

Algebra és számelmélet 5. jegyzet

Farkas Norbert Levente

2019. október 8.

Tartalomjegyzék

1. Emlék	1
1.1. Algebrai struktúrák	1
1.2. Normálosztó	4
2. Emlék	8
2.1. Faktorcsoporth	8
2.2. Direkt szorzat	11
3. Csoportelmélet	17
3.1. Centralizátor és centrum	17
3.2. Prímek és csoportok	21
3.3. Kürschák feladat	24
3.4. Kisméretű csoportok (1-8)	24

1. előadás

Emlék

1.1. Algebrai struktúrák

Számos algebrai struktúrával találkoztunk az elmúlt félévekben: csoport, gyűrű, test, vektortér. De mit jelent az, hogy algebrai struktúra? Egy halmaz és rajta értelmezett néhány művelet bizonyos megkötésekkel, axiómákkal. De mit jelent az, hogy művelet?

1.1.1. Definíció. Egy H halmazon értelmezett n változós **művelet** alatt egy

$$f : \overbrace{H \times H \times \dots \times H}^n \rightarrow H$$

n változós függvényt értünk.



Ismerünk olyan műveletet, hogy összeadás, például: $3 + 5 = 8$. Ez függvény formában is megfogalmazható. Adott a $+: \mathbb{R} \rightarrow \mathbb{R}$ függvény, melyre $+(3, 5) = 8$. Hasonló példaként $3 \cdot 5 = 15$ írható $\cdot(3, 5) = 15$ alakban.

Ismerünk egyváltozós műveleteket is, például az ellentett képzés: $-a$. De az is lehetséges, hogy egyetlen változótól sem függ valójában a függvény, vagyis az egy konstans, így $n = 0$ esetén konstans kijelöléséről beszélünk. Például ilyen mikor azt mondjuk, hogy $\exists 0$ nullelem.

Természetesen az egyes axiómák is könnyedén átfogalmazhatóak ezen szemlélet segítségével, például az asszociativitás axiómája: $a + (b + c) = (a + b) + c$ az eddigi szokásos felíráshoz képest $+(a + (b, c)) = +(+(a, b), c)$ alakra módosul.

1.1.2. Definíció. Legyen G halmazon definiálva egy kétváltozós művelet, ezt a továbbiakban szorzásnak hívjuk és \cdot jellel jelöljük. G halmazt **csoportnak** nevezzük, amennyiben teljesülnek a következők:

1. Asszociatív a szorzás: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. Létezik egységelem: $\exists e : \forall a \in G$ -re: $a \cdot e = e \cdot a = a$
3. Minden elemnek létezik inverze: $\forall a \in G : \exists a'$ melyre $a \cdot a' = a' \cdot a = e$



Jelölés: G csoport a szorzás műveletre: (G, \cdot) .

Megjegyzés. Amennyiben a csoporton nem egyetlen kétváltozós szorzás műveletet értelmeznénk, hanem emellett még egy egyváltozós inverzképzést és egy 0 változós nullelem konstans kijelölést, akkor elhagyhatóak lennének az egzisztenciális kvantorok a definícióból. Jelölésben: $(G, \cdot, {}^{-1}, e)$ csoport, amennyiben $\forall a, b, c \in G$ esetén teljesül, hogy

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $a \cdot e = e \cdot a = a$
3. $a \cdot a^{-1} = a^{-1} \cdot a = e$

Amennyiben $\forall a, b \in G$ -re teljesül, hogy $ab = ba$, akkor G csoportot kommutatív csoportnak, vagy **Ábel-csoport**nak neveztük.

1.1.1. Példa. Csoport $(\mathbb{Z}_n, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, sőt általában T test esetén $(T, +)$ is. Amennyiben a 0 elemet elhagyjuk, mely sértené azt az axiómát, hogy minden elemnek kell legyen inverze, akkor már $(T \setminus \{0\}, \cdot)$ is csoport. Tanultunk korábban S_n permutációcsoportokról, a páros permutációk A_n csoportjáról, szimmetriacsoportokról és speciálisan D_n az n oldalú szabályos sokszög szimmetria csoportjairól. Előkerült a K test feletti $n \times n$ -es invertálható mátrixok csoportja: $GL_n(K)$ is.

1.1.3. Definíció. Legyen R halmazon definiálva egy összeadás és egy szorzás, mindketten kétváltozós műveletek. Ekkor az R halmazt **gyűrűnek** nevezzük, amennyiben teljesülnek a következők:

1. $(R, +)$ Ábel-csoport¹:
 - Kommutativitás: $a + b = b + a$
 - Asszociativitás: $a + (b + c) = (a + b) + c$
 - Nullelem: $0 + a = a + 0 = a$
 - Ellentett: $a + a' = a' + a = 0$
2. Asszociatív a szorzás: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Disztributivitás: $(a + b) \cdot c = a \cdot c + b \cdot c$ és $a \cdot (b + c) = a \cdot b + a \cdot c$



Jelölés: $(R, +, \cdot)$ vagy $(R, +, -, \cdot, 0)$, ha ki szeretném hangsúlyozni az egyváltozós ellentettet és a nullelemet, mint nulla változós műveletet.

1.1.2. Példa. Gyűrű $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$, sőt általában T test esetén $(T, +, \cdot)$ is. A kvaterniók \mathbb{H} halmaza és $T[x]$, vagyis a T test feletti polinomok is gyűrűt alkotnak.

1.1.4. Definíció. Legyen T halmazon definiálva egy összeadás és egy szorzás, mindketten kétváltozós műveletek. Ekkor az T halmazt **testnek** nevezzük, amennyiben teljesülnek a következők:

1. $(T, +, \cdot)$ gyűrű:
 - Kommutatív az összeadás: $a + b = b + a$

¹Ha hangsúlyozni szeretnénk a mostani jelöléssel, akkor $(R, +, -, 0)$.

- Asszociatív a szorzás: $a + (b + c) = (a + b) + c$
- Nullelem: $\exists 0 : \forall a\text{-ra } 0 + a = a$
- Ellentett: $\forall a \exists a' : a + a' = 0$
- Asszociatív a szorzás: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Disztributivitás: $(a + b) \cdot c = a \cdot c + b \cdot c$

2. Kommutatív a szorzás: $a \cdot b = b \cdot a$

3. Egységelem: $\exists 1 : \forall a\text{-ra } 1 \cdot a = a$

4. Inverz: $\forall a \neq 0 : \exists a' \text{ melyre } a \cdot a' = 1$



1.1.3. Példa. Test \mathbb{R} , \mathbb{Q} , \mathbb{C} , vagy bármelyik testbővítés.

Ha $ab = ba$ nem teljesül bármely $a, b \in T$ elemekre, akkor T -t ferdetestnek nevezzük.

1.1.5. Definíció. Legyen V halmaz és T test, valamint definiálva egy összeadás V elemein és $\lambda \in T$ és $\mathbf{v} \in V$ elemekre egy $\lambda \cdot \mathbf{v}$ skalárral való szorzás². A V halmazt **vektortérnek** nevezzük, amennyiben teljesülnek a következők:

1. $(V, +)$ Ábel-csoport:

- Kommutativitás: $\mathbf{v} + \mathbf{u} = \mathbf{u} + \mathbf{v}$
- Asszociativitás: $\mathbf{v} + (\mathbf{u} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
- Nullelem: $\exists \mathbf{0} : \forall \mathbf{v}\text{-re } \mathbf{0} + \mathbf{v} = \mathbf{v}$
- Ellentett: $\forall \mathbf{v} : \exists \mathbf{v}' \text{ melyre } \mathbf{v} + \mathbf{v}' = \mathbf{0}$

2. $\lambda \cdot (\mu \cdot \mathbf{v}) = (\lambda \cdot \mu) \cdot \mathbf{v}$

3. $(\lambda + \mu) \cdot \mathbf{v} = \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{v}$

4. $\lambda \cdot (\mathbf{v} + \mathbf{u}) = \lambda \cdot \mathbf{v} + \lambda \cdot \mathbf{u}$

5. Egységelem: $1 \cdot \mathbf{v} = \mathbf{v}$



Említettük korábban is, hogy ezen 8 axióma egyike levezethető a másik 7 segítségével, nevezetesen a kommutativitás. Számoljuk ki kétféleképpen a következő értéket: $\mathbf{v} = (1 + 1) \cdot (\mathbf{a} + \mathbf{b})$.

Felhasználva a 3. axiómát ez nem más, mint

$$\mathbf{v} = 1 \cdot (\mathbf{a} + \mathbf{b}) + 1 \cdot (\mathbf{a} + \mathbf{b})$$

majd a 4. axióma szerint ez

$$\mathbf{v} = 1 \cdot \mathbf{a} + 1 \cdot \mathbf{b} + 1 \cdot \mathbf{a} + 1 \cdot \mathbf{b}$$

végül 5. axiómát használva

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

²Vagyis most sok egyváltozós műveletünk van, bármelyik λ -val való szorzása egy V -beli elemnek tekinthető egy önálló egyváltozós műveletnek.

Fordítva használva az első két axiómát viszont azt kapjuk, hogy

$$\mathbf{v} \stackrel{4.}{=} (1+1) \cdot \mathbf{a} + (1+1) \cdot \mathbf{b} \stackrel{3.}{=} 1 \cdot \mathbf{a} + 1 \cdot \mathbf{a} + 1 \cdot \mathbf{b} + 1 \cdot \mathbf{b} \stackrel{5.}{=} \mathbf{a} + \mathbf{a} + \mathbf{b} + \mathbf{b}$$

Így azt kaptuk, hogy

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

ahonnan baloldaltól kivonva \mathbf{a} -t és jobboldaltól \mathbf{b} -t adódik, hogy $\mathbf{b} + \mathbf{a} = \mathbf{a} + \mathbf{b}$.

Így tehát az összeadás kommutativitása **függ** a többi axiómától (levezethető belőlük), de beláthatjuk azt is, hogy az 5. axióma **független** a többitől. Ezt úgy lehet megmutatni, hogy mutatunk egy olyan konstrukciót, amikor nem teljesül, pedig az összes többi axióma igen.

Legyen például a skalárral való szorzás művelet definíciója a következő: $\forall \lambda \in T, \mathbf{v} \in V$ esetén $\lambda \cdot \mathbf{v} = \mathbf{0}$. Ekkor ha $\mathbf{v} \neq \mathbf{0}$ akkor speciálisan $\lambda = 1$ egységelemére a testnek nem teljesül, hogy $1 \cdot \mathbf{v} = \mathbf{v}$, ugyanakkor a többi axióma könnyen láthatóan teljesül. Ahol nem szerepel ez a művelet az nyilvánvalóan nem változik semmit, ahol szerepel (2., 3. és 4.) ott pedig mindkét oldalon $\mathbf{0}$ áll, tehát teljesülnek azok is.

1.2. Normálosztó

Beszéltünk korábban részcsoportokról, mellékosztályokról és ciklikus csoportról is.

Azt mondtuk, hogy egy $H \leq G$ részcsoportnak a $g \in H$ elem szerinti jobboldali mellékosztálya $H \cdot g = \{h \cdot g \mid h \in H\}$.

Definiáltunk egy relációt is G -n, mely szerint $g_1 \sim g_2$ akkor és csak akkor, ha $g_1 \cdot g_2^{-1} \in H$ és beláttuk, hogy ez egy ekvivalencia reláció G -n és az ekvivalencia osztályok éppen H -nak a jobboldali mellékosztályai. Így $g_1 \sim g_2 \Leftrightarrow H \cdot g_1 = H \cdot g_2$.

Definiáltuk csoportokra (és más struktúrára is) a homomorfizmus fogalmát, mely röviden fogalmazva művelettartó leképezés. Egy $\varphi : G_1 \rightarrow G_2$ leképezés homomorfizmus, amennyiben $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$.

Beláttuk, hogy ekkor egységelem egységelembe képződik, valamint inverz képe a kép inverze:

$$\varphi(e_1) = e_2 \quad \text{és} \quad \varphi(g^{-1}) = (\varphi(g))^{-1}$$

Esett szó a leképezés magjáról és képéről, $\text{Ker } \varphi$ és $\text{Im } \varphi$ -ről is. A mag azon G_1 -beli elemek halmaza melyek egységelembe képződnek, a kép pedig azon G_2 -beli elemeké, melyek előállnak képként.

Beláttuk, hogy $\text{Ker } \varphi$ részcsoport, hiszen zárt a szorzásra és az inverz képzésre. Ugyanis amennyiben $g_1, g_2 \in \text{Ker } \varphi$ akkor $g_1 \cdot g_2 \in \text{Ker } \varphi$ és $g_1^{-1} \in \text{Ker } \varphi$, hiszen

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) = e_2 \cdot e_2 = e_2$$

és

$$\varphi(g_1^{-1}) = (\varphi(g_1))^{-1} = e_2^{-1} = e_2$$

1.2.1. Tétel. A mag mellékosztályai megfelelnek a kép elemeinek.



Bizonyítás. Azt kell belátni, hogy g_1 és g_2 csoportelemek pontosan akkor vannak $\text{Ker } \varphi$ ugyanazon mellékosztályában, amennyiben ugyanoda képződnek. Induljunk ki abból, hogy mikor egyezik meg két elem képe, és jussunk el ekvivalens átalakításokkal oda, hogy ez a két elem biztosan ugyanazon mellékosztályában van $\text{Ker } \varphi$ -nek. Legyen $\varphi(g_1) = \varphi(g_2)$. Ekkor jobbról szorozva $\varphi(g_2^{-1})$ -zel:

$$\varphi(g_1) \cdot \varphi(g_2^{-1}) = \varphi(g_2) \cdot \varphi(g_2^{-1}) = \varphi(g_2 \cdot g_2^{-1}) = \varphi(e_1) = e_2$$

így $\varphi(g_1 \cdot g_2^{-1}) = e_2$ ami éppen azt jelenti, hogy $g_1 \cdot g_2^{-1} \in \text{Ker } \varphi$. Ahogy az előbbieken felidézttük, ez pontosan akkor teljesül, ha $g_1 \sim g_2$ vagyis $\text{Ker } \varphi$ -nek g_1 és g_2 szerinti jobboldali mellékosztálya megegyezik:

$$\text{Ker } \varphi \cdot g_1 = \text{Ker } \varphi \cdot g_2$$

Ezt akartuk belátni. ■

Beszéltünk általánosan a generálás fogalmáról: egy adott G algebrai struktúra S részhalmaza által generált halmaz azon legszűkebb, adott algebrai struktúra, mely tartalmazza S -et. Másképp fogalmazva az S -et tartalmazó adott struktúrájú részhalmazok metszete:

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H$$

Ez a definíció érvényes csoportra, gyűrűre, testre, vektortérre egyaránt. Természetesen be kell hozzá látni, hogy például csoportok esetében részcsoportok metszete is részcsoport lesz.

Az egy elem által generált csoportokat ciklikus csoportnak neveztük:

$$\langle g \rangle = \{ \dots, g^{-2}, g^{-1}, 1, g, g^2, \dots, g^n, \dots \}$$

Egy elem rendje a legkisebb pozitív egész kitevő melyre az elemet emelve egységelemet kapunk. Ez lehet véges, ha létezik ilyen szám, és végtelen ha nem létezik. Láttuk Algebra3-ból, hogy \mathbb{Z}_n^* , vagyis a redukált maradékosztályok csoportot alkotnak a szorzásra. Majd Algebra4-ből kimondtuk (és $n = p$ esetén be is láttuk), hogy $n = p^\alpha$ esetében létezik primitív gyök, ami azzal a tulajdonsággal rendelkezik, hogy $\varphi(n)$ a rendje, éppen ami a \mathbb{Z}_n^* csoport elemszáma. Mivel a rend a különböző hatványok száma, így ennek a primitív gyöknek $\varphi(n)$ különböző hatványa létezik, vagyis egy primitív gyök előállítja, generálja a teljes \mathbb{Z}_n^* csoportot. Így tehát ha modulo n létezik primitív gyök, akkor \mathbb{Z}_n^* ciklikus csoport.

Ha $o(g) = n < \infty$ akkor $\langle g \rangle = \{1, g, \dots, g^n\}$.

Definiáltunk egy újabb relációt is. Azt mondtuk, hogy $g_1 \sim g_2$ egymás konjugáltjai³, amennyiben $\exists h$ melyre $h^{-1} \cdot g_1 \cdot h = g_2$. Beláttuk, hogy jogos az "egymás konjugáltjai" kifejezés, ez is egy ekvivalencia reláció, így ez is meghatároz egy felosztást G -ben, beszélhetünk konjugátosztályokról.

Egy G csoport H részcsoportja zárt a szorzásra és inverzképzésre, így a csoporton belüli elemekkel való konjugálásra is. Különleges tulajdonságú az olyan részcsoport, mely a bővebb G csoportbeli elemekkel vett konjugálásra is zárt.

1.2.1. Definíció. Egy $N \leq G$ normálosztó G -ben, amennyiben $\forall x \in G$ -re $x^{-1} \cdot N \cdot x = N$ teljesül. Jelölés: $N \triangleleft G$. ♣

³A g elem x -szel vett konjugáltja alatt az $x^{-1} \cdot g \cdot x$ elemet értjük.

1.2.2. Tétel. Az $N \leq G$ csoport normálosztó tulajdonságának ekvivalens megfogalmazásai:

1. Definíció: $\forall x \in G$ -re $x^{-1} \cdot N \cdot x = N$
2. $\forall g \in N$ -re és $\forall x \in G$ -re $x^{-1} \cdot g \cdot x \in N$.
3. $N \leq G$ és N előáll konjugált osztályok uniojaként.
4. $\forall x \in G$ -re $x^{-1} \cdot N \cdot x \subset N$
5. Létezik olyan homomorfizmus, aminek a magja: $\exists \varphi : G \rightarrow G'$ homomorfizmus, melyre $\text{Ker } \varphi = N$.



Bizonyítás. Csak az első négy ekvivalenciáját bizonyítjuk most be.

4. *biz:*

Az 1. \Rightarrow 4. triviális, ha egyenlőek, akkor nyilván a részhalmaz tulajdonság is teljesül. Azt kellene belátnunk, hogy fordítva is igaz a tartalmazás, vagyis $N \subset x^{-1} \cdot N \cdot x$. Ehhez azt kellene belátni, hogy $\forall g \in N$ esetén $g \in x^{-1} \cdot N \cdot x$.

Mit használhatunk fel hozzá? Azt, hogy $x^{-1} \cdot N \cdot x \subset N$ vagyis $g \in x^{-1} \cdot N \cdot x \Rightarrow g \in N$. Tartsuk észben, hogy mivel ez minden x -re teljesül, így speciálisan $x := x^{-1}$ -re is, ami azt jelenti, hogy $g \in x \cdot N \cdot x^{-1} \Rightarrow g \in N$.

A bizonyítandóhoz kiindulunk onnan, hogy $g \in N$. Ekkor persze $x \cdot g \cdot x^{-1} \in x \cdot N \cdot x^{-1}$. Az előző hasznos észrevétel miatt ekkor $x \cdot g \cdot x^{-1} \in N$. Viszont ekkor

$$x^{-1} \cdot x \cdot g \cdot x^{-1} \cdot x = g \in x^{-1} \cdot N \cdot x$$

Ezt kellett bizonyítanunk.

2. *biz:*

Az 1. \Rightarrow 2. triviális, hiszen ha $g \in N$ akkor $x^{-1} \cdot g \cdot x \in x^{-1} \cdot N \cdot x \stackrel{1.}{=} N$.

Ha viszont teljesül 2., vagyis $g \in N \Rightarrow x^{-1} \cdot g \cdot x \in N$, az éppen azt jelenti, hogy $x^{-1} \cdot N \cdot x \subset N$, vagyis teljesül 4.

3. *biz:*

A 2. \Rightarrow 3. azért igaz, mert 2. szerint ha egy elem benne van a csoportban, akkor annak minden konjugáltja is, tehát az adott g elem egész konjugáltosztálya. Ezek szerint N minden elemének teljes konjugált osztályát is tartalmazza, vagyis N előáll elemeinek konjugált osztályainak uniojaként.

Fordítva ha N előáll konjugált osztályok uniojaként, akkor bármely elemére igaz, hogy annak teljes konjugált osztályát tartalmazza, így $g \in N$ esetén benne van annak tetszőleges x -szel vett konjugáltja is, tehát $x^{-1} \cdot g \cdot x \in N$, amivel így láttuk a 3. \Rightarrow 2. irányt is. ■

1.2.1. Állítás. Egy $\varphi : G_1 \rightarrow G_2$ homomorfizmus $\text{Ker } \varphi$ magja mindig normálosztó. ♣

Bizonyítás. Láttuk, hogy $\text{Ker } \varphi$ zárt az összeadásra és inverzképzésre, vagyis részcsoport, azt kellene még bizonyítani, hogy zárt a külső elemmel vett konjugálásra is. Ez könnyen látható,

hiszen $x \in G_1$ és $g \in \text{Ker } \varphi$ esetén:

$$\varphi(x^{-1} \cdot g \cdot x) = \varphi(x^{-1}) \cdot \varphi(g) \cdot \varphi(x) = \varphi(x^{-1}) \cdot e_2 \cdot \varphi(x) = \varphi(x^{-1}) \cdot \varphi(x) = \varphi(x^{-1} \cdot x) = \varphi(e_1) = e_2$$

így tehát $x^{-1} \cdot g \cdot x \in \text{Ker } \varphi$, ami éppen azt jelenti, hogy zárt a konjugálásra, vagyis normálosztó. ■

1.2.2. Definíció. Legyenek A és B részcsoportjai G -nek. Ekkor A és B **komplexusszorzatán** az $A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$ halmazt értjük. ♣

Például $H \cdot H$ komplexusszorzat maga a H lesz, hiszen $H \cdot H = \{a \cdot b \mid a, b \in H\}$. Mivel $b = 1$ választással megkapjuk a teljes H -t, így $H \subset H \cdot H$, ugyanakkor mivel $\forall g \in H \cdot H$ elemre teljesül, hogy $g \in H$, így $H \cdot H \subset H$ is teljesül, ami azt jelenti, hogy a két halmaz éppen megegyezik: $H \cdot H = H$.

1.2.3. Tétel. Ha $N \triangleleft G$, akkor N -nek a mellékosztályai csoportot alkotnak a komplexusszorzásra, mint műveletre. ♣

Bizonyítás. Lássuk be először, hogy zárt a komplexusszorzásra, vagyis hogy $N \cdot g_1$ és $N \cdot g_2$ elemek szorzata is N normálosztónak egy jobboldali mellékosztálya.

Mivel N normálosztó, így definíció szerint $N = x^{-1} \cdot N \cdot x$ bármely x -re, így tehát speciálisan $x = g_1$ választással $N = g_1^{-1} \cdot N \cdot g_1$. Vagyis az elemek szorzata:

$$N \cdot g_1 \cdot N \cdot g_2 = N \cdot g_1 \cdot g_1^{-1} \cdot N \cdot g_1 \cdot g_2 = N \cdot N \cdot g_1 \cdot g_2 = N \cdot g_1 \cdot g_2$$

Így tehát teljesül a **zárttság** a szorzásra.

Egységelem létezését sem nehéz bizonyítani, melynek megfelel maga N , hiszen tetszőleges $N \cdot g$ mellékosztályt megszorozva N mellékosztállyal, az önmaga marad:

$$N \cdot g \cdot N = N \cdot g \cdot g^{-1} \cdot N \cdot g = N \cdot N \cdot g = N \cdot g$$

Inverz létezését is könnyű igazolni: $(N \cdot g)^{-1} = N \cdot g^{-1}$. Ugyanis szorzatuk

$$N \cdot g \cdot N \cdot g^{-1} = N \cdot (g \cdot g^{-1}) = N \cdot e = N$$

és az N most az egységelem.

Az is könnyen látható, hogy a szorzás **asszociatív**, hiszen:

$$N \cdot a \cdot (N \cdot b \cdot N \cdot c) = N \cdot a \cdot N \cdot b \cdot c = N \cdot a \cdot (b \cdot c)$$

és

$$(N \cdot a \cdot N \cdot b) \cdot N \cdot c = N \cdot a \cdot b \cdot N \cdot c = N \cdot (a \cdot b) \cdot c$$

melyek megegyeznek, hiszen $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. ■

1.2.3. Definíció. Az $N \triangleleft G$ mellékosztályai által alkotott csoportot G -nek az N -szerinti **faktor-csoportjának** nevezzük. Jelölés: G/N . ♣

Megjegyzés. A faktorcsoport elemei halmazok! Ilyen „állatfajta” nem igazán volt dolgunk korábban: egy halmaz, melynek elemei halmazok.

2. előadás

Emlék

2.1. Faktorcsoporthoz

Múlt órán láttuk, hogy normálosztó két mellékosztályának szorzata mindig mellékosztály lesz és normálosztók szerinti mellékosztályok a (komplexus)szorzásra nézve csoportot alkotnak, erre vezettük be a faktorcsoporthoz elvezést és jelöltük: G/N -nel:

$$G/N = \{N \cdot g \mid g \in G\}$$

A jelölés egy osztásra hasonlít, ami nem véletlen, hiszen Lagrange-tétele szerint mivel $N \leq G$ így $|N| \mid |G|$ és $|G| = |N| \cdot |G : N|$ esetén a $|G : N|$ számot neveztük N -nek a G -beli indexének, vagyis ez adta meg az N részcsoport szerinti mellékosztályok számát. Tehát hány mellékosztály volt? Amennyi $|G : N| = \frac{|G|}{|N|}$. Innen származik a faktorcsoporthoz jelölése is, mely azt igyekszik kifejezni, hogy ebben éppen a G csoportnak az N szerinti mellékosztályai vannak, így jele G/N , számossága pedig $\frac{|G|}{|N|}$.

2.1.1. Tétel (Homomorfizmustétel). Legyen $\varphi: G \rightarrow H$ homomorfizmus. Ekkor $\text{Ker } \varphi \triangleleft G$ és $G/\text{Ker } \varphi \cong \text{Im } \varphi$. ♣

Bizonyítás. Az első részt, vagyis a mag normálosztó tulajdonságát már múlt órán beláttuk, az csupán azért szerepel, hogy beszélhessünk $G/\text{Ker } \varphi$ faktorcsoporthozról.

Ugyebár $G/\text{Ker } \varphi$ a mag szerinti mellékosztályok csoportja, melyekről korábban már beláttuk 1.2.1. tételben, hogy megfelelnek a kép elemeinek. Ez azt jelenti, hogy az izomorfizmusnak a bijekció részét kipipálhatjuk, már csak egy $\psi: \text{Ker } \varphi \rightarrow \text{Im } \varphi$ homomorfizmust kell mutatnunk. A továbbiakban $N = \text{Ker } \varphi$ rövidítést használom. Azt állítom, hogy $g \in G$ esetén $\psi(N \cdot g) = \varphi(g)$ jó lesz!

Ehhez annyit kell csupán belátnunk, hogy ψ művelettartó:

$$\psi(N \cdot g_1 \cdot N \cdot g_2) = \psi(N \cdot g_1 \cdot g_2) = \varphi(g_1 \cdot g_2)$$

valamint

$$\psi(N \cdot g_1) \cdot \psi(N \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

vagyis mivel φ homomorfizmus, így $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$ teljesül, így $\psi(N \cdot g_1 \cdot N \cdot g_2) = \psi(N \cdot g_1) \cdot \psi(N \cdot g_2)$, tehát ψ művelettartó leképezés. ■

2.1.1. Példa. Egy A ábel-csoport bármely $H \leq A$ részcsoportha normálosztó. Ez nyilvánvaló, hiszen ábel-csoportban a szorzás kommutativitása miatt $a \in H$ és $x \in A$ esetén $x^{-1} \cdot a \cdot x = a \cdot x^{-1} \cdot x = a \cdot e = a \in H$, vagyis a múlt órai 1.2.2. tétel 2. pontja alapján mivel zárt a bővebb csoportbeli elemmel való konjugálásra, így $H \triangleleft A$.

2.1.2. Példa. D_n esetén $\langle f \rangle \triangleleft D_n$, vagyis a forgatások részcsoportha normálosztó. Azt kell hozzá csak belátni, hogy egy forgatást forgatással vagy tükrözéssel konjugálva mindenképp forgatást kapok. Ez szemléletesen látszik, hiszen egy forgatást akár forgatással, akár 2 tükrözéssel szorozok, irányítás tartó transzformációt kapok, vagyis forgatást. Ha valaki számolással szeretné ezt látni: $f^n \in \langle f \rangle$ forgatást egy f^k forgatással konjugálva:

$$(f^k)^{-1} \cdot f^n \cdot f^k = f^n$$

forgatást, ha pedig $f^k \cdot t$ tükrözéssel konjugálom

$$(f^k \cdot t)^{-1} \cdot f^n \cdot f^k \cdot t = t \cdot f^{-k} \cdot f^n \cdot f^k \cdot t = t \cdot f^n \cdot t = f^{-n}$$

forgatást kapom. Így tehát a forgatások részcsoportha zárt a konjugálásra, tehát normálosztó.

Azt is megállapíthatjuk, hogy D_n -nek az $\langle f \rangle$ szerinti faktorcsoportha számossága: $|D_n / \langle f \rangle| = |D_n| / |\langle f \rangle| = \frac{2n}{n} = 2$. Mivel minden 2 elemű csoport izomorf \mathbb{Z}_2 -vel, így $D_n / \langle f \rangle \cong \mathbb{Z}_2$.

Hogyan találhattuk volna ezt ki, ha nem egy kételemű csoportot kaptunk volna? Hogyan tudunk normálosztót keresni? Megadunk egy homomorfizmust és annak a magja biztosan normálosztó, a faktorcsoporth pedig izomorf lesz a képpel a homomorfizmustétel alapján. Nézzük meg újra ezt a példát egy másik szempontból.

2.1.3. Példa. Olyan homomorfizmust kellene találnunk, ami a forgatások részcsoporthát egységelembe képi. Milyen tulajdonságát tudnánk kiemelni a forgatásoknak, amely a tükrözésekre biztosan nem lenne igaz? (Tehát csak a forgatásokat képezzék egységelembe.) Például az összes forgatás irányítás tartó, tükrözések viszont váltóak. Definiáljuk a következő leképezést:

$$\varphi: D_n \rightarrow \mathbb{Z}_2, \quad \varphi(g) = \begin{cases} 1, & \text{ha irányítástartó} \\ -1, & \text{ha irányításváltó} \end{cases}$$

Azt állítom, hogy φ homomorfizmus. Geometriából megtanultuk, hogy két transzformáció szorzata csakis akkor lehet irányítástartó, ha mindkét transzformáció egyszerre tartó vagy egyszerre váltó. Ennyi indoklás elegendő is ahhoz, hogy ez valóban egy homomorfizmus, de akinek van kedve és ideje hozzá, az itt is végignézheti a 4 esetet és beláthatja, hogy $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

- $a = f^n, b = f^k$ esetén:

$$\varphi(a \cdot b) = \varphi(f^{n+k}) = 1 \quad \varphi(a) \cdot \varphi(b) = \varphi(f^n) \cdot \varphi(f^k) = 1 \cdot 1 = 1$$

- $a = f^n, b = f^k \cdot t$ esetén:

$$\varphi(a \cdot b) = \varphi(f^{n+k} \cdot t) = -1 \quad \varphi(a) \cdot \varphi(b) = \varphi(f^n) \cdot \varphi(f^k \cdot t) = 1 \cdot (-1) = -1$$

- $a = f^n \cdot t$, $b = f^k$ esetén:

$$\varphi(a \cdot b) = \varphi(f^{n-k} \cdot t) = -1 \quad \varphi(a) \cdot \varphi(b) = \varphi(f^n \cdot t) \cdot \varphi(f^k) = (-1) \cdot 1 = -1$$

- $a = f^n \cdot t$, $b = f^k \cdot t$ esetén:

$$\varphi(a \cdot b) = \varphi(f^{n-k}) = 1 \quad \varphi(a) \cdot \varphi(b) = \varphi(f^n \cdot t) \cdot \varphi(f^k \cdot t) = (-1) \cdot (-1) = 1$$

Nézzünk néhány további példát homomorfizmusra. Tekintsük most $GL_n(K)$ -t, vagyis az általános lineáris csoportot. Erről algebra3-ból tanultunk és a K test feletti $n \times n$ -es invertálható mátrixok csoportját jelölte (vagyis melyek determinánsa 0-tól különböző). Könnyen látható, hogy $M \in GL_n(K)$ esetén homomorfizmusok a következő leképezések:

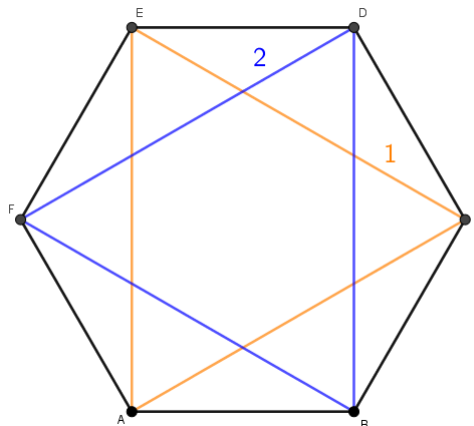
$$\varphi_1(M) = 1 \quad \varphi_2(M) = M \quad \varphi_3(M) = \det M$$

sőt $\varphi_4(M) = (M^T)^{-1}$ is. Az első kettő teljesen triviális, hogy művelettartó, a harmadik pedig a determinánsok szorzástétele miatt homomorfizmus. A legutolsó belátáshoz arra kell visszaemlékeznünk, hogy algebra2-ből tanultuk, hogy $(A \cdot B)^T = B^T \cdot A^T$. Emiatt:

$$\varphi_4(A \cdot B) = ((A \cdot B)^T)^{-1} = (B^T \cdot A^T)^{-1} = (A^T)^{-1} \cdot (B^T)^{-1} = \varphi_4(A) \cdot \varphi_4(B)$$

Algebra3-ból sokat vizsgáltuk a csoporthatásokat, melyek speciális homomorfizmusok, amik képhalmaza egy S_X permutációcsoport. Vizsgáltuk anno, hogy a hatszög szimmetriáinak csoportja, vagyis D_6 hat a hatszögbe írható 2 szabályos háromszög X halmazán és a 3 főátló Y halmazán is. Mi a mag az egyes esetekben és mi lesz D_6 -nak a mag szerinti faktorcsoportha?

Tekintsük először a háromszögek esetét!



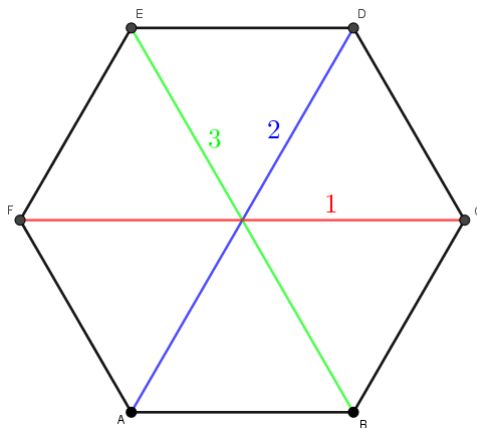
Adott tehát $\varphi: D_6 \rightarrow S_2$ hatás. Mi lesz a mag? Ami helyben hagyja mindkét háromszöget, más-képpen mondva ami a sárga háromszöget helyben hagyja (hiszen ekkor a kék is automatikusan marad). Például benne van a magban az identitás, f^2 , vagy f^4 is ahol f a 60° -os forgatás. De helyben hagyja őket az FB szakaszfelező merőlegesére való t tengelyes tükrözés is és ekkor persze $f^2 \cdot t$ és $f^4 \cdot t$ is. Összefoglalva:

$$\text{Ker } \varphi = \{id., f^2, f^4, t, f^2 \cdot t, f^4 \cdot t\}$$

Másképpen mondva a sárga háromszöget a sárga háromszög szimmetriái hagyják helyben, ezek éppen D_3 elemei, vagyis $\text{Ker } \varphi \cong D_3$.

Mivel a képtér S_2 , így a homomorfizmus-tétel alapján azt kaptuk, hogy $D_6/D_3 \cong S_2$.

Nézzük most a főátlók esetét!



Itt most $\varphi: D_6 \rightarrow S_3$. Ebben az esetben azt látjuk, hogy ami helyben hagyja mindhárom átlót az csupán 2 szimmetria: id és f^3 . Vagyis a mag: $\text{Ker } \varphi = \{id, f^3\} \cong \mathbb{Z}_2$.

Belátható, hogy S_3 minden eleme a képtérnek is eleme, például a $(2\ 3)$ benne van, hiszen az FC egyenesére tükrözés képe éppen ez. Hasonlóan látható, hogy az összes többi transzpozíció is benne van, mivel pedig bármely elem előáll transzpozíciók szorzataként, így a teljes S_3 lesz a kép.

Most tehát a homomorfizmus-tétel szerint $D_6/\mathbb{Z}_2 \cong S_3$.

Könnyen belátható, hogy bármely G csoportnak van legalább 2 normálosztója, hiszen $\{1\} \triangleleft G$ és $G \triangleleft G$. Ezeket szokás **triviális normálosztóknak** nevezni.

2.1.1. Definíció. Egy G csoport **egyszerű**, ha a két triviális normálosztóján kívül más normálosztója nincs. ♣

Algebra és számelmélet 3 tárgyából láttuk korábban, hogy egyszerű csoport A_5 .

2.1.2. Tétel (Feit-Thompson-tétel). Ha van egy páratlan elemű egyszerű csoportunk, az csak a \mathbb{Z}_p lehet, vagyis G egyszerű csoport esetén $2 \nmid |G| \Rightarrow \exists p$ prím, melyre $G \cong \mathbb{Z}_p$. ♣

2.2. Direkt szorzat

A direkt szorzatról is már tanultunk algebra3-ból, így ez a fejezet is lényegében ismétlés csupán.

2.2.1. Definíció. Az A és B halmazok direkt szorzata az A és B elemeiből képzett rendezett párok halmaza: $A \times B = \{(a, b) \mid a \in A, b \in B\}$ ♣

Azt is beláttuk korábban, hogy amennyiben A és B csoportok és definiálunk $A \times B$ elemein egy szorzást a következőképpen: $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$, akkor az $A \times B$ halmaz csoportot alkot erre a szorzásra.

Ennek bizonyítását most nem írom le újra, de a hozzá kapcsoló, előadáson ismét elhangzó tételeket igen, illetve emlék gyanánt az inverzképzés szabályát: $(a, b)^{-1} = (a^{-1}, b^{-1})$.

2.2.1. Lemma. Legyen G csoport, melyben $A, B \triangleleft G$ normálosztók. Amennyiben a halmazok komplexusszorzata $A \cdot B = G$, akkor

1. $A \cap B = \{1\}$

2. G csoport minden eleme egyértelműen áll elő egy A és egy B beli elem szorzataként állítások ekvivalensek. ♣

Bizonyítás. Külön-külön látjuk be a két irányt.

1. \Rightarrow 2. *bizonyítása:*

Annak jelentése, hogy $A \cdot B = G$ nem más, mint hogy $\forall g \in G$ esetén \exists olyan $a \in A$ és $b \in B$, melyekre $a \cdot b = g$. Azt kell belátni, hogy a és b egyértelmű is!

Tegyük fel, hogy létezik $a_1, a_2 \in A$ és $b_1, b_2 \in B$ melyek mindketten előállítják g -t, vagyis

$$a_1 \cdot b_1 = g = a_2 \cdot b_2$$

balról a_1^{-1} -zel, jobbról b_2^{-1} -zel szorozva:

$$b_1 \cdot b_2^{-1} = a_1^{-1} \cdot a_2$$

Viszont itt $b_1 \cdot b_2^{-1} \in B$ és $a_1^{-1} \cdot a_2 \in A$, ami azt jelenti, hogy mivel ez a két elem egymással egyenlő, ezért mindkét halmaznak eleme, tehát a metszetnek is. De a metszet egyetlen eleme az 1, amiből következően:

$$b_1 \cdot b_2^{-1} = 1 = a_1^{-1} \cdot a_2$$

ahonnan látszik, hogy $a_1 = a_2$ és $b_1 = b_2$, tehát tényleg egyértelmű az előállítás.

2. \Rightarrow 1. *bizonyítása:*

Indirekt tegyük fel, hogy A és B halmazoknak van más közös eleme is az 1-en kívül, legyen ez $g \neq 1$. Ekkor azt állítom, hogy ellentmondást kapunk, mert g kétféleképpen is előállítható, mégpedig:

$$g = g \cdot 1 = 1 \cdot g$$

ami azt jelenti, hogy az $a_1 = g, b_1 = 1$ és $a_2 = 1, b_2 = g$ különböző előállításai g -nek, hiszen $a_1 \neq a_2$ és $b_1 \neq b_2$. ■

2.2.2. Lemma. Legyen G csoport, melyben $A, B \triangleleft G$ normálosztók. Ha $A \cap B = \{1\}$, akkor $\forall a \in A, b \in B$ -re $a \cdot b = b \cdot a$. ♣

Bizonyítás. Tekintsük a következő szorzatot:

$$b^{-1} \cdot a \cdot b \cdot a^{-1}$$

Na most ha $a \in A$ és $b \in B \Rightarrow b \in G$, akkor mivel A normálosztó G -ben, ezért rajta kívüli, G -beli elemekkel is zárt a konjugálásra, ami azt jelenti, hogy $b^{-1} \cdot a \cdot b \in A$, továbbá zárt inverzképzésre, tehát $a^{-1} \in A$, vagyis akkor ez az egész szorzat A -nak eleme. Akkor ennek a szorzatnak az inverze is eleme A -nak:

$$(b^{-1} \cdot a \cdot b \cdot a^{-1})^{-1} = a \cdot b^{-1} \cdot a^{-1} \cdot b$$

Tekintsünk most erre B szempontjából. Ott van egy $b^{-1} \in B$ elem megkonjugálva $a^{-1} \in A$ elemmel: $(a^{-1})^{-1} \cdot b^{-1} \cdot a^{-1}$, ez eleme B -nek, továbbá b is. Tehát ez a valami B -nek is eleme és láttuk, hogy A -nak is.

Mivel pedig $A \cap B = \{1\}$, ez csakis akkor lehetséges, ha ez maga az egységelem, akkor viszont a bal oldali valami is az egységelem volt, aminek az inverzét vettük (hiszen csak az egységelem inverze lehet az egységelem):

$$b^{-1} \cdot a \cdot b \cdot a^{-1} = 1$$

ahonnan balról szorozva b -vel, jobbról a -val adódik, hogy

$$a \cdot b = b \cdot a$$

Éppen ezt akartuk. ■

2.2.1. Tétel. Legyen G csoport az A és B csoportok direkt szorzata: $G = A \times B$, tekintsük $A' = \{(a, 1) \mid a \in A, 1 \in B\}$ és $B' = \{(1, b) \mid 1 \in A, b \in B\}$ halmazokat. Ekkor

1. $A', B' \triangleleft G$
2. $A' \cap B' = \{(1, 1)\}$
3. $A' \cdot B' = G$

állítások teljesülnek. ♣

Bizonyítás. Csak $A' \triangleleft G$ állítást látom be, B' -re hasonlóan megy. Az nyilvánvaló, hogy $A' \leq G$, hiszen

- részhalmaza, mert az összes (a, b) pár közül csak azokat tartalmazza, ahol $b = 1$
- egységelem benne van $a = 1$ választással
- zárt a szorzásra: $(a_1, 1) \cdot (a_2, 1) = (a_1 \cdot a_2, 1) \in A'$, mert $a_1 \cdot a_2 \in A$
- zárt az inverzképzésre: $(a, 1)^{-1} = (a^{-1}, 1) \in A'$, mert $a^{-1} \in A$

Tehát azt kell még belátni, hogy zárt a konjugálásra G -ben, kell: $\forall a' \in A'$ és $g \in G$ esetén $g^{-1} \cdot a' \cdot g \in A'$. Legyen $a' = (a, 1)$ és $g = (x, y)$, ekkor

$$g^{-1} \cdot a' \cdot g = (x^{-1}, y^{-1}) \cdot (a, 1) \cdot (x, y) = (x^{-1} \cdot a \cdot x, y^{-1} \cdot 1 \cdot y) = (x^{-1} \cdot a \cdot x, 1) \in A'$$

mert $x^{-1} \cdot a \cdot x \in A$.

2. *biz:* Ez nyilvánvaló, amennyiben (x, y) elem benne van mindkét halmazban, akkor mindkét koordinátája 1 kell legyen.

3. *biz:* Ez sem bonyolult, mivel A' és B' részcsoport G -ben, ezért elemeik szorzata nyilván nem vezethet kívül G -n, azt kell csak megmutatni, hogy minden G -beli elem előáll egy A' -beli és

egy B' -beli szorzataként. Ha az ellenség ad egy G belüli (x, y) elemet, akkor mi azt mondjuk neki, hogy $(x, 1) \in A'$ és $(1, y) \in B'$ és

$$(x, 1) \cdot (1, y) = (x \cdot 1, 1 \cdot y) = (x, y)$$

tehát minden elem előáll szorzatként. ■

2.2.2. Tétel. Legyen G csoport, melyben van olyan A és B részcsoport, melyekre

1. $A, B \triangleleft G$
2. $A \cap B = \{1\}$
3. $A \cdot B = G$

akkor $G \cong A \times B$. ♣

Bizonyítás. Izomorfizmus igazolásához meg kell adjunk egy bijektív leképezést a bal és jobb oldal között és igazoljuk, hogy szorzattartó. Legyen $(a, b) \in A \times B$, ekkor $\varphi((a, b)) = a \cdot b$ azt állítom, hogy jó leképezés lesz.

Bijektív, mert minden $a \cdot b$ előáll képként (szürjektív) és a 2. tulajdonság és a 2.2.1. lemmánk miatt, minden $x \in G$ egyértelműen áll elő (a, b) képe, vagyis $a \cdot b$ alakban (injektív).

Szorzattartás igazolása: Kell, hogy ha $(a, b) \in A \times B$ és $(c, d) \in A \times B$, akkor szorzat képe a képek szorzata, vagyis

$$\varphi((a, b) \cdot (c, d)) = \varphi((a, b)) \cdot \varphi((c, d))$$

bal oldalon elvégezve belül a szorzást

$$\varphi((ac, bd)) = \varphi((a, b)) \cdot \varphi((c, d))$$

φ általunk adott definíciója

$$(ac) \cdot (bd) = (ab) \cdot (cd)$$

Csoportelemekről beszélünk, elhagyhatók a zárójelek és balról a^{-1} -zel, jobbról d^{-1} -zel szorozva egyszerűsödik a kifejezés

$$c \cdot b = b \cdot c$$

kellene teljesülnön és mivel végig ekvivalens átalakításokat csináltunk, ezért akkor a szorzattartás igaz volna. De hát ez teljesül is a tétel feltételei között megint csak a 2-es pont és a korábbi 2.2.2. lemmánk miatt A és B elemei között kommutatív a szorzás, kész vagyunk. ■

Vegyük észre, hogy a bijekció miatt G és $A \times B$ csoportnak ugyanannyi eleme van, sőt meg is feleltethetőek egymásnak. Azért kellett mégis izomorfizmust írunk, mert a két csoport struktúrája hasonló, de nem ugyanaz! Az $A \times B$ -ben G elemeiből képezett rendezett párok vannak. Ugyanakkor az egyértelmű megfeleltetés miatt definiálhattuk volna $A \times B$ -t úgy is, hogy az is G elemeiből álljon. Éppen ezért a továbbiakban nem teszünk különbséget aközött, hogy $G \cong A \times B$ vagy $G = A \times B$.

2.2.1. Példa. Mutassuk meg, hogy $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$.

1. Mivel Ábel-csoport esetén bármely részcsoport normálosztó, így $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ csoport normálosztója $\mathbb{Z}_2 = \{0, 3\}$ és $\mathbb{Z}_3 = \{0, 2, 4\}$.

2. Teljesül, hogy közös elemük csak az egységelem, tehát $\mathbb{Z}_2 \cap \mathbb{Z}_3 = \{0\}$.
3. Sőt az is igaz, hogy szorzatuk $\mathbb{Z}_2 \cdot \mathbb{Z}_3 = \mathbb{Z}_6$, hiszen \mathbb{Z}_2 másik (a 3-as) eleme \mathbb{Z}_3 -nak nem eleme, így 6 féle különböző szorzat képezhető elemeikből, vagyis \mathbb{Z}_6 minden eleme előállítható.

Az előző tétel szerint ekkor $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$.

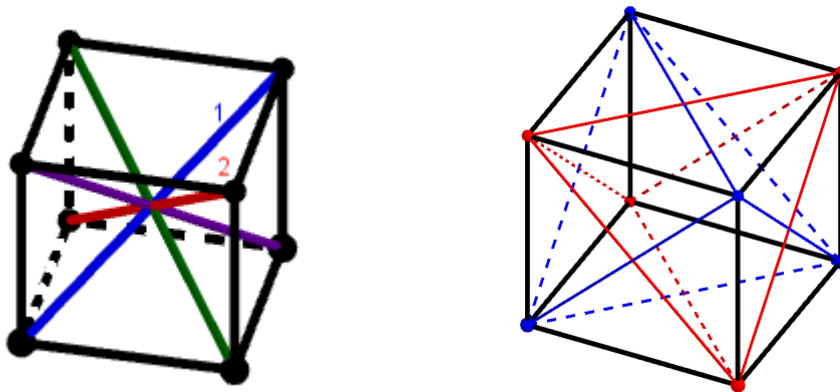
2.2.2. Példa. Lássuk be, hogy $D_6 = \mathbb{Z}_2 \times D_3$.

Foglalkoztunk korábban a hatszög szimmetriáinak csoportjával és azt láttuk, hogy a háromszögek esetében is hatást kapunk, melynek magja $\text{Ker } \varphi \cong D_3$ -mal, illetve átlók esetében $\text{Ker } \varphi \cong \mathbb{Z}_2$.

1. Mivel a mag mindig normálosztó, így $\mathbb{Z}_2 \triangleleft D_6$ és $D_3 \triangleleft D_6$.
2. Teljesül, hogy közös elemük csupán az identitás, tehát $D_3 \cap \mathbb{Z}_2 = \{id.\}$.
3. Sőt az is igaz, hogy szorzatuk $\mathbb{Z}_2 \cdot D_3 = D_6$, hiszen \mathbb{Z}_2 másik (vagyis f^3) eleme D_3 -nak nem eleme, így 12 féle különböző szorzat képezhető elemeikből, vagyis D_6 minden eleme előállítható.

Az előző tétel szerint ekkor $D_6 = \mathbb{Z}_2 \times D_3$.

Tanultuk tavaly, hogy a kocka szimmetriái (amiből 48 van) hat a testátlók és a beírt tetraéderek halmazán is.



A testátlók esetében belátható, hogy a magban csupán 2 transzformáció lesz: a helybenhagyás és a középpontos tükrözés: $\text{Ker } \varphi = \{id., k\} \cong \mathbb{Z}_2$.

Tetraéderek esetében pedig az lesz a mag, ami az egyik tetraédert helyben hagyja (hiszen akkor a másik is helyben marad), vagyis a tetraéder szimmetriáinak csoportja: S_4 .

2.2.3. Példa. Bizonyítsuk be, hogy a kocka szimmetriáinak K csoportjára $K = \mathbb{Z}_2 \times S_4$.

1. Mivel a mag mindig normálosztó, így $\mathbb{Z}_2 \triangleleft K$ és $S_4 \triangleleft K$.
2. Teljesül, hogy közös elemük csupán az identitás (hiszen a középpontos tükrözés pont megcseréli a tetraédereket), tehát $\mathbb{Z}_2 \cap S_4 = \{id.\}$.
3. Sőt az is igaz, hogy szorzatuk $\mathbb{Z}_2 \cdot S_4 = K$, hiszen \mathbb{Z}_2 másik (vagyis k) eleme S_4 -nek nem eleme, így 48 féle különböző szorzat képezhető elemeikből, vagyis K minden eleme előállítható.

Most is teljesül a három feltétel, tehát $K = \mathbb{Z}_2 \times S_4$.

2.2.3. Tétel (Ábel-csoportok alaptétele). Ha A Ábel-csoport, akkor A előáll a következő alakban:

$$A = \mathbb{Z}_{p_1}^{\alpha_1} \times \mathbb{Z}_{p_2}^{\alpha_2} \times \dots \times \mathbb{Z}_{p_k}^{\alpha_k}$$

ahol $\forall p_i$ prím és a felbontás a prímszámok erejéig egyértelmű (tehát maga a felbontás nem egyértelmű, de a prímszámok igen). ♣

Például $\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$, hiszen $6 = 2^1 \cdot 3^1$. Hasonlóan mondhatjuk, hogy mivel $18 = 2^1 \cdot 3^2$, így $\mathbb{Z}_{18} = \mathbb{Z}_2 \times \mathbb{Z}_9$.

3. előadás

Csoportelmélet

3.1. Centralizátor és centrum

Tanultunk korábban a konjugálás műveletéről, jelölésben használtuk h -nak a g -vel vett konjugáltjára a $g^{-1} \cdot h \cdot g$ jelölést és a h^g jelölést is. Utóbbi a hatványozás művelete miatt megtévesztő lehet, így amennyiben lehetséges én a továbbiakban mellőzöm a használatát.

Volt szó arról, hogy a konjugálás ekvivalencia reláció, így osztályokra bontja a G csoportot, ezeket neveztük **konjugátosztályoknak**:


$$\mathcal{K}(a) = \{b \in G \mid \exists x \in G: x^{-1} \cdot g \cdot x = b\}$$

vagyis egy g elem konjugátosztályán azon elemek halmazát értjük, melyekbe "átkonjugálódhat", vagy másképp fogalmazva eljuthat konjugálás által.

3.1.1. Definíció. Egy $a \in G$ csoportelem **centralizátorán** azon csoportbeli elemek halmazát értjük, melyekkel a felcserélhető a csoporton definiált szorzás műveletére:

$$C_G(a) = \{h \in G \mid a \cdot h = h \cdot a\}$$



3.1.1. Tétel. Egy $a \in G$ elem centralizátora mindig részcsoportot alkot G -ben: $C_G(a) \leq G$. 

Bizonyítás. Részcsoport teszt: zártság szorzásra, inverzképzésre, egységelemet tartalmazza-e:

- Nyilván $1 \in C_G(a)$ hiszen $1 \cdot a = a \cdot 1$ teljesül $\forall a \in G$ esetén.
- Szorzásra zártság: $g, h \in C_G(a)$, vagyis $ga = ag$ és $ha = ah$, kellene $g \cdot h \in C_G(a)$, vagyis $gh \cdot a = a \cdot gh$ ami nyilván teljesül, hiszen egyesével elvégezve a cseréket $gh \cdot a = g \cdot a \cdot h = a \cdot gh$
- Inverzképzésre zártság: $g \in C_G(a)$, vagyis $ga = ag$ esetén természetesen mindkét oldalról g^{-1} -zel szorozva kapjuk, hogy $a \cdot g^{-1} = g^{-1} \cdot a$, ami éppen azt jelenti, hogy $g^{-1} \in C_G(a)$.



Észrevétel: a centralizátor elemei éppen azok, amelyek átkonjugálják az a elemet önmagába, hiszen ha $ah = ha$ akkor $h^{-1} \cdot a \cdot h = a$ teljesül.

3.1.2. Tétel. Az $a \in G$ elem esetén $|\mathcal{K}(a)| \cdot |C_G(a)| = |G|$. ♣

Bizonyítás. Ha már $C_G(a) \leq G$, akkor beszélhetünk a centralizátor jobboldali mellékosztályairól. Könnyen belátható, hogy az egyes jobboldali mellékosztályok elemeinek van egy közös tulajdonsága: mindannyian ugyanoda konjugálják az a elemet. Vagyis $x \in C_G(a) \cdot y$ esetén x és y -nal képzett konjugáltja a -nak megegyezik.

Ez könnyen látható, hiszen $x \in C_G(a) \cdot y$ esetén $x \cdot y^{-1} \in C_G(a)$, vagyis $x \cdot y^{-1}$ elemmel felcserélhető az a elem, azaz:

$$x \cdot y^{-1} \cdot a = a \cdot x \cdot y^{-1}$$

balról x^{-1} -el, jobbról y -al szorozva $x^{-1} \cdot a \cdot x = y^{-1} \cdot a \cdot y$ adódik, vagyis éppen azt kapjuk, hogy a -nak az x és y szerinti konjugáltja megegyezik.

Ezek alapján a G csoportnak a $C_G(a)$ részcsoport szerint éppen annyi mellékosztálya van, ahány konjugáltja a elemnek, vagyis a mellékosztályok száma a konjugáltosztályának elemszáma: $|\mathcal{K}(a)|$.

Lagrange-tétele alapján a csoport elemszáma megegyezik egy részcsoport elemszámának és azon részcsoport szerinti mellékosztályok számának szorzatával, így: $|\mathcal{K}| \cdot |C_G(a)| = |G|$. ■

Ezen utóbbi tétel egy másik megfogalmazása a következő.

3.1.3. Tétel. Egy G csoport hat önmagán konjugálással, vagyis $\varphi: G \rightarrow S_G$ leképezés, melyre $\varphi(g) = \pi \in S_G$, melyre $\pi(h) = g^{-1} \cdot h \cdot g$ permutáció egy homomorfizmus. ♣

Bizonyítás. Van most egy furcsa φ leképezésünk, mely minden csoportbeli elemhez egy olyan permutációt rendel, mely esetén minden csoportbeli elem képe a g -vel vett konjugáltja. Tehát most φ egy g elemhez hatás lévén egy függvényt rendel! Azt kell belátnunk, hogy művelettartóan teszi mindezt.

- Szorzástartó: Kellene, hogy g_1 és g_2 elemek esetén $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$. Mit rendel g_1 -hez φ ? Egy olyan permutációt, amely minden h elemhez a konjugáltját rendeli. Hasonlóan g_2 esetében:

$$\varphi(g_1) = h \rightarrow g_1^{-1} \cdot h \cdot g_1 \quad \text{és} \quad \varphi(g_2) = h \rightarrow g_2^{-1} \cdot h \cdot g_2$$

Mi lesz ekkor $\varphi(g_1) \cdot \varphi(g_2)$? Egyszerűen az elemekhez rendelt permutációkat is össze kell "szoroznunk", ami permutációk esetén természetesen kompozíciót jelent: az első h -t elviszi $g_1^{-1} \cdot h \cdot g_1$ -be, majd a második ezt az elemet konjugálja tovább:

$$\varphi(g_1) \cdot \varphi(g_2) = h \rightarrow g_1^{-1} \cdot h \cdot g_1 \rightarrow g_2^{-1} \cdot g_1^{-1} \cdot h \cdot g_1 \cdot g_2 = h \rightarrow g_2^{-1} \cdot g_1^{-1} \cdot h \cdot g_1 \cdot g_2$$

átírva az inverzet:

$$= (g_1 \cdot g_2)^{-1} \cdot h \cdot g_1 \cdot g_2 = \varphi(g_1 \cdot g_2)$$

- Inverztartó: Kellene, hogy $\varphi(g)^{-1} = \varphi(g^{-1})$:

$$\varphi(g)^{-1} = (h \rightarrow g^{-1} \cdot h \cdot g)^{-1} = g^{-1} \cdot h \cdot g \rightarrow h = h \rightarrow g \cdot h \cdot g^{-1} = \varphi(g^{-1})$$

Egy a elem pályáján azon G -beli elemeket értettük, ahová φ hatás által eljuthat a . Vagyis a $g^{-1} \cdot a \cdot g$ elemek halmazát, így ebben az esetben az orbit éppen az a elem konjugáltosztálya lesz: $\mathcal{K}(a)$.

Másik fontos észrevétel, hogy, mely elemek hagyják fixen a -t? Vagyis melyek azon $g \in G$ elemek, melyekkel képzett konjugáltja önmaga? Ezek éppen a centralizátor elemei, tehát jelenlegi φ csoporthatás esetén egy $a \in G$ elem stabilizátora éppen a centralizátora: $C_G(a)$.

És az orbit-stabilizátor lemma szerint ismét megkaptuk az előző tétel állítását, vagyis, hogy $|\mathcal{K}(a)| \cdot |C_G(a)| = |G|$. ■

Emlék: Egy $(1 \ 2 \ \dots \ n)$ ciklus konjugáltja egy σ permutációval:

$$\sigma^{-1} \cdot (1 \ 2 \ \dots \ n) \cdot \sigma = (\sigma(1) \ \sigma(2) \ \dots \ \sigma(n))$$

3.1.1. Példa. Határozzuk meg S_4 -ben $\pi = (1 \ 2 \ 3 \ 4)$ permutáció centralizátorát!

Tudjuk, hogy a centralizátor azon σ permutációk halmaza, melyekkel felcserélhető, vagyis

$$(1 \ 2 \ 3 \ 4) \cdot \sigma = \sigma \cdot (1 \ 2 \ 3 \ 4)$$

vagyis azon σ permutáció, mely önmagába konjugálja:

$$\sigma^{-1} \cdot (1 \ 2 \ 3 \ 4) \cdot \sigma = (1 \ 2 \ 3 \ 4) = (\sigma(1) \ \sigma(2) \ \sigma(3) \ \sigma(4))$$

Ha $(1 \ 2 \ 3 \ 4)$ permutáció konjugáltja is ugyanezen ciklus kell legyen, akkor σ négyféleképpen választható meg:

$$\sigma = id. \quad \text{vagy} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \text{vagy} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \text{vagy} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

így tehát a $\sigma = (1 \ 2 \ 3 \ 4)$ permutáció centralizátora négy elemű, elemei a lehetséges σ permutációk, avagy $(1 \ 2 \ 3 \ 4)$ hatványai, hiszen egy ciklus a saját hatványaival mindig felcserélhető.

Másképpen is megállapíthattuk volna ezt, például ha centralizátora helyett konjugáltosztályát vizsgáljuk. Tudjuk, hogy egy permutáció konjugáltja azonos ciklus szerkezetű, ezért $(1 \ 2 \ 3 \ 4)$ konjugáltosztályában 4 hosszú ciklusok szerepelnek. Hány darab van belőlük? Hányféleképpen lehet 4 elemet ciklikusan permutálni? Rögzítjük az első helyét, majd a második helyre 3 féle elem kerülhet, a harmadik helyre 2 féle, majd végül az utolsóra 1 féle, így $3 \cdot 2 \cdot 1 = 6$ elemű a konjugáltosztálya. Mivel $|S_4| = 24$, így a 3.1.2. tétel alapján

$$|C_G((1 \ 2 \ 3 \ 4))| = \frac{|S_4|}{|\mathcal{K}((1 \ 2 \ 3 \ 4))|} = \frac{24}{6} = 4$$

ahonnan ismét látjuk, hogy $(1 \ 2 \ 3 \ 4)$ centralizátorában 4 elem van csupán, és mivel saját hatványaival mindig felcserélhető, így centralizátora a hatványaiából álló (generált ciklikus) részcsoporthoz $C_{S_4}((1 \ 2 \ 3 \ 4)) = \langle (1 \ 2 \ 3 \ 4) \rangle$.

Mit kapok ha veszem minden $a \in G$ elem centralizátorának a metszetét? Olyan elemeket, amelyek G bármely elemével felcserélhetőek, ezek halmazát szokás centrumnak nevezni.

3.1.2. Definíció. Egy G csoport **centruma** alatt a $Z(G) = \{g \in G \mid \forall h \in G: gh = hg\}$ halmazt értjük. ♣

3.1.4. Tétel. Csoport centruma normálosztója a csoportnak: $Z(G) \triangleleft G$. ♣

Bizonyítás. Be kell látnunk, hogy részcsoport és zárt a konjugálásra.

- Szorzásra zárt: $g_1, g_2 \in Z(G)$ esetén $\forall h \in G$ -re $g_1 \cdot h = h \cdot g_1$ és $g_2 \cdot h = h \cdot g_2$ teljesül, így

$$g_1 \cdot g_2 \cdot h = g_1 \cdot h \cdot g_2 = h \cdot g_1 \cdot g_2$$

miatt $g_1 \cdot g_2 \in Z(G)$

- Egységelem benne van nyilván: $1 \in Z(G)$
- Inverzképzésre zárt: $g \in Z(G)$ esetén $\forall h \in G$ -re $gh = hg$, vagyis mindkét oldalról g^{-1} -zel szorozva $h \cdot g^{-1} = g^{-1} \cdot h$, így $g^{-1} \in Z(G)$.
- Konjugálásra zárt: $g \in Z(G)$ esetén $x^{-1} \cdot g \cdot x \in Z(G)$, hiszen ha $g \in Z(G)$ akkor $gx = xg$, vagyis $x^{-1} \cdot g \cdot x = x^{-1} \cdot x \cdot g = g \in Z(G)$. Megjegyzés: Centrumbeli elemek konjugáltosztálya egyelemű, így mikor azt kérdezzük, hogy g centrumbeli elem összes konjugáltja benne van-e $Z(G)$ -ben, akkor nyilvánvalóan igen, hiszen egyetlen konjugáltja önmaga.

■

3.1.2. Példa. Határozzuk meg $Z(S_4)$ -et!

A centrum elemei minden csoportbeli elemmel felcserélhetőek, így egy centrumbeli elem felcserélhető kell legyen konkrétan a $\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$ ciklussal is, mellyel láttuk, hogy csak saját hatványai cserélhetők fel, így $Z(G) \subseteq \langle \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \rangle$. Ugyanakkor hasonlóan elmondható ez $\begin{pmatrix} 1 & 3 & 2 & 4 \end{pmatrix}$ ciklussal is, így az általa generált ciklikus csoportnak is részhalmaza a centrum. Igen ám, csak hogy ezen két darab 4 elemű csoportoknak egyetlen közös eleme az identitás, így $Z(G) = \{id.\}$.

Megjegyzés. Az előző példa elmondható lett volna tetszőleges S_n esetében, így a permutációcsoportok centruma nem túlságosan izgalmas: $Z(S_n) = \{id.\}$.

3.1.3. Példa. Határozzuk meg D_4 és D_5 centrumát!

Lehet-e egy tükrözés a centrumban? Nem lehet, mivel egy tükrözés nem cserélhető fel minden elemmel, hiszen minden tükrözés esetén tudunk mondani legalább egy olyan másik tükrözést amellyel nem cserélhető fel, hiszen különböző sorrendben szorozva őket, különböző irányú forgatásokhoz jutunk.

Így tehát a centrumban biztosan csak fogatások lehetnek. Azok közül is csak különlegesek, hiszen egy f^n forgatás csakis akkor lehet a centrumban, amennyiben egy t tengelyes tükrözéssel felcserélhető, vagyis:

$$t \cdot f^n = f^n \cdot t$$

ugyanakkor tudjuk, hogy $t \cdot f^n = f^{-n} \cdot t$, tehát azt a szükséges feltételt kaptuk¹, hogy:

$$f^n \cot t = f^{-n} \cdot t$$

¹Ez egyben elégséges feltétel is, hiszen a forgatások felcserélhetők egymással.

amelyet t -vel egyszerűsítve $f^n = f^{-n}$ feltételhez jutunk, vagyis csakis olyan forgatás felelhet meg nekünk, amely önmaga inverze. Ilyet csak kettőt ismerünk, az identitást és a 180° -os forgatást, vagyis $Z(D_4) = \{id., f^2\}$.

Az ötszög szimmetriái esetében annyit változik a problémánk, hogy középpontos tükrözés nincs a diédercsoportban, így $Z(D_5) = \{id.\}$.

Megjegyzés. Hasonlóan meggondolva tetszőleges D_n diédercsoport centruma: $Z(D_{2n+1}) = \{id.\}$, illetve $Z(D_{2n}) = \{id., f^n\}$.

3.2. Prímek és csoportok

Lagrange tétele szerint ha $H \leq G$, akkor $|H| \mid |G|$. Igaz-e a tétel megfordítása olyan értelemben, hogy ha egy szám osztja a csoport rendjét, akkor létezik olyan részcsoporthoz, amelynek éppen az az elemszáma? Nem igaz, például belátható, hogy $|A_4| = \frac{4!}{2} = 12$ és $6 \mid 12$, de nem létezik A_4 -nek 6 elemű részcsoporthoz.

Hasonló kérdés merülhet fel elemrendek esetén, ugyanis tanultuk, hogy bármely elem rendje osztja a csoport rendjét: $a \in G$ esetén $o(a) \mid |G|$. Ugyanakkor az nem igaz, hogy ha $b \mid |G|$, akkor van olyan eleme G -nek, amelynek rendje éppen b . Például D_6 esetében $4 \mid 12 = |D_6|$, de nem létezik olyan elem D_6 -ban, amelynek rendje 4, hiszen a tükrözések rendje 2, a forgatásoké pedig $o(f) = 6$, $o(f^2) = 3$, $o(f^3) = 2$, $o(f^4) = 3$, és $o(f^5) = 6$. Ha viszont az osztó egy p prímszám, akkor már létezik p rendű elem.

3.2.1. Tétel (Cauchy). Ha $p \mid |G|$ akkor $\exists g \in G: o(g) = p$.



Bizonyítás. Képezzünk G elemeiből rendezett p -eseket a következő módon: (g_1, g_2, \dots, g_p) legyen egy rendezett p -es, akkor ha

$$g_1 \cdot g_2 \cdot \dots \cdot g_p = 1$$

Nyilvánvaló, hogy tudunk ilyen elem p -est képezni, például $\forall g_i = 1$ számunkra megfelelő.

Az is könnyen meghatározható, hogy hány darab ilyen tudunk képezni: tetszőlegesen megválaszthatjuk G elemei közül az első $p-1$ ilyen elemet, melyeket bárhogyan is választunk meg és $a = g_1 \cdot g_2 \cdot \dots \cdot g_{p-1}$ szorzatukat tekintjük, az utolsó g_p elem mindig egyértelműen megválasztható lesz $g_p = a^{-1}$. Éppen ezért annyi ilyen elem p -est tudunk készíteni, ahányféleképpen az első $p-1$ elem megválasztható, tehát: $|G|^{p-1}$.

Hasznos észrevétel, hogy ha (g_1, g_2, \dots, g_p) egy számunkra megfelelő p -es volt, akkor jó lesz (g_2, \dots, g_p, g_1) is, hiszen balról g_1^{-1} -el, jobbról g_1 -vel szorozva:

$$g_1 \cdot g_2 \cdot \dots \cdot g_p = 1 \quad \Rightarrow \quad g_2 \cdot \dots \cdot g_p \cdot g_1 = g_1^{-1} \cdot g_1 = 1$$

Ez azt jelenti, hogy egy megfelelő rendezett p -est találva egyben annak ciklikus elforgatottjai is jó rendezett p -esek.

Hányféle különböző elforgatottja lehet egy rendezett p -esnek? Azt állítom, hogy vagy p vagy csak 1. Amennyiben ugyanis van neki 2 azonos elforgatottja, akkor könnyen belátható, hogy a rendezett p -es minden eleme megegyezik.

Például ha 3-al elforgatva egy rendezett p -est önmagát kapjuk, akkor

$$(g_1, g_2, g_3, g_4, g_5, g_6, g_7, \dots, g_p) = (g_4, g_5, g_6, g_7, \dots, g_p, g_1, g_2, g_3)$$

$g_1 = g_4$ illetve $g_4 = g_7$ és így tovább. Vagyis ha 3-al elforgatva önmagát kapom akkor minden elem megegyezik az őt követő harmadikkal.

NODE! Akkor a_1 elemmel megegyezik bármely, tőle $3k$ -ra lévő elem, vagyis az összes $3k + 1$ indexű elem. Vagyis az a_1 elemmel azok az a_b elemek egyeznek meg, melyek esetén tudunk mondani olyan k -t, hogy $3k + 1 \equiv b \pmod{p}$. Könnyen látható, hogy ez bármely b esetén teljesül, hiszen $3k \equiv b - 1 \pmod{p}$ kongruencia mindig megoldható k -ra, mivel $(3, p) = 1$.

Ezzel tehát beláttuk, hogy egy rendezett p -es minden elforgatottja megegyezik, ha van két azonos eleme. Tehát innentől kezdve két esetet vizsgálunk, amikor a rendezett p -es minden eleme azonos, és amikor minden eleme különbözik.

Vannak olyan g elemek, amelyekből p darabot véve kapunk egy jó rendezett p -est melynek minden eleme azonos. Ez éppen azt jelenti, hogy $g^p = 1$. Nem tudjuk hány ilyen elem van, de egy darab biztosan, az 1. Továbbiakban jelölje x azon g elemek számát melyre teljesül $g^p = 1$.

Nézzük egy picit a másik esetet, amikor a rendezett p -es minden eleme különbözik. Hány darab ilyen van? Jelöljük ezt mondjuk y -al. Ha találunk egy p különböző elemből egy rendezett p -est, akkor annak bármely elforgatottja is jó rendezett p -es számunkra, tehát ha találunk egy jó, csupa különböző elemből álló rendezett p -est, akkor azzal együtt igazából p darabot találtunk egyszerre. Ez azt jelenti, hogy a különböző elemekből álló jó rendezett p -esek számát osztja p , vagyis: $p \mid y$.

Összesen hány jó p -es létezik? Kiszámoltuk, hogy $|G|^{p-1}$. De úgy is mondhatnánk, hogy ahány jó csupa azonos, és ahány jó csupa különböző elemű, vagyis

$$|G|^{p-1} = x + y$$

Most használjuk ki a tétel feltételét, hogy $p \mid |G|$, ekkor persze $p \mid |G|^{p-1}$ is teljesül, illetve láttuk, hogy $p \mid y$, így adódik az előbbi egyenletből, hogy $p \mid x$.

Viszont ez azt jelenti, hogy p osztja azon g elemek számát, melyeket p -edik hatványra emelve 1-et kapunk. Viszont mivel $p \nmid 1$, így ezek száma több mint 1, vagyis az 1 elemen kívül most már látjuk, hogy ténylegesen létezik még olyan $g \neq 1$ elem, melyre $g^p = 1$. Viszont ez azt is jelenti, hogy $o(g) = p$, hiszen g -re nézve a p egy jó kitevő, márpedig a jó kitevőket osztja a rend, tehát p osztójaként $o(g) = p$ vagy $o(g) = 1$ jöhet csak szóba, de utóbbi esetében $g = 1$ teljesülne, viszont mi olyan g -t is tudtunk választani, mely az egységelemtől különbözik. ■

Egy csoport centrumának mindig eleme az egységelem, hiszen az minden elemmel felcserélhető. Amennyiben egy csoport centruma csupán az 1 elemet tartalmazza, akkor a **triviális centrum** elnevezést szokás használni.

3.2.2. Tétel. Prímhatványrendű csoport centruma nem triviális: $|G| = p^n \Rightarrow |Z(G)| > 1$. ♣

Bizonyítás. Bontsuk fel a G csoportot konjugáltosztályok uniójára²:

$$G = \bigcup \mathcal{K}(a)$$

²Ezt az egyenletet neveztük előadáson **osztályegyenletnek** is.

Láttuk a 3.1.4. tételben, hogy a centrum is normálosztó, így $Z(G)$ is előáll konjugáltosztályok uniójaként. Válasszuk ebben az unióban két részre a halmazokat, vegyük azon a konjugáltosztályokat, melyek előállítják $Z(G)$ -t, illetve azokat, melyek elemei nem centrumbeliek:

$$G = Z(G) \cup \bigcup_{a \notin Z(G)} \mathcal{K}(a)$$

Ha ezek a halmazok megegyeznek, akkor számosságuk is, mivel pedig a jobboldali unióban szereplő halmazok diszjunktak, így uniójuk számossága a számosságaik összege:

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} |\mathcal{K}(a)|$$

Mivel $|G| = p^n$, és 3.1.2. tétel miatt $|\mathcal{K}(a)| \cdot |C_G(a)| = |G|$ teljesül, így $|\mathcal{K}(a)|$ csakis p^n osztója, vagyis prímszámhatvány lehet. Sőt még azt is tudjuk, hogy ha nem egy centrumbeli konjugáltosztályról van szó, akkor $|\mathcal{K}(a)| \neq 1$, hiszen ha a elem konjugáltosztálya egyelemű lenne, akkor minden elemmel felcserélhető lenne a , vagyis centrumbeli elem lenne. Ezek szerint p -vel osztható az összes $|\mathcal{K}(a)|$.

Viszont ekkor $p \mid |Z(G)|$ is teljesül, így $|Z(G)| > 1$. ■

3.2.3. Tétel. Ha egy G csoport H részcsoportjának indexe 2, akkor H normálosztó: $H \leq G$ és $|G : H| = 2 \Rightarrow H \triangleleft G$. ♣

Bizonyítás. Mivel H indexe 2, így H -nak két különböző (jobboldali) mellékosztálya van, vagyis $H \neq G$, így $\exists g \in G$, melyre $g \notin H$.

Ekkor $H \neq H \cdot g$, hiszen utóbbi tartalmazza g elemet, tehát mellékosztályokra bontva G csoportot: $G = H \cup H \cdot g$, másképp fogalmazva $H \cdot g = G \setminus H$.

Hasonlóan baloldali mellékosztállyal $H \neq g \cdot H$, hiszen utóbbi tartalmazza g elemet, tehát mellékosztályokra bontva: $G = H \cup g \cdot H$, másképp $g \cdot H = G \setminus H$.

Innen pedig azt kaptuk, hogy $H \cdot g = g \cdot H$, ami a normálosztó $g^{-1} \cdot H \cdot g = H$ tulajdonságnak egy ekvivalens átfogalmazása. ■

Megjegyzés. Másképp fogalmazva, ha találunk egy H részcsoportot, melynek elemszáma éppen $|H| = \frac{|G|}{2}$, akkor azonnal adódik, hogy az normálosztó is.

Érdekes észrevétel, hogy amennyiben G csoport kommutatív, akkor minden elem mindennel felcserélhető, tehát minden elem a centrumban van, így $Z(G) = G$. Mivel $Z(G)$ normálosztó, így tekinthetünk G -nek a $Z(G)$ szerinti faktorcsoportját, melynek elemszáma:

$$|G/Z(G)| = \frac{|G|}{|Z(G)|}$$

vagyis jelen esetben 1, mégpedig egyetlen eleme $Z(G) = G$. Ekkor persze ez az egyelemű $\{G\}$ csoport ciklikus de ez nem túl izgalmas, mert az 1 elemű csoportról sok érdekeset nem tudunk megállapítani. Tekintsük helyette azt, amikor G nem kommutatív.

3.2.4. Tétel. Tetszőleges G nemkommutatív csoport esetén $G/Z(G)$ nem ciklikus. ♣

Bizonyítás. Indirekt tegyük fel, hogy G nem kommutatív, de $G/Z(G)$ mégis ciklikus. Ekkor $\exists a \in G$, melyre $Z(G) \cdot a$ generálja a faktorcsoportot, vagyis melyre

$$G/Z(G) = \langle Z(G) \cdot a \rangle = \{Z(G), Z(G) \cdot a, Z(G) \cdot a^2, \dots, Z(G) \cdot a^{n-1}\}$$

Ekkor G csoportot előállítva $Z(G)$ részcsoport szerinti mellékosztályok uniójaként:

$$G = \bigcup_{i=0}^{n-1} Z(G) \cdot a^i$$

Mivel tetszőleges $g_1 \in G$ benne van valamelyik mellékosztályban, így $\exists z_1 \in Z(G)$ és a^i , melyre $g_1 = z_1 \cdot a^i$. Hasonlóan $g_2 \in G$ esetén $g_2 = z_2 \cdot a^j$. Ekkor viszont használva, hogy z_1, z_2 centrum-beli elemek, tehát bármivel felcserélhetőek:

$$g_1 \cdot g_2 = z_1 \cdot a^i \cdot z_2 \cdot a^j = z_1 \cdot z_2 \cdot a^i \cdot a^j = z_2 \cdot z_1 \cdot a^{i+j} = z_2 \cdot z_1 \cdot a^j \cdot a^i = z_2 \cdot a^j \cdot z_1 \cdot a^i = g_2 \cdot g_1$$

Vagyis azt kaptuk, hogy ekkor G csoport tetszőleges g_1, g_2 eleme felcserélhető egymással, tehát G kommutatív, ami ellentmondás, hiszen feltettük, hogy nem az. ■

3.3. Kürschák feladat

Ismétlésként elhangzott egy piros-kék korongos feladat, mely megtalálható az algebra3-as jegyzetemben is a 7. előadás alkalmazásaként, ennek most csak itt hagyom a linkjét: [Algebra3.pdf](#)

3.4. Kisméretű csoportok (1-8)

Ebben a fejezetben azt fogjuk vizsgálni, hogy elemszámtól függően izomorfizmus erejéig hány csoport létezik.

3.4.1. Lemma. Az $A \times B$ csoport egy (a, b) elemének rendje az a és b rendjeinek legkisebb közös többszöröse. ♣

Bizonyítás. Mi lehet egy $(a, b) \in A \times B$ elem rendje? A legkisebb pozitív k egész, melyre $(a, b)^k = (a^k, b^k) = (1, 1)$, vagyis melyre $a^k = 1$ és $b^k = 1$. Ezek szerint k egy jó kitevő a -hoz és b -hez is, mivel pedig a rend osztja a jó kitevőket, így $o(a) \mid k$ és $o(b) \mid k$, vagyis k -nak éppen a rendek közös többszörösei felelnek meg. Ezek közül pedig a legkisebb, az elemrendek legkisebb közös többszöröse. ■

Speciálisan tehát ha A csoportban a legnagyobb elemrend $o(a) = n$, és B csoportban $o(b) = m$, akkor $A \times B$ maximális elemrendje $o(a, b) = [n, m]$.

Még speciálisabb esetként azt is látjuk, hogy $A = \mathbb{Z}_n$ és $B = \mathbb{Z}_m$ választással $\mathbb{Z}_n \times \mathbb{Z}_m$ csoport maximális elemrendje $[n \times m]$.

Állapítsunk meg néhány dolgot az Ábel-csoportokról. Hány darab 18 elemű Ábel-csoport van? Hát egyrészt ott van \mathbb{Z}_{18} , ami persze az Ábel-csoportok alaptétele szerint felbomlik prímszámú rendű csoportok direkt szorzatára, így $p_1^{\alpha_1} = 2$ és $p_2^{\alpha_2} = 3^2$ prímszámúakkal

$$\mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^2} = \mathbb{Z}_2 \times \mathbb{Z}_9$$

Mi történik akkor, ha \mathbb{Z}_9 -et tovább szeretném bontani, hiszen $\mathbb{Z}_3 \times \mathbb{Z}_3$ -nak is 9 eleme van. Az alaptétel szerint a felbontás a prímszámhatványok erejéig egyértelmű, így ebben az esetben $p_1^{\alpha_1} = 2$ és $p_2^{\alpha_2} = 3$ és $p_3^{\alpha_3} = 3$ prímszámhatványokkal a

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

már nem az eddigi \mathbb{Z}_{18} csoport volna. Látható ez abból is, hogy ebben a csoportban nincs 9 rendű elem, pedig \mathbb{Z}_{18} -ban van. Mivel máshogyan a 18 nem bontható prímszámhatványokra (sorrendtől és egységszeresektől eltekintve), így izomorfizmus erejéig ez a 2 darab 18 elemű Ábel-csoport van.

Mi a tapasztalatunk tehát? Hány darab n elemű Ábel-csoport létezik? Ahányféleképpen n -et prímszámhatványok szorzatára tudjuk bontani. Innen már könnyen látható, hogy például hány 8 elemű Ábel-csoport van. Mivel a 8-at csak $8 = 2^3 = 2 \cdot 2^2 = 2 \cdot 2 \cdot 2$ módon bonthatjuk prímszámhatványok szorzatára, így izomorfizmus erejéig 3 darab 8 elemű Ábel-csoport van:

$$\mathbb{Z}_8 \quad \text{és} \quad \mathbb{Z}_2 \times \mathbb{Z}_4 \quad \text{és} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Ezek valóban nem izomorf csoportok, hiszen 3.4.1. lemma alapján az elsőben 8, a másodikban 4, a harmadikban pedig 2 a maximális elemrend.

Most pedig, hogy elméletileg megfelelően előkészítettük ezt a témakört, kezdjük el vizsgálni a kis elemszámú csoportokat.