Számítástudomány alapjai
12. gyakorlat
2005. 05. 12.

1. Van-e a C_{24}-ben 4-edrendű, 5-ödrendű illetve 6-odrendű elem?
2. Adjuk meg C_{15}-ben az egyes elemek rendjét.
3. Bizonyítsuk be, hogy ha egy G csoportban minden elem rendje 2, akkor G kommutatív csoport!
4. Hány részcsoportja van a 15 rendű ciklikus csoportnak?
5. Mutassunk a D_{10} diéder csoportban $2, 4, 5$ illetve 10 rendű részcsoportot.
6. Izomorf-e C_6-tal $C_2 \otimes C_3$? És C_8-cal $C_2 \otimes C_4$?
7. Adjunk meg 3, páronként nem izomorf 20 rendű csoportot.

Csoportok

A G halmaz a $*$ művelettel csoport, ha
1. $(a * b) * c = a * (b * c)$ minden $a, b, c \in G$-re (asszociativitás)
2. van egy e, melyre $a * e = e * a = a$ minden $a \in G$-re (egységelem)
3. minden $a \in G$-hez van $a^{-1} \in G$, melyre $a * a^{-1} = a^{-1} * a = e$ (inverz)

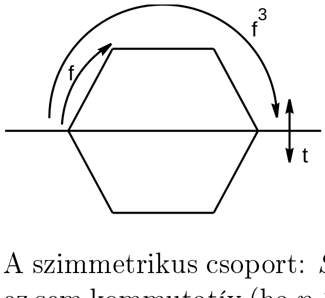
Kommutatív csoport, ha az előbbiek mellett
4. $a * b = b * a$ minden $a, b \in G$-re (kommutativitás)

Példák végtelen csoportokra:

- Az egész/racionális/valós számok az összeadással
- a pozitív racionális/valós számok a szorzással
- a nemnulla racionális/valós számok a szorzással
- a nemnulla determinánsú $n \times n$-es mátrixok a mátrixszorzással

Példák véges csoportokra:

- A ciklikus csoport: C_n, aminek n eleme van: $1, f, f^2, \dots f^{n-1}$, és két elem szorzata az f megfelelő hatványa, ahol ha a kitevő legalább n, akkor n-nel csökkentjük (ettől az egész „körbeér”, innen a neve); ez kommutatív csoport.
- A diéder csoport: D_n, aminek elemeit legegyszerűbb úgy elképzelni, mint egy szabályos n-szög forgatásait és tükrözéseit, amikor minden csúcs csúcsba megy; $2n$ eleme van: $1, f, f^2, \dots, f^{n-1}, t, ft, f^2t, \dots, f^{n-1}t$. D_n nem kommutatív, ha $n > 2$. Még valami: a szimmetrikus csoport is felfogható így geometriailag, és elemei csak a forgatások.



- A szimmetrikus csoport: S_n, ami az $1, 2, \dots, n$ halmaz permutációiból áll, elemszáma $n!$, és ez sem kommutatív (ha $n > 2$). El lehet úgy képzelni, mint az $1, \dots, n$ elemek megkeverését; két keverés szorzata az a keverés, amit úgy kapunk, hogy egymás után végrehajtjuk őket, először a szorzat *jobboldali* elemét, aztán a baloldalit (kicsit szokatlan módon).

Izomorfia. Két csoport izomorf, ha van az elemeik között olyan kölcsönösen egyértelmű megfeleltetés (bijekció), ami a műveletet megtartja.

Rend. Egy véges csoportban minden elemnek valahányadik hatványa az egységelem. A legkisebb ilyen hatványa az elem rendje. Azt is mondjuk, hogy egy csoport rendje k, ez csak annyit jelent, hogy k elemű. A Lagrange-tétel szerint minden elem rendje osztója a csoport rendjének.

Részcsoport. Egy csoport részcsoportja az elemek olyan részhalmaza, amiben benne van az egységelem, zárt a szorzásra és minden elemének az inverze is benne van. Az asszociativitás nyilván teljesül, hiszen ugyanazok az elemek vannak benne. Minden részcsoport rendje osztója a csoport rendjének. A részcsoport indexe az a csoport rendje osztva a részcsoport rendjével (azaz: „ahányadrésze" a csoportnak). Egy példa részcsoportra: D_n-nek részcsoportja C_n.

Normálosztó. A normálosztó olyan részcsoport, aminek az elemeit ha balról végigszorozzuk egy tetszőleges a elemmel, akkor ugyanazt a halmazt kapjuk, mintha jobbról szoroztuk volna végig. Kommutatív csoport esetén minden részcsoport egyúttal normálosztó is.

Direkt szorzat. Két csoport direkt szorzatán az elemeikből képzett párok halmazát értjük, ahol a művelet a tagonkénti szorzás, tehát pl. $C_2 = \{1, a\}, C_3 = \{1, b, b^2\}$ jelöléssel (figyelem, a két 1-es különböző, mindegyik a saját csoportjának egységeleme!): $C_2 \otimes C_3 = \{(1,1),(1,b),(1,b^2),(a,1),(a,b),(a,b^2)\}$, ahol pl. $(a,b) * (1,b^2) = (a,1)$. A direkt szorzat rendje $|G_1 \otimes G_2| = |G_1| \cdot |G_2|$. Ha N a G csoport normálosztója, akkor azzal le lehet „osztani", az eredmény a G/N faktorcsoport, amire $G = G/N \otimes N$.