

Algebrai struktúrák

Csoportok

Definíció 1 (Csoport) Legyen $G \neq \emptyset$ halmaz egy \cdot művelettel, amely az alábbi tulajdonságú:

1. **asszociatív**, azaz $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. létezik **egységelem**, azaz $\exists e \in G, \forall a \in G : a \cdot e = e \cdot a = a$
3. minden elemnek létezik **inverze**, azaz $\forall a \in G \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = e$

Ekkor a (G, \cdot) algebrai struktúrát csoportnak nevezzük.

Ha csak az asszociativitás teljesül, akkor (G, \cdot) -t félcsoportnak nevezzük. Megj: Itt a \cdot jel nem feltétlenül a számoknál megszokott szorzást jelenti, hanem tetszőleges egyéb művelet is lehet.

Példák:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ csoport, az egységelem mindegyik esetben a 0, az inverz pedig az ellentett.
- Mod m maradékosztályok az összeadásra, az egységelem a $\bar{0}$ maradékosztály.
- Tetszőleges vektortér az összeadásra, az egységelem a nullvektor.
- $(\mathbb{Z} \setminus \{0\}, \cdot), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$ csoport, az egységelem mindegyik esetben az 1, az inverz pedig a reciprokok.
- Az $n \times n$ -es nem szinguláris (nem nulla determinánsú) mátrixok a mátrixszorzásra csoport. Egységelem az egységmátrix, inverz elem a mátrix inverze.

Definíció 2 (Abel csoport) Ha a (G, \cdot) csoportban a \cdot művelet kommutatív (azaz $\forall a, b \in G : a \cdot b = b \cdot a$), akkor a (G, \cdot) csoportot kommutatív csoportnak, más néven Abel csoportnak nevezzük.

Példák: A fenti példák az utolsó kivételével (nem szinguláris mátrixok a szorzásra) Abel csoportok.

Definíció 3 (Hatványozás csoportban) Legyen (G, \cdot) egy csoport, e a csoport egységeleme.

$$a^0 := e$$

$$a^1 := a$$

$$a^n := a^{n-1} \cdot a \quad n > 1$$

Tétel 1 (Hatványozás tulajdonságai)

Minden csoportban igaz:

$$a^n \cdot a^m = a^{n+m}$$

$$(a^n)^m = a^{nm}$$

Abel csoportokban igaz:

$$(a \cdot b)^n = a^n \cdot b^n$$

Definíció 4 (Gyűrű) Legyen $R \neq \emptyset$ halmaz, $+$ és \cdot műveletekkel. Az $(R, +, \cdot)$ algebrai struktúrát gyűrűnek nevezzük, ha

1. $(R, +)$ Abel csoport (a gyűrű additív csoportja)
2. (R, \cdot) félcsoport (a gyűrű multiplikatív félcsoportja)
3. \cdot művelet disztributív a $+$ -ra nézve.

Példa: $n \times n$ -es mátrixok a mátrixösszeadásra és a mátrixszorzásra gyűrű.

Definíció 5 (Test) Legyen $T \neq \emptyset$ halmaz, $+$ és \cdot műveletekkel. A $(T, +, \cdot)$ algebrai struktúrát testnek nevezzük, ha

1. $(T, +)$ Abel csoport
2. $(T \setminus \{0\}, \cdot)$ Abel csoport
3. $A \cdot$ művelet disztributív a $+$ -ra nézve.

Példa: $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ testek.

Definíció 6 (Elem rendje) Legyen (G, \cdot) csoport, e az egységeleme. Az $a \in G$ elem rendje az a legkisebb pozitív k egész, melyre $a^k = e$. Ha ilyen nincs, akkor azt mondjuk, hogy a rendje végtelen. Jelölés: $o(a) = k$ ill. $o(a) = \infty$.

Megj: Ha $o(a) = k$, akkor a -nak éppen k darab különböző hatványa van.

Definíció 7 (Ciklikus csoport) A (G, \cdot) csoport ciklikus, ha G egyetlen elem (összes) hatványából áll. Azaz $\exists g \in G : \forall a \in G \exists k \in \mathbb{N}, a = g^k$. Ekkor G elemeit g generálja. Jelölés: $G = \langle g \rangle$.

Tétel 2 (Speciális Lagrange tétel) Véges csoportban az elem rendje osztója a csoport rendjének (elemszámának). Azaz, ha $|G| = n$, akkor $\forall a \in G : o(a) | n$. Ez éppen azt jelenti, hogy $\forall a \in G : a^{|G|} = e$.

Definíció 8 (Részcsoporthoz) Legyen (G, \cdot) , $H \subseteq G$. A (H, \cdot) részcsoporthoz (G, \cdot) -nek, ha maga is csoport a G -beli műveletre nézve. Jelölés: $H \leq G$.

Például: $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

Tétel 3 (Lagrange tétel) Véges csoport bármely részcsoporthozának rendje osztója a csoport rendjének. Azaz: Ha G véges, $|G| = n$, $H \leq G$, $|H| = k$, akkor $k | n$.

Definíció 9 (Mellékosztályok)

G csoport, H részcsoporthoz, $g \in G$.

A g -nek a H szerinti baloldali mellékosztálya: $gH := \{g \cdot h, h \in H\}$

A g -nek a H szerinti jobboldali mellékosztálya: $Hg := \{h \cdot g, h \in H\}$

Megj: Két elemhez tartozó adott részcsoporthoz szerinti mellékosztály vagy egyenlő vagy diszjunkt.

Definíció 10 (Részcsoporthoz indexe) Legyen $H \leq G$. H szerinti baloldali mellékosztályok száma H indexe G -ben. Jelölés: $[G : H]$
(Lehetne jobboldalival is definiálni, ugyanaz az index adódik.)

Tétel 4 (Lagrange tétel (a másik ilyen nevű tétel pontosítása)) Ha G véges, $|G| = n$, $H \leq G$, akkor

$$[G : H] = \frac{|G|}{|H|}$$

Tétel 5 (Normálosztó) Legyen $N \leq G$. Ha $\forall a : aN = Na$, akkor N -et normálosztónak (normális részcsoporthoznak) nevezzük. Jelölés: $N \triangleleft G$

Megj: Abel csoportban minden részcsoporthoz normálosztó.

Ha $[G : H] = 2$, akkor $H \triangleleft G$.

Tétel 6 (Normálosztó (és csak az) zárt a konjugáltra) Legyen $H \leq G$.

$$H \triangleleft G \iff \forall g \in G, h \in H : g^{-1} \cdot h \cdot g \in H$$

ahol $g^{-1} \cdot h \cdot g$ -t a h g szerinti konjugáltjának nevezzük.

Tétel 7 (Faktorcsoporthat) Legyen $N \triangleleft G$. Az N szerinti (baloldali) mellékosztályok csoportot alkotnak az $aN \diamond bN := abN$ műveletre nézve. Ezt a G csoport N szerinti faktorcsoporthatjának nevezzük. Jelölés: G/N

Megj: Ha G véges, akkor

$$|G/N| = [G : N] = \frac{|G|}{|N|}$$

Definíció 11 ((Csoport)morfizmus (vagy homomorfizmus)) Ha $(G_1, \star), (G_2, \diamond)$ csoportok, akkor a $\varphi : G_1 \rightarrow G_2$ leképezést (csoport)morfizmusnak nevezzük, ha az művelettartó. Azaz $\forall a, b \in G_1 : \varphi(a \star b) = \varphi(a) \diamond \varphi(b)$. Ha φ bijektív, akkor (csoport)izomorfizmusnak nevezzük.

Két csoportot izomorfának nevezünk, ha létezik köztük izomorfizmus. Ennek jelölése: $G_1 \cong G_2$.

Definíció 12 (Morfizmus képtere és magtere) Legyen $\varphi : G_1 \rightarrow G_2$ morfizmus.

Képtér: $\text{Im}\varphi := \{v \in G_2 : \exists u \in G_1, \varphi(u) = v\}$

Magtér: $\text{Ker}\varphi := \{z \in G_1 : \varphi(z) = e_2\}$, ahol e_2 a G_2 egységeleme.

Tétel 8 Legyen $\varphi : G_1 \rightarrow G_2$ morfizmus. Ekkor $\text{Ker}\varphi \triangleleft G_1$.

Tétel 9 (Homomorfia tétel) Legyen $\varphi : G_1 \rightarrow G_2$ morfizmus. Ekkor $G_1/\text{Ker}\varphi \cong \text{Im}\varphi$.

Definíció 13 (Permutáció) Legyen $H \neq \emptyset$ véges halmaz. A bijektív $\varphi : H \rightarrow H$ leképezéseket a H permutációknak nevezzük. (A H elemeinek egy rendezését adják.)

Definíció 14 (Szimmetrikus csoport) Legyen $H \neq \emptyset$ véges halmaz, $|H| = n$. A H permutációi csoportot alkotnak a kompozícióra, mint műveletre. Ezt a csoportot n -edfokú szimmetrikus csoportnak nevezzük. Jelölés: S_n

Az S_n részcsoportjait permutációcsoportoknak nevezzük.

Megj: $|S_n| = n!$

Tétel 10 (Cayley tétel)

Minden véges csoport lényegében permutációcsoport.

Pontosabban: Ha $|G| = n$, akkor van S_n -nek olyan H részcsoportja, melyre $G \cong H$.

Hálók

Definíció 15 (Háló - algebrai struktúráként definiálva) Legyen $A \neq \emptyset$ halmaz, \cup és \cap műveletekkel. Az (A, \cup, \cap) algebrai struktúrát hálónak nevezzük, ha $\forall a, b, c \in A$ esetén

1. $a \cup b = b \cup a$, $a \cap b = b \cap a$ (kommutativitás)
2. $(a \cup b) \cup c = a \cup (b \cup c)$, $(a \cap b) \cap c = a \cap (b \cap c)$ (asszociativitás)
3. $a \cap (a \cup b) = a$, $a \cup (a \cap b) = a$ (elnyelési azonosságok)

Definíció 16 (Háló - részbenrendezett halmazokkal definiálva) Az A részbenrendezett halmazt hálónak nevezzük, ha A bármely kételemű részhalmazának létezik legkisebb felső korlátja és legnagyobb alsó korlátja.

Példák: Csoport részcsoportjai a halmazelméleti tartalmazásra, mint részbenrendezésre nézve hálót alkotnak.

Gyűrű részgűrűi a halmazelméleti tartalmazásra, mint részbenrendezésre nézve hálót alkotnak.

Vektortér alterei a halmazelméleti tartalmazásra, mint részbenrendezésre nézve hálót alkotnak.

A természetes számok halmazán két számhoz hozzárendelve azok legnagyobb közös osztóját és legkisebb közös többszörösét két olyan műveletet definiálunk, amelyekkel együtt a természetes számok hamaza hálót alkot.

Definíció 17 (Disztributív háló) Olyan háló, amely teljesíti a disztributivitási szabályokat. Ezek alakja:

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$$

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$$

Definíció 18 (*Moduláris háló*) Olyan háló, amely teljesíti a moduláris szabályt. Ennek alakja:

$$a \leq c \implies a \cup (b \cap c) = (a \cup b) \cap c$$