváltozós belső művelet a valós számok halmazán.

Definíció: Legyen ***A*** egy tetszőleges halmaz. Ekkor egy tetszőleges
f: $\boldsymbol{A^n = A \times \ldots \times A \to A}$
függvényt az ***A*** halmazban értelmezett **n változós belső műveletnek** nevezzük ($n \geq 1$).

Definíció: Az ***A*** halmazban értelmezett f belső művelet **asszociatív** , ha
f (f (**a**, **b**) , **c**) = f (**a**, f (**b** , **c**)), minden **a**, **b**, **c** $\in$ ***A*** esetén.

Példa: A valós számok összeadása asszociatív művelet.

Definíció: Az ***A*** halmazon értelmezett f belső művelet **kommutatív** , ha
f (**a**, **b**) = f (**b** , **a**) , minden **a**, **b** $\in$ ***A*** esetén.

Példa: A természetes számok összeadása, szorzása kommutatív művelet, a hatványozás művelete nem kommutatív.

4. A számfogalom bővítése

A természetes számok bevezetése

Definíció: A **természetes számok** definiálása az úgynevezett **Peano axiómákkal** történik (Giuseppe Peano (1858 - 1932) olasz matematikus után):

1. Az **1** természetes szám.
2. Minden $\mathbf{n} \in \boldsymbol{N}$ természetes számhoz egyértelműen létezik egy $\mathbf{n'} \in \boldsymbol{N}$ természetes szám, az **n** közvetlen rákövetkezője.
3. $\mathbf{n'} \neq \mathbf{1}$, (azaz az **1** egyetlen természetes szám után sem következik).
4. Ha $\mathbf{m'} = \mathbf{n'}$, akkor $\mathbf{m} = \mathbf{n}$ (azaz minden természetes szám legfeljebb egy természetes szám után következhet).
5. A természetes számok minden olyan részhalmaza , amely tartalmazza az **1**-et, és minden **n** elemével együtt **n'**-t is, tartalmaz minden természetes számot (teljes indukció vagy matematikai indukció elve).

Megjegyzés: Ez utóbbi axióma adja a teljes indukciós bizonyítási módszer jogosságát, miszerint legyen $\mathbf{A_1}$, $\mathbf{A_2}$, … állítások megszámlálható sorozata és

1. lássuk be, hogy $\mathbf{A_1}$ igaz,
2. tegyük fel, hogy minden $\mathbf{n} \in \boldsymbol{N}$ esetén , ha $\mathbf{A_n}$ igaz , akkor $\mathbf{A_{n'}}$ is igaz.
3. Ekkor $\mathbf{A_n}$ igaz minden **n** természetes számra.

Megjegyzés: Tekintsük az **1, 1', (1')', ((1')')'**, …. számokból álló halmazt.
Ez tartalmazza **1**-et és ha tartalmazza **n** -t , akkor tartalmazza **n'** –t is.
Az 5. axióma miatt ekkor ez a halmaz tartalmaz minden természetes számot.
Azaz a természetes számok sorba rendezhetőek.

Definíció: Az **összeadás rekurzív definíciója** természetes számok esetén:

1. $\mathbf{n} + \mathbf{1} := \mathbf{n'}$ $\qquad \forall\, \mathbf{n} \in \boldsymbol{N}$
2. $\mathbf{n} + \mathbf{m'} := \mathbf{(n + m)'}$ $\qquad \forall\, \mathbf{n, m} \in \boldsymbol{N}$

Megjegyzés: Az 1. és 2. definíció valóban egyértelműen meghatározza **n, m** összegét minden $\forall\, \mathbf{n, m} \in \boldsymbol{N}$ tetszőleges számra, ugyanis
legyen $\mathbf{n} \in \boldsymbol{N}$ tetszőlegesen rögzített, és legyen $\mathbf{A_m}$ az az állítás, hogy $\mathbf{n} + \mathbf{m}$ összeg kiszámítható. Ekkor $\mathbf{A_1}$ igaz 1. definíció miatt. Ha $\mathbf{A_m}$ igaz, akkor 2. definíció miatt $\mathbf{A_{m'}}$ is igaz, azaz az 5. Peano-féle axióma miatt $\mathbf{A_m}$ igaz $\forall\, \mathbf{m} \in \boldsymbol{N}$ esetén.

Definíció: Az **szorzás rekurzív definíciója** természetes számok esetén:

$\forall\, \mathbf{n, m} \in \boldsymbol{N}$ természetes számhoz hozzárendelünk egy $\mathbf{m} * \mathbf{n}$ természetes számot a következő módon:

1. $\mathbf{m * 1 := m}$ $\quad \forall \mathbf{m} \in \boldsymbol{N}$
2. $\mathbf{m * n' := m * n + m}$ $\quad \forall \mathbf{n, m} \in \boldsymbol{N}$

Megjegyzés: Belátható , hogy az így definiált összeadás és szorzás asszociatív és kommutatív, továbbá teljesül a disztributivitás.

Definíció: Bevezethető a <, > **reláció** a köv. módon:
Azt mondjuk, hogy **m < n (m > n)**, ha az **1, 1', (1')', ((1')')'**, …. sorozatban **n** később következik (korábban következik) **m**-nél.

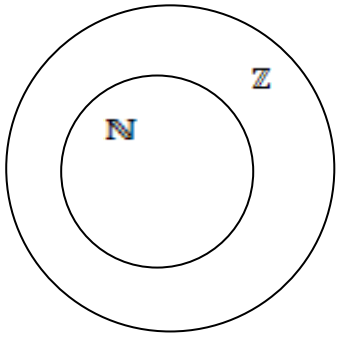
A számfogalom bővítése

Definíció: A természetes számok halmazán az

$$\mathbf{a + x = b}$$

egyenlet nem oldható meg tetszőleges $\mathbf{a, b} \in \boldsymbol{N}$ esetén.

A természetes számok halmazának kibővítése olyan módon, hogy a fenti egyenlet minden $\mathbf{a, b} \in \boldsymbol{N}$ esetén megoldható legyen adja az **egész számok (*Z*)** halmazát. (Ld. 4.1. ábra)



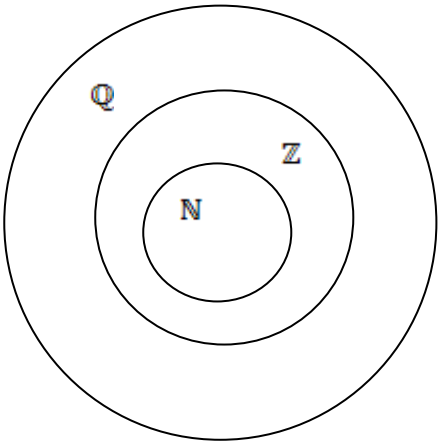
4.1.ábra

Definíció: Az egész számok halmazán a szorzás művelete, az

$$\mathbf{a * x = b}$$

egyenlet nem oldható meg tetszőleges $\mathbf{a, b} \in \boldsymbol{Z}$ esetén ($\mathbf{a} \neq \mathbf{0}$).

Az egész számok halmazának kibővítése olyan módon, hogy a fenti egyenlet minden $\mathbf{a, b} \in \boldsymbol{Z}$ ($\mathbf{a} \neq \mathbf{0}$) esetén megoldható legyen adja az **racionális számok (*Q*)** halmazát. (Ld. 4.2. ábra)



4.2. ábra

Megjegyzés: A racionális számok halmazán az alábbi egyenlet:

$$x^n = c$$

nem oldható meg tetszőleges $n \in N$, $c \in Q$, $c > 0$ esetén.

Definíció: A valós számok bevezetése axiomatikus úton történik:
Legyen a valós számok halmaza (R) egy olyan halmaz, melyre definiálva van:

1. két művelet, az összeadás (+) és a szorzás (*), valamint
2. egy rendezési reláció (≤),

a következő tulajdonságokkal:

I. Az R halmaz **test** (ld. majd algebrai struktúrák), azaz:

1. $x + (y + z) = (x + y) + z$ minden $x, y, z \in R$ esetén, azaz az összeadás asszociatív,
2. $x + y = y + x$ minden $x, y \in R$ esetén, azaz az összeadás kommutatív,
3. Létezik egy olyan $0 \in R$ elem, hogy $0 + x = x$ minden $x \in R$ esetén, azaz létezik nullelem,
4. Minden $x \in R$ esetén létezik egyértelműen egy olyan $-x \in R$, melyre $x + (-x) = 0$, azaz létezik inverzelem,
5. $x * (y * z) = (x * y) * z$ minden $x, y, z \in R$ esetén, azaz a szorzás asszociatív,
6. $x * y = y * x$ minden $x, y \in R$ esetén, azaz a szorzás kommutatív,
7. Létezik egy olyan $1 \in R$ elem, hogy $1 \neq 0$ és $1 * x = x$ minden $x \in R$ esetén, azaz létezik egységelem,
8. Minden $x \in R$ esetén, ha $x \neq 0$, létezik egyértelműen egy olyan $x^{-1} (= 1/x) \in R$, melyre $x * (x^{-1}) = 1$, azaz a 0 kivételével létezik inverzelem a szorzásra vonatkozóan,
9. $x * (y + z) = (x * y) + (x * z)$ minden $x, y, z \in R$ esetén, azaz érvényesül a disztributivitás.

II. Az ***R*** halmaz **rendezett test,** azaz definiált rajta a **≤** teljes rendezési reláció az alábbi tulajdonságokkal:

1. $\mathbf{x} \le \mathbf{x}$ minden $\mathbf{x} \in \boldsymbol{R}$ esetén, azaz a reláció reflexív,
2. $\mathbf{x} \le \mathbf{y}$ és $\mathbf{y} \le \mathbf{z} \Rightarrow \mathbf{x} \le \mathbf{z}$ minden $\mathbf{x, y, z} \in \boldsymbol{R}$ esetén, azaz a reláció tranzitív,
3. $\mathbf{x} \le \mathbf{y}$ és $\mathbf{y} \le \mathbf{x} \Rightarrow \mathbf{x} = \mathbf{y}$ minden $\mathbf{x, y} \in \boldsymbol{R}$ esetén, azaz a reláció antiszimmetrikus,
4. vagy $\mathbf{x} \le \mathbf{y}$ vagy $\mathbf{y} \le \mathbf{x}$ teljesül (kizáró vagy értelmében) minden $\mathbf{x, y} \in \boldsymbol{R}, \mathbf{x} \ne \mathbf{y}$ esetén, azaz a reláció dichotom,
5. $\mathbf{x} \le \mathbf{y} \Rightarrow \mathbf{x} + \mathbf{z} \le \mathbf{y} + \mathbf{z}$ minden $\mathbf{x, y, z} \in \boldsymbol{R}$ esetén,
6. $\mathbf{0} \le \mathbf{x}$ és $\mathbf{0} \le \mathbf{y} \Rightarrow \mathbf{0} \le \mathbf{x} * \mathbf{y}$ minden $\mathbf{x, y} \in \boldsymbol{R}$ esetén.

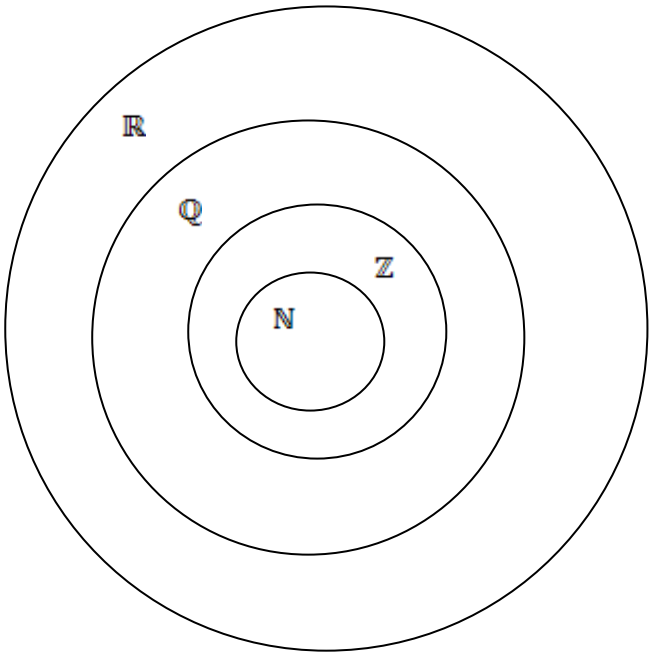
III. Az ***R*** halmaz **rendezése archimedesi,** azaz teljesül az alábbi archimedesi axióma:

Minden $\mathbf{0} \le \mathbf{x}$ és $\mathbf{x} \ne \mathbf{0}$ (azaz $\mathbf{0} < \mathbf{x}$) és minden $\mathbf{0} \le \mathbf{y}$ számpárra, ahol $\mathbf{x, y} \in \boldsymbol{R}$, létezik egy olyan $\mathbf{n} \in \boldsymbol{N}$ természetes szám, amelyikre teljesül, hogy $\mathbf{y} \le \mathbf{n} * \mathbf{x}$ (ahol $\mathbf{n} * \mathbf{x}$ nem más, mint **n** db **x** összege) .

IV. Teljesül az alábbi **intervallum-skatulyázási** axióma:

Legyen $[\ \mathbf{a}_n, \mathbf{b}_n\ ]$ (n = 1, 2, …), intervallumok egymásba ágyazott (skatulyázott) tetszőleges sorozata, azaz $\mathbf{a}_n \le \mathbf{a}_{n+1}$ és $\mathbf{b}_{n+1} \le \mathbf{b}_n$ (n = 1, 2, …). Ekkor ezen egymásba skatulyázott intervallumok metszete nem az üres halmaz.

Az így definiált (a racionális számok halmazánál bővebb) számhalmaz a valós számok halmazát ld.a 4.3. ábrán:



4.3.ábra

Megjegyzés: A valós számok halmazán az alábbi egyenlet:

$$x^n = c$$

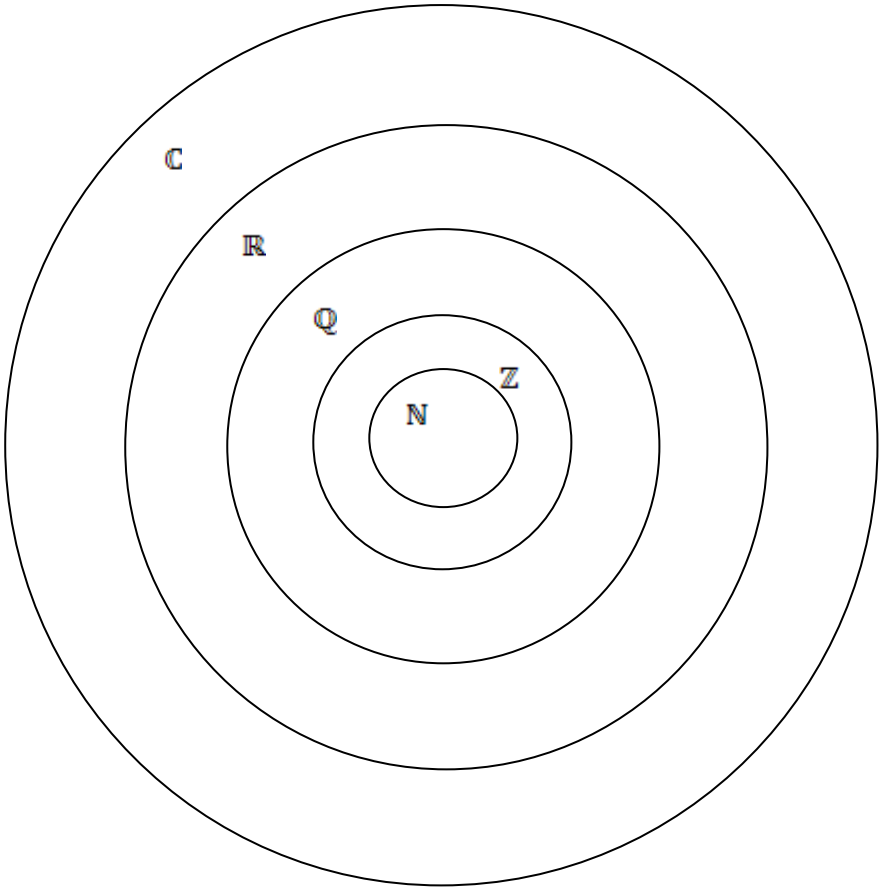
már megoldható tetszőleges $n \in N$, $c \in Q$, $c > 0$ esetén.

Definíció: A valós számok halmazán az alábbi egyenlet:

$$x^2 + 1 = 0$$

nem oldható meg.

A valós számok halmazának kibővítése olyan módon, hogy a fenti egyenlet megoldható legyen, adja a **komplex számok (*C*)** halmazát (ld. 4.4. ábra).



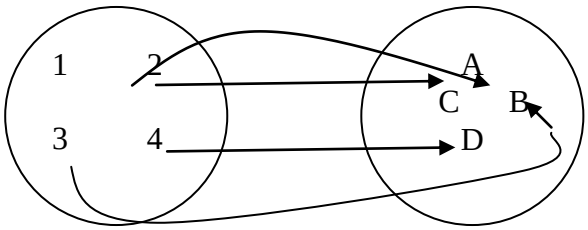
4.3.1. ábra

5. Halmazok számossága

Definíció: A és B halmazok **egyenlő számosságúak (**más szóval **ekvivalensek)**, ha elemeik között kölcsönösen egyértelmű leképezés létesíthető.

Jelölés: $A \sim B$.

Példa1: Legyen $D_1 := \{1, 2, 3, 4\}$ és $D_2 := \{A, B, C, D\}$. Ekkor D_1 egyenlő számosságú D_2 –vel. Egy lehetséges kölcsönösen egyértelmű leképezést szemléltet az alábbi 5.1. ábra.



5.1.ábra

Megjegyzés: Véges halmazok egyenlő számosságúak, ha elemszámuk megegyezik.

Példa2: A pozitív egész számok halmaza és a pozitív páros egész számok halmaza egyenlő számosságú. Ugyanis a két halmaz között létesíthető kölcsönösen egyértelmű leképezés, melyet az alábbi 5.2. ábra szemléltet:

1	2	3	…	n	…
↓	↓	↓		↓	
2	4	6	…	2n	…

5.2. ábra

Definíció: Az olyan halmazt, mely egyenlő számosságú a természetes számok halmazával, **megszámlálható számosságú halmaz**nak nevezzük.

Jelölés: χ_0 (alef null) a megszámlálható halmazok számossága.

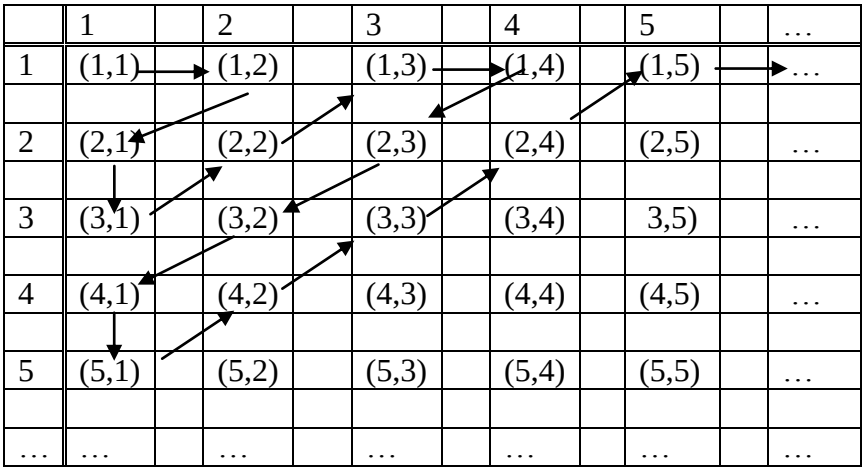
Tétel: Egy végtelen halmaz akkor és csak akkor megszámlálható számosságú, ha elemei sorba rendezhetők.

Tétel: Megszámlálható számosságú halmaz minden részhalmaza véges vagy megszámlálható számosságú.

Tétel: Véges vagy megszámlálhatóan sok véges vagy megszámlálható számosságú halmaz uniója is véges vagy megszámlálható számosságú.

Tétel: A természetes számokból képezhető rendezett számpárok halmaza megszámlálható számosságú.

Bizonyítás: A fenti tétel alapján elég belátni, hogy a természetes számokból képezhető rendezett számpárok sorba rendezhetők. Egy lehetséges sorba rendezést (ahol minden számpár helye pontosan ismert, meg lehet mondani az őt megelőző és az őt követő számpárt) mutat az alábbi 5.3. ábra:



5.3.ábra

Következtetés: A racionális számok halmaza megszámlálható.

Bizonyítás: Tekintsük a fenti számpárok első tagját mint a racionális szám számlálóját, második tagját mint a racionális szám nevezőjét.

Tétel: A valós számok halmaza (***R***) nem megszámlálható.

Bizonyítás: Belátjuk, hogy $0 \le \mathbf{x} < 1$, $\mathbf{x} \in \boldsymbol{R}$ halmaz nem megszámlálható számosságú:

Minden fenti tulajdonságú **x** szám felírható tizedestört, azaz $0,a_1a_2\ldots$ alakban, ahol $0 \le a_i \le 9$, minden $i \in \boldsymbol{N}$ esetén.
Tegyük fel indirekt, hogy a $0 \le \mathbf{x} < 1$, $\mathbf{x} \in \boldsymbol{R}$ halmaz megszámlálható. Ekkor elemi sorozatba rendezhetők, legyen egy ilyen lehetséges sorba rendezés az alábbi:

$x_1 = 0, a_{11}\ a_{12}\ a_{13}\ldots$
$x_2 = 0, a_{21}\ a_{22}\ a_{23}\ldots$

Belátható, hogy bármilyen is a fenti sorozat, létezik olyan
$\mathbf{y}=0,b_1b_2b_3\ldots$, $0 \le \mathbf{y} < 1$, amely **y** nem eleme a sorozatnak.

Egy ilyen **y** szám konstrukciója a következő:
Legyen b_k (k=1,2, ...) olyan számjegy melyre $b_k \ne a_{kk}$ és $b_k \ne 9$.

Ekkor $0 \le \mathbf{y} < 1$ és $\mathbf{y} \neq x_n$ semmilyen $n \in \boldsymbol{N}$ esetén, ugyanis ha $\mathbf{y} = x_n$ lenne, akkor $a_{n1} = b_1$, $a_{n2} = b_2$, ... $a_{nn} = b_n$ lenne, ami ellentmondana b_n származtatásának. (□)

Definíció: A valós számok halmazával ekvivalens halmazokat **kontinuum számosságú** halmaznak nevezzük.

Jelölés: C.

Megjegyzés: Az irracionális számok halmaza kontinuum számosságú.

Definíció: Az **A** halmaz **kisebb számosságú**, mint **B** halmaz, ha **A** ekvivalens a **B** halmaz egy részhalmazával, de magával a **B**-vel nem.

Következmény: $n(\{\text{véges halmazok}\}) < \chi_0 < C$, azaz a véges halmazok számossága kisebb, mint a megszámlálhatóan végtelen halmazok számossága, amely kisebb, mint a kontinuum számosságú halmazok számossága.

Definíció: Legyen **X** tetszőleges halmaz, $X \neq \emptyset$ és **Y** egy legalább 2 elemű halmaz. Az **Y** halmaz **X kitevős hatványhalmaza** azon leképezések (függvények) halmaza, amelyek az **X** halmazt az **Y** halmazba képezik le.

Jelölés: $\mathbf{Y}^{\mathbf{X}} = \{ \phi : \mathbf{X} \rightarrow \mathbf{Y} \}$.

Példa: $\mathbf{X} := \{ a, b, c \}$ $\mathbf{Y} := \{ 0, 1 \}$

Az alábbi 8 darab $\phi_i : \mathbf{X} \rightarrow \mathbf{Y}$ (**X** halmazt az **Y** halmazba leképező) függvény definiálható $(1 < i < 8)$:

	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6	ϕ_7	ϕ_8
a	0	0	0	1	0	1	1	1
b	0	0	1	0	1	0	1	1
c	0	1	0	0	1	1	0	1

Látható tehát, hogy $\mathbf{Y}^{\mathbf{X}}$ számossága 8, azaz
$n(\mathbf{Y}^{\mathbf{X}}) = n(\mathbf{Y})^{n(\mathbf{X})} = 2^3 = 8$.

Tétel: Legyen $\mathbf{X} \neq \emptyset$ tetszőleges halmaz és **Y** legalább két elemű halmaz. Ekkor az **Y** halmaz **X** kitevős hatványhalmazának, $\mathbf{Y}^{\mathbf{X}}$ -nek a számossága mindig nagyobb, mint **X** halmaz számossága.

Tétel: Minden $\mathbf{X} \neq \emptyset$ halmaz összes részhalmazainak halmaza nagyobb számosságú **X**-nél.

Következmény: Minden halmaznál van nagyobb számosságú halmaz, nevezetesen a hatványhalmaza.

Tétel: Egy megszámlálható számosságú halmaz összes részhalmazainak halmaza kontinuum számosságú. Azaz $2^{\chi_0} = C =: \chi_1$

Megjegyzés: Kontinuum-hipotézis (Cantor-féle hipotézis): χ_0 és χ_1 közé nem esik számosság. Általánosan χ_n és χ_{n+1} közé nem esik számosság.
Ez a hipotézis, sem az ellentettje nem vezet ellentmondásra a többi halmazelméleti axiómával.

6. Algebrai struktúrák

Definíció: Az S={α, β,…} halmazon definiált egy **művelet** (jelölés pl.: *), ha S minden α, β elempárjához egyértelműen hozzárendeli S egy elemét (* : S × S → S).

Definíció: Egy S={α, β,…} halmazt **algebrai struktúrá**nak nevezzük, ha definiált benne legalább egy művelet.

Definíció: Az S={α, β,…} halmazon definiált művelet **asszociatív,** ha minden α, β, γ ∈ S esetén (α * β) * γ = α * (β * γ).

Definíció: Egy algebrai struktúra **félcsoport,** ha egy műveletet definiálunk benne és ez a művelet egy asszociatív szorzás.

Definíció: Az S={α, β,…} halmazon definiált művelet **invertálható,** ha az ξ * γ = β és a γ * ξ = β egyenleteknek minden β, γ ∈ S esetén van S-ben megoldása.

Definíció: Egy algebrai struktúra **csoport**, ha egy műveletet definiálunk benne és ez a művelet egy asszociatív, invertálható szorzás. Azaz egy algebrai struktúra csoport, ha félcsoport és a benne definiált szorzás invertálható is.

Definíció: Ha egy csoportban definiált szorzás művelet kommutatív is, akkor a csoportot **Abel-csoport**nak nevezzük.

Definíció: Az additív módon írt Abel-csoportot **modulus**nak nevezzük. Azaz egy algebrai struktúra modulus, ha egy műveletet definiálunk benne és ez a művelet egy asszociatív, invertálható, kommutatív összeadás (jelölés: +).

Definíció: Egy algebrai struktúra **gyűrű**, ha egyidejűleg modulus és félcsoport, és ha a műveletekre teljesül a disztributivitás. Azaz egy algebrai struktúra gyűrű, ha két műveletet definiálunk benne, egy asszociatív szorzást (*), valamint egy asszociatív, invertálható, kommutatív összeadást (+). Emellett teljesül a disztributivitás:
α * (β + γ) = α * β + α * γ valamint
(β + γ) * α = β * α + γ * α minden α, β, γ ∈ S.

Definíció: Egy algebrai struktúra **ferdetest**, ha gyűrű, és benne lévő félcsoport a **0** elem elhagyása után csoportot alkot. Azaz egy algebrai struktúra ferdetest,ha két műveletet definiálunk benne, egy asszociatív és a nullelem kivételével invertálható szorzást (*), valamint egy asszociatív, invertálható, kommutatív összeadást (+). Emellett teljesül a disztributivitás.

Definíció: Egy algebrai struktúra **test**, ha a benne definiált szorzás kommutatív.

Definíció: Ha $\alpha \neq 0$ és $\beta \neq 0$, de $\alpha * \beta = 0$, akkor α -t **bal oldali**, β -t **jobb oldali nullosztó**nak nevezzük.

Definíció: Egy gyűrű (R) **nullosztómentes**, ha nincs nullosztója a nullelemen (**0**) kívül.

Definíció: A kommutatív, nullosztómentes gyűrűt **integritási tartomány**nak nevezzük.

Megjegyzés: Egy R gyűrűben érvényes az alábbi következtetés: $\alpha * \beta = \alpha * \gamma \Rightarrow \beta = \gamma$ akkor és csak akkor, ha α nem baloldali nullosztó.

Definíció: Ha valamely $\varepsilon_b \in R$ elemre $\varepsilon_b * \alpha = \alpha$ minden $\alpha \in R$ esetén, akkor ε_b az R gyűrű **bal oldali egységeleme**.
Ha $\alpha * \varepsilon_j = \alpha$ minden $\alpha \in R$ esetén, akkor ε_j **jobb oldali egységelem**.

Tétel: Ha az R gyűrűben van bal oldali és jobb oldali egységelem is, akkor egyikből sincs több és ezek egyenlőek ($\varepsilon_b = \varepsilon_j := \varepsilon$).

Definíció: Legyen R egységelemes (ε) gyűrű. Ha $\alpha \in R$ esetén létezik olyan α_b, amelyre $\alpha_b * \alpha = \varepsilon$, akkor α_b az α **bal oldali inverz**e.
Hasonlóan definiálható a **jobb oldali inverz**.

Tétel: Ha létezik bal és jobboldali inverz is, akkor ezek egyenlőek, és nincs több egyoldali inverz.

Példa1: A mátrix-ok a mátrix-szorzásra és összeadásra nézve gyűrűt, de nem nullosztómentes gyűrűt alkotnak.

Példa2: Legyen $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$,
legfeljebb k-ad fokú polinom ($a_0, a_1, \ldots, a_k \in \boldsymbol{R}$).
Az összeadást definiálhatjuk az alábbi módon:
$(a_0 + a_1 x + \ldots) + (b_0 + b_1 x + \ldots) = (a_0 + b_0) + (a_1 + b_1) x + \ldots$
A szorzást definiálhatjuk a következőképpen:
$(a_0 + a_1 x + \ldots) * (b_0 + b_1 x + \ldots) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \ldots$
Ezekkel a műveletekkel a legfeljebb k-ad fokú polinomok nullosztómentes gyűrűt alkotnak.
Ha $a_0, a_1, \ldots, a_k \in \boldsymbol{R}$, akkor a valós számok teste feletti polinomgyűrűről beszélünk. Ha $a_0, a_1, \ldots, a_k \in \boldsymbol{C}$, akkor a komplex számok teste feletti polinomgyűrűről beszélünk.

Példa3: A valós számok ($\boldsymbol{R}$), a komplex számok ($\boldsymbol{C}$), a racionális számok ($\boldsymbol{Q}$) testet alkotnak.

Tétel (az algebra alaptétele):
Legyen $\boldsymbol{C[x]}$ a komplex számok teste feletti polinomgyűrű és legyen $f(x) \in \boldsymbol{C[x]}$ legalább elsőfokú polinom. Ekkor f(x)-nek a komplex számok között létezik gyöke, azaz létezik $\alpha \in \boldsymbol{C}$ olyan, hogy $f(\alpha) = 0$.

Következmény: A komplex számok között f(x) n-edfokú polinomnak pontosan n gyöke van – multiplicitással számolva.

7. Boole algebra

Példa1: Legyen H egy tetszőleges halmaz és legyen $\mathcal{H}$ a H összes részhalmazainak halmaza. Ekkor $\mathcal{H}$-t teljes halmazalgebrának nevezzük.
Legyen A, B, C $\in \mathcal{H}$. Ekkor teljesülnek az alábbi tulajdonságok a halmazok műveleteire vonatkozóan:

$A \cup B = B \cup A$,

$A \cap B = B \cap A$,

$A \cup (B \cup C) = (A \cup B) \cup C$,

. $A \cap (B \cap C) = (A \cap B) \cap C$,

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

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

$A \cup A = A$,

$A \cap A = A$,

$A \cup \overline{A} = H$,

$A \cap \overline{A} = \emptyset$,

$A \cup H = H$,

$A \cap H = A$,

$A \cup \emptyset = A$,

$A \cap \emptyset = \emptyset$.

Definíció: Egy H halmaz részhalmazainak τ összessége **halmazalgebra**, ha

1. $H \in \tau$
2. Ha $A \in \tau$ és $B \in \tau$, akkor $A \cup B \in \tau$
3. Ha $A \in \tau$, akkor $\overline{A} \in \tau$

Megjegyzés: A fenti tulajdonságok egy tetszőleges τ halmazalgebrában is érvényesek.

Példa2: Legyenek A, B, C ítéletek. Ekkor igazak az alábbi tulajdonságok az ítéletműveletekre vonatkozóan:

$A \vee B = B \vee A$,

$A \wedge B = B \wedge A$,

$A \vee (B \vee C) = (A \vee B) \vee C$,

. $A \wedge (B \wedge C) = (A \wedge B) \wedge C$,

$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$,

$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$,

$A \vee A = A$,

$A \wedge A = A$,

$A \vee (\neg A) = \uparrow$,

$A \wedge (\neg A) = \downarrow$,

$A \vee \uparrow = \uparrow$,

$A \wedge \uparrow = A$,

$A \vee \downarrow = A$,

$A \wedge \downarrow = \downarrow$.

Az ítéleteket a fenti műveletekkel **ítéletalgebrának** nevezzük.

Definíció: Az **a**, **b**, **c** elemek egy ***B*** halmazát Boole-algebrának nevezzük, ha értelmezve van benne három művelet: $\oplus$, *, ’ az alábbi tulajdonságokkal:

$\mathbf{a} \oplus \mathbf{b} = \mathbf{b} \oplus \mathbf{a}$,

$\mathbf{a} * \mathbf{b} = \mathbf{b} * \mathbf{a}$,

$\mathbf{a} \oplus (\mathbf{b} \oplus \mathbf{c}) = (\mathbf{a} \oplus \mathbf{b}) \oplus \mathbf{c}$,

. $\mathbf{a} * (\mathbf{b} * \mathbf{c}) = (\mathbf{a} * \mathbf{b}) * \mathbf{c}$,

$\mathbf{a} * (\mathbf{b} \oplus \mathbf{c}) = (\mathbf{a} * \mathbf{b}) \oplus (\mathbf{a} * \mathbf{c})$,

$\mathbf{a} \oplus (\mathbf{b} * \mathbf{c}) = (\mathbf{a} \oplus \mathbf{b}) * (\mathbf{a} \oplus \mathbf{c})$,

$\mathbf{a} \oplus \mathbf{a} = \mathbf{a}$,

$\mathbf{a} * \mathbf{a} = \mathbf{a}$.

Továbbá létezik ***B*** –ben nullelem: **0** és egységelem: **1**, az alábbi tulajdonságokkal:

$\mathbf{a} \oplus \mathbf{a'} = \mathbf{1}$,

$\mathbf{a} * \mathbf{a'} = \mathbf{0}$,

$\mathbf{a} \oplus \mathbf{1} = \mathbf{1}$,

$\mathbf{a} * \mathbf{1} = \mathbf{a}$,

$\mathbf{a} \oplus \mathbf{0} = \mathbf{a}$,

$\mathbf{a} * \mathbf{0} = \mathbf{0}$.

Jelölés: $< \boldsymbol{B}, \oplus, *, ', \mathbf{0}, \mathbf{1} >$.

Példa1: A halmazalgebra Boole-algebra az alábbi műveletekkel:

$< \boldsymbol{H}, \cup, \cap, \bar{}, \emptyset, H >$.

Példa2: Az ítéletalgebra Boole-algebra az alábbi műveletekkel:

$< \{ \uparrow, \downarrow \} , \vee , \wedge , \neg , \downarrow , \uparrow >$.

Definíció: Legyen $< \boldsymbol{B} , \oplus , * , ' , \mathbf{0} , \mathbf{1} >$ tetszőleges Boole-algebra.

Az $f(x_1 , x_2 , \dots , x_n)$ függvény egy **n változós Boole-függvény**, ha f leképezi $\boldsymbol{B}^n$–t $\boldsymbol{B}$ halmazba, azaz $f : \boldsymbol{B}^n \rightarrow \boldsymbol{B}$.

Példa: Legyen B = {0, 1}. Ekkor 4 Boole-függvény lehetséges:

x	0	1
$f_0(x)$	0	0

x	0	1
$f_1(x)$	0	1

x	0	1
$f_2(x)$	1	0

x	0	1
$f_3(x)$	1	1

Definíció: Legyen $< \boldsymbol{B} , \oplus , * , ' , \mathbf{0} , \mathbf{1} >$ tetszőleges Boole-algebra. Az $x_1 , x_2 , \dots , x_n$ változók fussanak végig a $\boldsymbol{B}$ halmaz elemein. Ekkor

1. A **0** és az **1** Boole-formák.
2. Az $x_1 , x_2 , \dots , x_n$ változók Boole-formák.
3. Ha α Boole-forma, akkor (α) is az.
4. Ha α Boole-forma, akkor α' is az.
5. Ha α és β Boole-forma, akkor $\alpha \oplus \beta$ is az.
6. Ha α és β Boole-forma, akkor $\alpha * \beta$ is az.
7. Csak azok a Boole-formák, melyek az 1 – 6. szabályokkal véges számú lépésben előállíthatók.

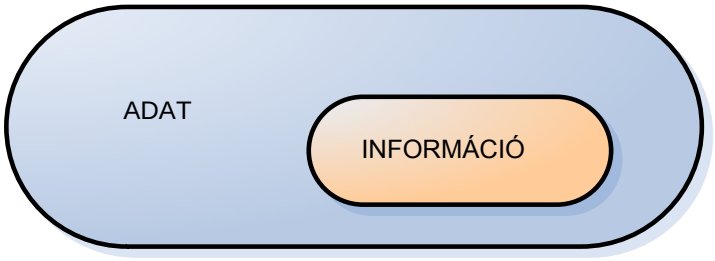
Példa1: Legyen A, B, C $\subset$ H halmazok. Ekkor $A \cap B \cup (B \cap \overline{A}) \cup C$ Boole-forma.

Példa2: Legyenek A, B, C ítéletváltozók. Ekkor $A \wedge B \vee (B \wedge \neg A) \vee C$ Boole-forma.

8. Kódelmélet

Információ, információs csatorna

Definíció: Az **információ** az adatoknak az a része, amelynek számunkra újdonság tartalma van (ld. 8.1. ábra).

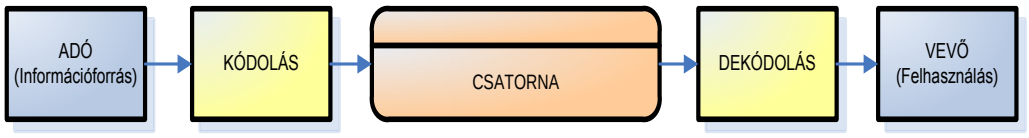


8.1.ábra

Megjegyzés: Az információ tulajdonságai:

- Nem szükségszerűen változik az információt hordozó jelek számával.
- Kétszer adott közleménynek nincs kétszeres értéke.
- Egyidejűleg több egyed részére adott információból mindenki ugyanannyi információt nyerhet – az információ nem osztódik.
- Adott közlemény különböző jelekkel is rögzíthető.
- Azonos jelek különböző összefüggésben mást jelenthetnek.

Definíció: Az információcsere folyamatának három fő komponense az adó- és a vevőberendezés, valamint az őket összekötő **információs csatorna** (ld. 8.2. ábra).



8.2.ábra

Az adó tevékenysége:

- A hírek, közlemények kialakítása
  (Többnyire valamilyen A = {a1, a2, …, an} kimeneti ábécé jeleit küldi ki)

- A közlemények átalakítása a rendelkezésre álló csatorna igényei szerint, azaz a **kódolás.**
  (Rendszerint kétféle jel továbbítására alkalmas, a 0 és az 1 továbbítására, ebben az esetben **bináris csatorná**nak nevezzük)

A vevő tevékenysége:

- A közlemények átalakítása a felhasználó igényei szerint, azaz a **dekódolás.**
- A hírek, közlemények felhasználása.

Kódolás, dekódolás

Definíció: Legyen $A = \{a_1, a_2, \ldots, a_n\}$ tetszőleges kimeneti ábécé és legyen $K = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ véges hosszúságú bináris sorozatok.

Rendeljük hozzá $a_i \in A$ betűk mindegyikéhez a K halmaz egy-egy α_i elemét úgy, hogy különböző betűkhöz különböző bináris sorozatok tartozzanak.

A kódolásnak ezt a formáját **betű szerinti kódolás**nak nevezzük.

Definíció: A K halmazt **kód**nak, az $\alpha_1, \alpha_2, \ldots, \alpha_n$ elemeket **kódszavak**nak, ezek tetszőleges sorozatát **kódolt közlés**nek nevezzük.

1. Példa: A:= {a, b, c,d} , K = {00, 01, 100, 101}

Ekkor a „dac” szó kódja: 10100100.

Definíció: A $K = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ kódot **felbontható**nak nevezzük, ha tetszőleges bináris sorozat legfeljebb egyféleképpen bontható kódszavak sorozatára.

2. Példa: A:= {a, b, c,d} , K = {00, 01, 11, 0001}

Ez a kód nem felbontható, mert pl. az „ab” és a „d” szavaknak ugyanaz a kód felel meg.

Definíció: A $K = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ kódot **prefix kód**nak nevezzük, ha egyetlen kódszó sem valódi kezdőszelete (prefixuma) egy másik kódszónak.

1. Példa: Az 1. Példában leírt kód prefix kód.

2. Példa: A 2. Példában leírt kód nem prefix kód, mert „00” prefixuma „0001”-nek.

Tétel: Minden prefix kód felbontható.

Optimális kódok

Célunk a továbbiakban a legrövidebb kódolt szöveg elérése. Ezt úgy érjük el, hogy a leggyakrabban előforduló betűkhöz rendeljük a legrövidebb kódszavakat, a ritkábban előfordulókhoz a hosszabb kódszavakat. Pontosabban:

Legyen F egy jelforrás, amelyik az A = $\{a_1, a_2, \ldots, a_n\}$ ábécé betűit véletlenszerűen bocsátja ki és legyen p_i annak a valószínűsége, hogy az F által kibocsátott jel a_i .
(Ekkor $p_i > 0$ és $p_1+p_2+\ldots+p_n = 1$)

Legyen a_i kódja α_i és legyen α_i hossza l_i.

Mivel a_i egy M hosszú jelsorozatban átlagosan p_i M –szer fordul elő, ezért a hozzá tartozó átlagos összkódhossz: $l_i\ p_i$ M.

Az M hosszú jelsorozatot kódoló kódolt közlés átlagos összhossza tehát:

$$l_1\ p_1\ M + l_2\ p_2\ M + \ldots + l_n\ p_n\ M.$$

Cél ennek a hossznak, azaz $l_1\ p_1 + l_2\ p_2 + \ldots + l_n\ p_n$ összegnek csökkentése.

Definíció: Az $L(K) := l_1\ p_1 + l_2\ p_2 + \ldots + l_n\ p_n$ összeget a K kód F forrás melletti **költség**ének nevezzük.

Definíció: A K^O felbontható kódot az F jelforrásra nézve **optimális**nak mondjuk, ha tetszőleges K felbontható kódnak az F mellett számított L(K) költsége nem kisebb $L(K^O)$-nál.

Az optimális kódok tehát a kódolt közlések átlagos hosszát minimalizálják.

Tétel: Tetszőleges F jelforráshoz létezik optimális prefix kód.

Definíció: A $H(F) := -\ p_1 \log_2 p_1 - p_2 \log_2 p_2 - \ldots - p_n \log_2 p_n$ számot az F forrás **entrópiá**jának nevezzük.

Tétel (Shannon tétele zajmentes csatornákra): Egy F jelforráshoz tartozó tetszőleges K felbontható kódra $L(K) \geq H(F)$, azaz teszőleges kód költsége nagyobb vagy egyenlő, mint a forrás entrópiája.

Tétel: Egy F jelforráshoz tartozó K^O optimális kód költségére teljesül, hogy $L(K^O) \leq H(F)+1$, azaz az optimális kód költsége kisebb vagy egyenlő, mint a forrás entrópiája +1.

Megjegyzés: Az optimális kódra: $H(F) \leq L(K^O) \leq H(F)+1$

Példa: Az optimális kód előállítható a **Huffmann-féle algoritmus**sal. Legyen a kimeneti ábécé A = {a_1, a_2, …, a_7}, a betűk kibocsátásának valószínűsége rendre: {0.2, 0.2, 0.19, 0.12, 0.11, 0.9, 0.9}. (A kibocsátott betűket előfordulásuk valószínűsége szerint csökkenő sorrendbe állítottuk). Az algoritmus első részében a kimeneti ábécét redukáljuk, olyan módon, hogy lépésenként a legkisebb valószínűséggel kibocsátott 2 betűt összevonjuk. Így végül egy olyan feladathoz jutunk el, melynél 2 betűs ábécéhez kell optimális kódot megadnunk. Ebben az esetben a {0, 1} kód nyilván optimális lesz. (Az alábbi táblázatban + jel jelöli az összevonandó betűk előfordulási valószínűségeit, = pedig az eredményül kapott valószínűséget.)

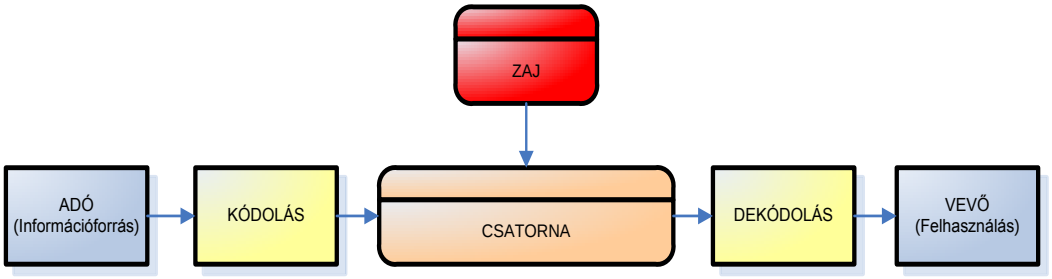
F	p_i					
a_1	0,2	0,2	= 0,23	= 0,37	= 0,4	= 0,6
a_2	0,2	0,2	0,2	0,23	0,37 +	0,4
a_3	0,19	0,19	0,2	0,2 +	0,23 +	
a_4	0,12	= 0,18	0,19 +	0,2 +		
a_5	0,11	0,12 +	0,18 +			
a_6	0,09 +	0,11 +				
a_7	0,09 +					

Az algoritmus második részében visszafele haladunk az eredeti összevonások mentén és az egyre növekvő elemszámú ábécéhez határozzuk meg az optimális kódokat a redukált ábécé kódjait kibővítve (ld. az alábbi táblázatot).

F	Kódok					
a_1	10	10	01	00	1	0
a_2	11	11	10	01	00	1
a_3	000	000	11	10	01	
a_4	010	001	000	11		
a_5	011	010	001			
a_6	0010	011				
a_7	0011					

Hibajavító kódolás

Definíció: Általában az információs csatorna nem működik mindig kellő biztonsággal, így előfordulhat, hogy vevőhöz érkező üzenet különbözik attól, mint amit az adó továbbított. Az ilyen csatornákat **zajos csatorná**knak nevezzük (ld. 8.3. ábra).



8.3.ábra

Ebben a részben olyan kódokkal foglalkozunk, melyekkel védekezni tudunk a zaj okozta hibáktól. A védekezés két szintű lehet: a hiba felismerése ill. a hiba kijavítása.

A továbbiakban bináris, állandó hosszúságú kódokkal foglalkozunk.

Megjegyzés: Ezek a kódok prefixek.

Definíció: A bináris, állandó hosszúságú kódok esetén a kódszavakat **blokk**oknak, a kódszavak hosszát **blokkméret**nek nevezzük.

Definíció: Legyen a $K = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ kódhoz tartozó blokkméret n, és legyen $t \leq n$ tetszőleges.

Az információs csatorna legfeljebb t egyedi hibát okoz, ha a csatorna alapzajának hatására tetszőleges blokkban legfeljebb t jel értéke változik meg.

Példa: n=3, t=1: 001 → 011, 001 → 101 (a vastagított jel a hibás)

Példa 1 hibát **felismerő** kódra**:** A kódszavak első és második fele megegyezik.

A küldendő üzenet: 010

Az elküldött üzenet: 010010 Vevőhöz érkezett: 010010

Az érkezett üzenet első és második fele megegyezik: az üzenet helyes.

Az elküldött üzenet: 010010 Vevőhöz érkezett: 010011

Az érkezett üzenet első és második fele nem egyezik meg: az üzenet hibás.

Példa 1 hibát **javító** kódra**:** A kódszavak első, második és harmadik harmada megegyezik.

A küldendő üzenet: 010

Az elküldött üzenet: 010 010 010 Vevőhöz érkezett: 010 110 010

Az érkezett üzenet három része nem egyezik meg: az üzenet hibás.

Az elküldött üzenet: 010 010 010 Vevőhöz érkezett: 010 010 110

Az érkezett üzenet három része nem egyezik meg: az üzenet hibás.

A két azonos sorozatot tekintjük helyesnek.

Definíció: Legyen K = $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ kód, melyben a kódszavak száma m, a blokkméret n. Ekkor a **kód sűrűsége** = $\log_2 m / n$, azaz az m jelhez szükséges legrövidebb blokkméret és a tényleges blokkméret aránya.

Példa: A fenti 1 hibát **felismerő** kód sűrűsége: $\log_2(2^{n/2}) / n = 1/2$,

(Ugyanis a blokkméret n, ekkor a kódszó hossza a kód konstrukciója miatt n/2. Az n/2 hosszon maximum $2^{n/2}$ kódszó kódolható, így $m = 2^{n/2}$.)

A fenti 1 hibát **javító** kód sűrűsége: $\log_2(2^{n/3}) / n = 1/3$.

Definíció: Az α és β kódszavak **Hamming-távolság**a azon pozíciók száma, ahol a kódszavak eltérnek egymástól.

Jelölés : ρ (α, β)

Példa: α:= 001, β:=111. Ekkor ρ(α, β) = 2.

α:= 1001, β:=0000. Ekkor ρ(α, β) = 2.

Definíció: Tetszőleges K kódra **kódtávolság**nak nevezzük a különböző K-beli szavak egymás közti távolságának minimumát.

Jelölés : d(K)

Példa: 1 hibát **felismerő** kód kódtávolsága: 2,

1 hibát **javító** kód kódtávolsága : 3.

Tétel: Tetszőleges K kód pontosan akkor alkalmas t darab hiba felismerésére, ha $d(K) \geq t+1$.

Tétel: Tetszőleges K kód pontosan akkor alkalmas t darab hiba javítására, ha $d(K) \geq 2t+1$.

Példa1: **Paritásellenőrző kód**

Blokkonként az 1-esek száma páros (vagy páratlan) kell, hogy legyen. (Ezt a blokk utolsó bitje, a paritás bit biztosítja.)

Kódtávolsága 2, így 1 hiba felismerésére alkalmas.

Sűrűsége: $\log_2 (2^{n-1}) / n = (n-1)/n = 1-1/n$, amely igen magas.

(A gyakorlatban n = 5 ~ 8)

Hibajavításra nem alkalmas.

Példa páratlan paritásra: :

Elsődleges kód:	Paritásbit:	Végleges kód:
11010	1	110101
10010	0	100100

Példa2: **Hamming-kód**

Több paritásbitet helyezünk el a kódszóban, a 2 egész hatványainak helyén, azaz az 1., 2., 4., 8., stb. helyeken.

Kódtávolsága legalább 3, így 1 hiba javítására alkalmas.

Sűrűsége: ~ $1 - (\log_2 (n) / n)$

Pozíciók		1	2	3	4	5	6	7
Paritásbitek		P	P	*	P	*	*	*
Paritásszintek	P_1	+		+		+		+
	P_2		+	+			+	+
	P_4				+	+	+	+

A fenti táblázatban a * -gal jelölt helyre kerül az elsődleges kód, P a paritásbitek helye. A paritásbitek a kódszóban a 2 egész hatványainak helyére kerülnek, azaz 1., 2., 4., 8., 16., stb. helyre.

A + -szal jelölt helyek az ellenőrzésbe bevonandó pozíciók. Helyüket a kettes számrendszerben felírt számokban előforduló egyesek helye alapján határozhatjuk meg, ahol a P_1 paritásszint a $2^0 = 1$, P_2 paritásszint a $2^1 = 2$, .., P_k paritásszint a 2^{k-1}-en pozíciónak felel meg.

A paritást az egyes paritásszinteken ellenőrizzük.

Példa páratlan paritású Hamming-kódra (ld. alábbi táblázat)**:**

Elsődleges kód: 1010

Paritásbit az 1. pozición: 0

Paritásbit a 2. pozición: 1

Paritásbit a 4. pozición: 0

Végleges kód: 0110010

Pozíciók		1	2	3	4	5	6	7
Paritásbitek		P	P	**1**	P	**0**	**1**	**0**
Paritásszintek	P_1	0		1		0		0
	P_2		1	1			1	0
	P_4				0	0	1	0
Kód		0	1	1	0	0	1	0

Hibajavítás 0110**1**10 hibás kód érkezése esetén:

Pozíciók		1	2	3	4	5	6	7	
Paritásbitek		0	1	**1**	0	**1**	**1**	**0**	
Paritásszintek	P_1	0		1		1		0	Hibás paritás
	P_2		1	1			1	0	Helyes paritás
	P_4				0	1	1	0	Hibás paritás

Mivel a hibás paritásszint az 1. és a 4., a hibás kódpozíció: 1 + 4 = 5.

Megjegyzés: Ha a Hamming-kód elé a 0. pozícióra egy olyan un. vezérparitásbitet helyezünk el, melynek értékét mindegyik bit figyelembe vételével alakítottuk ki, akkor 1 hibát javító és még egy hibát felismerő kódhoz jutunk.

Irodalom

[1] **Dringó László – Kátai Imre: Bevezetés az matematikába**
Tankönyvkiadó, Budapest, 1988.

[2] **Demetrovics János – Jordan Denev – Radiszlav Pavlov: A számítástudomány matematikai alapjai**
Tankönyvkiadó, Budapest, 1989.

[3] **Szelezsán János: Matematika I.**
LSI Oktatóközpont, 2005.

[4] **Kógelmann Gábor: Bevezetés az informatikába**
Dunaújvárosi Főiskola, Dunaújváros, 1991.