

Bevezetés a Számításelméletbe II. 11. előadás

Sali Attila

Budapest Műszaki és Gazdaságtudományi Egyetem

Számítástudományi Tsz.

I. B. 137/b

`sali@cs.bme.hu`

2002 április 23.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Részcsoport

1. Definíció. Legyen G csoport. Egy $H \subseteq G$ részhalmazt **részcsoportnak** nevezünk, ha H is csoport **ugyanarra a műveletre** nézve. Jelölése: $H \leq G$.

Példák:

1. $G \leq G$, $\{e\} \leq G$: **triviális részcsoportok** az ezektől különböző részcsoportokat **valódi részcsoportok**
2. A valós számok additív csoportjának részcsoportja a racionális számok, annak pedig az egész számok additív csoportja.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

3. A szabályos háromszög egybevágóságainak (D_3) részcsoportját alkotják a forgatások.
4. Az $n \times n$ -es invertálható mátrixok csoportjának részcsoportja az 1 determinánsú mátrixok.
5. n elem permutációinak részcsoportját alkotják a páros permutációk.
6. A nem 0 komplex számok ($\mathbb{C} - \{0\}$) a szorzásra nézve csoportot alkotnak. Ennek egy részcsoportját alkotják az 1 abszolút értékű komplex számok, annak pedig részcsoportját az n -edik egységgyökök.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Generált részcsoporth

2. Állítás. *Részcsoporthok metszete is részcsoporth, azaz legyenek $H_i \leq G$ ($i \in A$), ahol A valamilyen indexhalmaz, akkor $\bigcap_{i \in A} H_i$ is részcsoporth.*

3. Definíció. *Legyen $K \subseteq G$. K által **generált részcsoporthnak** nevezzük és $\langle K \rangle$ -mal jelöljük a K -t tartalmazó legszűkebb részcsoporthot. Ez nem más, mint a K -t tartalmazó részcsoporthok metszete.*

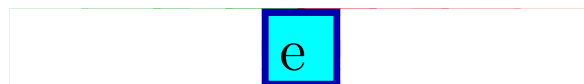
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Ciklikus csoport

G csoport, $a \in G$. $\langle a \rangle$ tartalmazza aa -t, aaa -t, stb.

$\underbrace{aa \dots a}_{n \text{ darab}} = a^n$ jelöléssel: $a^{n+k} = a^n a^k$ és $(a^n)^k = a^{nk}$ $n, k \in \mathbb{N}$.

$\langle a \rangle \ni a^{-1} \implies (a^{-1})^n \in \langle a \rangle$. Tekintsük $(a^{-1})^n a^n$ szorzatot.



Tehát $(a^{-1})^n = (a^n)^{-1}$. Jelöljük ezt az elemet a^{-n} -nel. \implies

$$a^k a^l = a^{k+l} \text{ és } (a^k)^l = a^{kl} \quad \text{tetszőleges } k, l \in \mathbb{Z} \text{ esetén.}$$

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, azaz egy elem által generált részcsoporthoz az elem (negatív és pozitív kitevős) hatványaiából áll.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Véges – végtelen

Két eset:

- a összes hatványa különböző
- van olyan k, l , hogy $a^k = a^l \implies a^{k-l} = 1$, azaz van a -nak olyan hatványa, amely az egységelem.

4. Definíció. A legkisebb ilyen számot a **rendjének** nevezzük, és $o(a)$ -val jelöljük. Ha nincs ilyen szám, végtelen rendű elemről beszélünk.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

$$o(a) = n \implies \langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}.$$

Ezen elemek különbözőek, mert $a^j = a^i$, $i > j$ esetén $a^{i-j} = 1$ lenne, ahol $i - j < n$.

Minden $k \in \mathbb{Z}$ előáll $k = qn + r$ alakban, ahol $0 \leq r < n$, és $a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = 1^q a^r = a^r$, tehát a minden hatványa szerepel $\{1, a, a^2, \dots, a^{n-1}\}$ között.

5. Állítás. *Egy elem rendje megegyezik az általa generált részcsoport rendjével.*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Hány ciklikus csoport van?

Legyen \mathbb{Z}_n a mod n maradékosztályok additív csoportja.

6. Állítás. *Azonos rendű ciklikus csoportok izomorfak.*

BIZONYÍTÁS Legyen $G = \langle a \rangle$ végtelen ciklikus csoport. Tekintsük a

$$\phi: G \rightarrow \mathbb{Z}$$

$\phi(a^n) = n$ megfeleltetést. ϕ bijektív és művelettartó.

Legyen most $G = \langle a \rangle$, $|G| = n$. A $\phi(a^k) = k \pmod{n}$ izomorfizmus.

n elemű ciklikus csoportra további példa az n -edik komplex egységgyökök a szorzásra, a szabályos n -szög forgatásai.

Az n -ed rendű ciklikus csoportot C_n -el jelöljük.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Ciklikus csoport részcsoportjai

7. Állítás. *Ciklikus csoport részcsoportja ciklikus.*

BIZONYÍTÁS Legyen $G = \langle a \rangle$ ciklikus, $H \leq G$ valódi részcsoport. \implies Van H -ban a -nak pozitív kitevős hatványa. Legyen k a legkisebb olyan pozitív szám, hogy $a^k \in H$. $\implies \langle a^k \rangle = H$.

$\langle a^k \rangle \subseteq H$ nyilvánvaló. Tegyük fel, hogy $a^l \in H$. Van olyan $q \geq 0$, $0 \leq r < k$, hogy $l = kq + r$. $\implies a^l (a^k)^{-q} = a^r \in H$, de mivel k volt a legkisebb H -ban szereplő hatványa, $r = 0$ lehet csak, tehát $k \mid l$, $\implies H \subseteq \langle a^k \rangle$.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Mellékosztályok

8. Definíció. Legyenek K, M részhalmazok G -ben. A KM szorzaton a

$$KM = \{km \mid k \in K, \quad m \in M\}$$

halmazt értjük. Legyen $H \leq G$ részcsoporth, $g \in G$. A Hg (gH) szorzatot H g szerinti jobboldali (baloldali) **mellékosztályának**, g -t pedig a mellékosztály **reprezentánsának** nevezzük.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Példa

\mathbb{Z}_{12}

$H = \langle 4 \rangle$	$H + 9$	$H + 6$	$H + 3$
0	1	2	3
4	5	6	7
8	9	10	11
4	9	6	3

Nem véletlen!

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

9. Állítás. Legyen $H \leq G$. Ekkor

1. $g \in Hg$;
2. a Hg mellékosztály minden eleme reprezentálja a Hg mellékosztályt;
3. két különböző jobboldali mellékosztály vagy egybeesik, vagy diszjunktak;
4. ha H véges, akkor bármely mellékosztály elemszáma megegyezik H rendjével.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Bizonyítás

1. $1 \in H, \implies g = 1g \in Hg$

2. Legyen $h \in Hg. \implies \exists h_1 \in H: h = h_1g. \forall x \in H: \quad xh = (xh_1)g \implies Hh \subseteq Hg$, és $\forall x \in H: \quad g = xh_1^{-1}h \implies Hg \subseteq Hh$.

3. = 1. + 2.

4. A $h_1g = h_2g$ egyenlőséget g^{-1} -zel szorozva jobbról kapjuk, hogy $h_1 \neq h_2$ esetén h_1g és h_2g különböznek.

A (jobboldali) mellékosztályok egy ekvivalencia relációt adnak a G csoporton. $x \sim y \iff x$ és y ugyanabban a (jobboldali) mellékosztályban van H szerint $\iff yx^{-1} \in H$ ($\iff xy^{-1} \in H$).

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Lagrange tétele

10. Tétel (Lagrange). *Legyen G véges, $H \leq G$. Ekkor H rendje osztja G rendjét.*

BIZONYÍTÁS $G = \bigcup Hg$. Mivel minden elem pontosan egy mellékosztályban szerepel, ezért $|G| = |\bigcup Hg|$ miatt $|G| = : |Hg| = k|H|$.

11. Definíció. A $k = |G|/|H|$ számot H G -beli **indexének** nevezzük és $|G : H|$ -val jelöljük. $|G : H||H| = |G|$.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Következmények

12. Következmény. *Egy elem rendje osztja a csoport rendjét.*

BIZONYÍTÁS Egy elem rendje megegyezik az általa generált részcsoporthat rendjével.

13. Következmény. *Minden prímmrendű csoport ciklikus.*

BIZONYÍTÁS Legyen $|G| = p$, p prím. Ekkor egy $1 \neq x \in G$ rendje csak p lehet. $\implies \{1, x, x^2, \dots, x^{p-1}\}$ mind különbözőek, azaz $G = \{1, x, x^2, \dots, x^{p-1}\}$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Jobb és baloldali mellékosztályok

PÉLDA Legyen G az $\{1, 2, 3, 4\}$ elemek permutációinak csoportja. $G_1 \leq G$ azon permutációk, melyek az 1 elemet fixen hagyják. (Ez részcsoport!) $\implies |G_1| = 6, |G : G_1| = 4$.

Legyen π_{1i} az a permutáció, ami az 1 és az i elemeket felcseréli, a többi helyben hagyja. $\pi_{1i} \cdot G_1$ **baloldali** mellékosztály elemei azon permutációk, melyek az 1 elemet i -be viszik. \implies A négy baloldali mellékosztály: $\pi_{1i} \cdot G_1, i = 1, 2, 3, 4$.

A $G_1 \cdot \pi_{12}$ **jobboldali** mellékosztály egy-egy eleme a π_{12} , valamint a $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \cdot \pi_{12}$ permutáció. Ezek az 1 elemet különböző helyekre viszik, azaz nincsenek ugyanabban a baloldali mellékosztályban. \implies A G_1 -szerinti jobb és baloldali mellékosztályok különbözőek.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Normálosztó

14. Definíció. Legyen G csoport, $N \leq G$. N **normálosztó** G -ben ($N \triangleleft G$), ha N jobboldali és baloldali mellékosztályai megegyeznek.

Azaz minden jobboldali mellékosztály egyben baloldali is.

Nh mellékosztály előáll h_1N alakban. Mivel $h \in Nh$ és $h \in hN$ ez csak úgy lehet, ha $hN = Nh$ minden $h \in G$ -re.

\implies Abel csoport minden részcsoporthja normálosztó.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Normálosztók jellemzése

15. Állítás. *Az alábbi állítások ekvivalensek:*

1. $N \triangleleft G$;
2. $gN = Ng$ minden $g \in G$ -re;
3. $g^{-1}Ng = N$ minden $g \in G$ -re;
4. tetszőleges $h \in N, g \in G$ esetén $g^{-1}hg \in N$.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Bizonyítás

1. \Leftrightarrow 2. Láttuk.

2. \Leftrightarrow 3. Szorozzuk meg a $gN = Ng$ egyenlőség mindkét oldalát balról g^{-1} -zel.

3. \Rightarrow 4. nyilvánvaló.

4.-ből következik, hogy $g^{-1}Ng \subseteq N$, valamint, hogy $gNg^{-1} \subseteq N$. Ez utóbbi tartalmazási relációt jobbról g -vel, balról g^{-1} -zel szorozva $N \subseteq g^{-1}Ng$ -t kapjuk, amiből következik 3.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Faktorcsoporth

Legyen $N \triangleleft G$, $g, h \in G$. Mivel $g^{-1}Ng = N$ és $NN = N$, $NgNh = Ngg^{-1}Ngh = Ngh$, azaz egy normálosztó két mellékosztályának szorzata megegyezik egy harmadik mellékosztállyal.

$N(Ng) = (Ng)N = Ng, \implies$ maga a normálosztó egységelemként viselkedik.

$Ng^{-1}Ng = NN = N, \implies$ az új műveletre nézve minden mellékosztálynak van inverze.

Tehát egy normálosztó szerinti mellékosztályok csoportot alkotnak a részhalmaz-szorzásra, mint műveletre.

16. Definíció. Ezt a csoportot a G csoport N normálosztója szerinti **faktorcsoporthjának** nevezzük, G/N -nel jelöljük. Elemszáma megegyezik az N szerinti mellékosztályok számával, vagyis N indexével, azaz $|G/N| = |G : N|$.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Abel-csoport minden faktorcsoportja kommutatív, ciklikus csoport minden faktorcsoportja ciklikus,

$$Nxy = Nyx,$$

$$G = \langle a \rangle \implies$$

$$G/N = \langle Na \rangle.$$

Egy faktorcsoport rendje osztója a csoport rendjének.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Homomorfizmus

17. Definíció. Legyenek G_1, G_2 csoportok. A $\phi: G_1 \rightarrow G_2$ leképezést homomorfizmusnak nevezzük, ha ϕ értelmezve van G_1 minden elemén és művelettartó, azaz tetszőleges $a, b \in G_1$ esetén

$$\phi(ab) = \phi(a)\phi(b).$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Példák

1. Legyen $G_1 = G_2$, ϕ a helybenhagyás.
2. Legyen $G_1 = (\mathbb{C}, +)$, $G_2 = (\mathbb{R}, +)$, azaz a komplex illetve valós számok additív csoportja. Legyen

$$\begin{aligned}\phi: \mathbb{C} &\rightarrow \mathbb{R} \\ a + bi &\rightarrow a,\end{aligned}$$

vagyis rendeljük hozzá minden számhoz a valós részét. Ez a leképezés homomorfizmus, hiszen amikor komplex számokat összeadunk, a valós részek összeadódnak.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

3. Jelölje $GL(n, \mathbb{R})$ az $n \times n$ -es valós elemű invertálható mátrixok csoportját a mátrixszorzásra nézve. Legyen

$$\begin{aligned} \phi: GL(n, \mathbb{R}) &\rightarrow (\mathbb{R} - \{0\}, \cdot) \\ A &\rightarrow \det(A), \end{aligned}$$

A determinánsok szorzástétele alapján ez homomorfizmus.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Mag, kép

18. Definíció. Legyen $\phi: G_1 \rightarrow G_2$ homomorfizmus. Azon G_1 -beli elemek halmazát, amelyek képe 1_{G_2} (vagyis a G_2 -beli egységelem) a leképezés **magjának** nevezzük és $\text{Ker}(\phi)$ -vel jelöljük. Azon G_2 -beli elemek halmazát, amelyek előállnak egy G_1 -beli elem képeként, a leképezés **képének** nevezzük és $\text{Im}(\phi)$ -vel jelöljük.

$$\text{Ker}(\phi) = \{g \in G_1 \mid \phi(g) = 1_{G_2}\},$$

$$\text{Im}(\phi) = \{g \in G_2 \mid \exists h \in G_1 \quad \phi(h) = g\}.$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

19. Állítás. *Homomorfizmusnál egységelem képe egységelem, inverz képe a kép inverze, a kép részcsoport, a mag normálosztó:*

$$\begin{aligned} \phi(1_{G_1}) &= 1_{G_2}, & \phi(g^{-1}) &= \phi(g)^{-1}, \\ \text{Im}(\phi) &\leq G_2, & \text{Ker}(\phi) &\triangleleft G_1. \end{aligned}$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Bizonyítás

Tetszőleges $g \in G_1$ -re

$$\phi(1_{G_1})\phi(g) = \phi(1_{G_1}g) = \phi(g),$$

$$\implies \phi(1_{G_1}) = 1_{G_2}.$$

$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1_{G_1}) = 1_{G_2},$$

$$\implies \phi(g^{-1}) = \phi(g)^{-1}.$$

Legyen $\phi(g_1) = h_1$, $\phi(g_2) = h_2$. Ekkor

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) \in \text{Im}(\phi),$$

azaz $\text{Im}(\phi) \leq G_2$, mivel azt már korábban láttuk, hogy egy elemmel együtt az inverze is benne van a képen.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Legyen $\phi(g_1) = \phi(g_2) = 1_{G_2}$ Ekkor

$$\phi(g_1 g_2) = \phi(g_1) \phi(g_2) = 1_{G_2},$$

$\phi(g_1^{-1}) \in \text{Ker}(\phi), \implies \text{Ker}(\phi) \leq G_1$. Legyen $h \in G_1$. Ekkor

$$\phi(h^{-1}gh) = \phi(h^{-1}) \phi(g) \phi(h) = \phi(h^{-1}) 1_{G_2} \phi(h) = 1_{G_2},$$

tehát $\text{Ker}(\phi)$ normálosztó is.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Természetes homomorfizmus

Homomorfizmus \leftrightarrow Normálosztó

20. Állítás. Legyen $N \triangleleft G$. Ekkor a

$$\phi: G \rightarrow G/N$$

$$g \rightarrow Ng$$

leképezés homomorfizmus. A homomorfizmus magja N , képe G/N . Ezt a leképezést G -nek G/N -re való **természetes homomorfizmusának** nevezzük.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

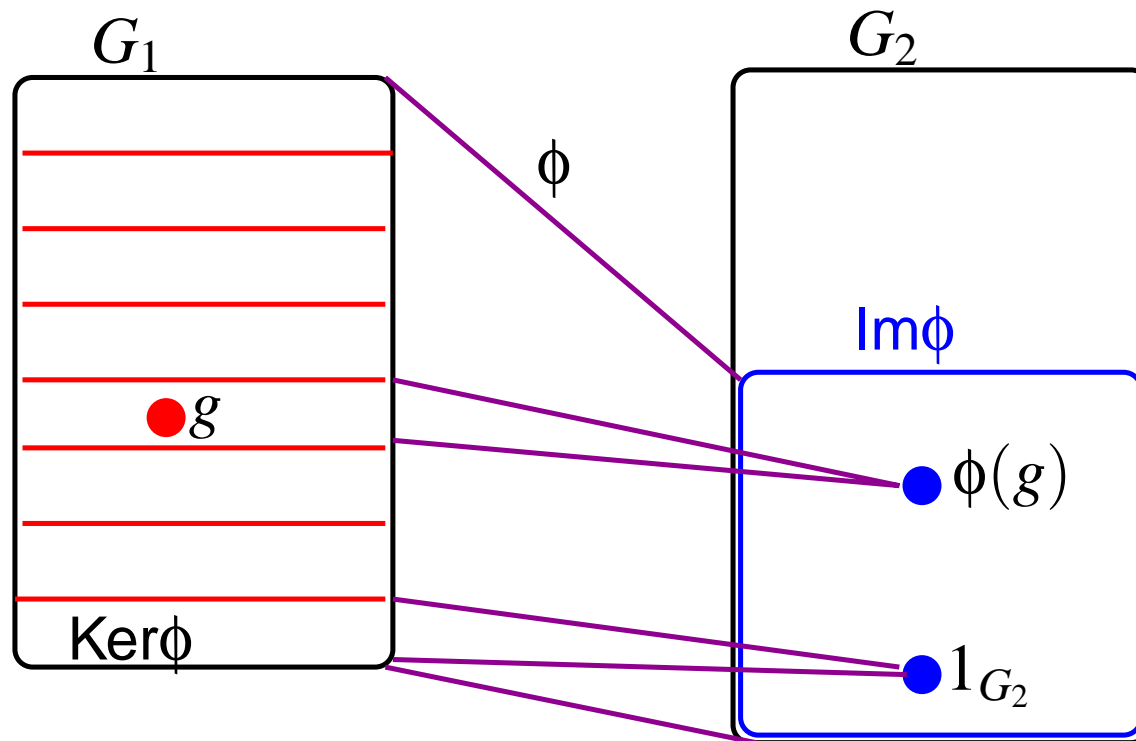
Homomorfizmus tétel

21. Tétel (homomorfizmus tétel). Legyen $\phi: G_1 \rightarrow G_2$ homomorfizmus. Ekkor

$$G_1 / \text{Ker}(\phi) \simeq \text{Im}(\phi).$$

Emlékezzünk a dimenzió tételre!

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$



$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Bizonyítás

$$\sigma: \text{Im}(\phi) \rightarrow G_1/\text{Ker}(\phi), \sigma(\phi(g)) = \text{Ker}(\phi)g$$

σ izomorfizmus: 1. Legyen $g \in \text{Im}(\phi)$ tetszőleges, $x \in G_1$ olyan, hogy $\phi(x) = g$, $h \in \text{Ker}(\phi) \implies \phi(h) = 1_{G_2}$ miatt $\phi(xh) = \phi(x)\phi(h) = g \implies \phi$ leképezésénél a $\text{Ker}(\phi)x$ mellékosztály minden eleme ugyanabba az elembe, g -be képződik.

2. $\phi(y) = g \implies \phi(yx^{-1}) = \phi(y)\phi(x^{-1}) = gg^{-1} = 1_{G_2}$, azaz $yx^{-1} = k \in \text{Ker}(\phi)$, $y = kx$, azaz y benne van az x szerinti (jobboldali) mellékosztályban, $\implies \text{Im}(\phi)$ tetszőleges elemébe $\text{Ker}(\phi)$ egyetlen mellékosztálya képződik le. \implies Tehát σ kölcsönösen egyértelmű.

3. σ művelettartó: Legyen ugyanis $\sigma(x') = \text{Ker}(\phi)x$ $\sigma(y') = \text{Ker}(\phi)y \implies \phi(x) = x' \phi(y) = y'$, ezért $\phi(xy) = \phi(x)\phi(y) = x'y' \implies \sigma(x'y') = xy\text{Ker}(\phi) = x\text{Ker}(\phi)y\text{Ker}(\phi) = \sigma(x')\sigma(y') \implies \sigma$ izomorfizmus.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Példák

$\text{Im}(\phi) \simeq G/\text{Ker}(\phi)$ miatt $|G| = |\text{Im}(\phi)| |\text{Ker}(\phi)|$, tehát $|\text{Im}(\phi)|$ osztja $|G|$ -t.

1. Tetszőleges G csoportra $G/\{1\} \simeq G$.
2. $(\mathbb{C}, +)/i(\mathbb{R}, +) \simeq (\mathbb{R}, +)$, hisz itt a 0-ba a tiszta képzetes számok képződnek.
3. A 3. példában a mag az 1 determinánsú mátrixokból $(SL(n, \mathbb{R}))$ áll, azaz $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$ és $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq (\mathbb{R} \setminus \{0\}, \cdot)$.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Permutációcsoportok

n elem összes permutációja csoportot alkot a kompozícióra, mint műveletre. Ezt S_n jelöli.

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

Permutációk szorzása:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

Nem kommutatív:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Ciklus

22. Definíció. Az (i_1, i_2, \dots, i_k) **ciklus**, ahol i_1, i_2, \dots, i_k különbözőek, azt a σ permutációt jelöli, amelynél i_1 i_2 -be, i_2 i_3 -ba, i_{k-1} i_k -ba, i_k pedig i_1 -be képződik, a többi elem helyben marad.

$$(i_1, i_2, \dots, i_k) = \begin{pmatrix} i_1 & i_2 & \dots & i_k \\ i_2 & i_3 & \dots & i_1 \end{pmatrix}$$

A permutációnál helyben maradó elemeket **fixpontoknak** nevezzük. A „kettes” ciklusokat $((i, j), i \neq j)$ **transzpozíciónak** nevezzük.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Ciklusokra bontás

Diszjunkt ciklusok felcserélhetőek, hiszen különböző elemeket mozgatnak.

23. Állítás. Minden permutáció előáll diszjunkt ciklusok szorzataként. Ez a felírás sorrendtől eltekintve egyértelmű.

Például

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 7 & 5 & 1 & 6 \end{pmatrix} = (1476)(23)(5).$$

A fixpontok (egy hosszú ciklusok) a ciklikus felírásnál elhagyhatók. Ekkor $\sigma = (1476)(23)$.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

S_n generálása

24. Tétel. Az $(1, 2), (1, 3), \dots, (1, n)$ transzpozíciók generálják S_n -et.

BIZONYÍTÁS $(i_1, i_2, \dots, i_k) = (i_1, i_2)(i_1, i_3) \dots (i_1, i_k)$, azaz minden ciklus (így minden permutáció) felírható transzpozíciók szorzataként. $(i, j) = (1, i)(1, j)(1, i)$

25. Tétel. $S_n = \langle (1, 2, \dots, n), (1, 2) \rangle$.

BIZONYÍTÁS $(2, \dots, n)(1, 2) = (1, 2, \dots, n)$ és $(2, \dots, n)^{-k+1}(1, 2)(2, \dots, n)^{k-1} = (1, k)$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \exists e \in G \forall a \in G: a \cdot e = e \cdot a = a \quad \forall a \in G \exists a' \in G: a \cdot a' = a' \cdot a = e$$

Páros permutációk – alternáló csoport

Páros permutációk szorzata is páros. $\implies A_n \leq S_n$, ahol A_n = Páros permutációk.

26. Tétel. $A_n \triangleleft S_n$, $|S_n : A_n| = 2$, azaz a páros permutációk normálosztót alkotnak S_n -ben, ennek indexe 2, így ugyanannyi páros permutáció van, mint páratlan.

BIZONYÍTÁS Tekintsük a

$$\begin{aligned} \phi: S_n &\rightarrow C_2 \\ \pi &\rightarrow \begin{cases} 1 & \text{ha } \pi \text{ páros} \\ a & \text{ha } \pi \text{ páratlan} \end{cases} \end{aligned}$$

leképezést.