1. Izomorf csoportok

A kételemű csoportok szerkezete.

Legyen $G = \{1, b\}$ kételemű csoport, 1 az egységelem.
Ekkor $1 * 1 = 1$ és $1 * b = b = b * 1$. Mennyi lesz $b * b$? Csak 1 vagy b lehet. Ha $b*b = b = b*1$, akkor az egyszerűsítési szabály miatt $b = 1$ lenne, ami ellentmondás. Tehát $b * b = 1$. Vagyis az összes szorzatot ismerjük!

G	1	b
1	1	b
b	b	1

$\mathbb{Z}^\times$	1	-1
1	1	-1
-1	-1	1

S_2	id	(12)
id	id	(12)
(12)	(12)	id

$\mathbb{Z}_2^+$	0	1
0	0	1
1	1	0

Ez a csoportok *teljesen EGYFORMA SZERKEZETŰEK*!
Képlettel: $\psi : 1 \mapsto id,\ -1 \mapsto (12)$ *bijektív* és *művelettartó*: $\psi(xy) = \psi(x)\psi(y)$.
Például $\psi\big((-1)(-1)\big) = id = \psi(-1)\psi(-1)$.

Példák izomorfizmusra.

4.3.1. Definíció
Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre. A $\psi : G \to H$ leképezés *csoporthomomorfizmus*, ha *művelettartó*: $\psi(a*b) = \psi(a) \bullet \psi(b)$ minden $a, b \in G$-re. Ha ψ kölcsönösen egyértelmű is a G és H halmazok között, akkor ψ *izomorfizmus*. A G és a H *izomorf csoportok*, ha van közöttük izomorfizmus, jele $G \cong H$.

4.3.3. Példa

(1) G a valós számok az összeadásra, H a pozitív valós számok a szorzásra, $\psi(g) = 10^g$.

(2) G a sík P pontja körüli forgatások a kompozícióra, H a sík Q pontja körüli forgatások a kompozícióra, $\psi(g) = fgf^{-1}$, ahol f eltolás $\overrightarrow{PQ}$-val.

Példák négyelemű csoportra.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Mely csoportok izomorfak ezek közül?

$\psi : \mathbb{Z}_4^+ \to \mathbb{Z}_5^\times$, $\psi(g) = 2^g$ (azaz $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$). Ez művelettartó: $2^{x+y} = 2^x 2^y$, így $\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$. (Pontosabban azt kell ellenőrizni, hogy $2^{x+_4 y} = 2^x *_5 2^y$).

$\mathbb{Z}_5^\times$ *és* $\mathbb{Z}_8^\times$ *nem izomorfak*, mert utóbbinál $g * g = 1$ minden g-re, a másikban pedig nem (a két táblázat főátlójában látszik).

HF: izomorfizmusnál egységelem képe egységelem.

2. Elemrend

Hatványozás csoportban (ismétlés).

2.2.19. Definíció
Legyen $*$ asszociatív művelet és n pozitív egész. Ekkor a^n jelentse az n tényezős $a*a*\ldots*a$ szorzatot. Ez az a elem n-edik *hatványa*. Ha a művelet jele $+$, akkor a^n helyett na-t írunk. Ez az a elem n-szerese (*többszörös*).

Ha a $*$ szorzásra van 1 egységelem, akkor legyen $a^0 = 1$. Ha a $+$ összeadásra van nullelem, akkor legyen $0a = 0$.

Ha a-nak van egy b inverze, akkor legyen $a^{-n} = b^n$. Ha a-nak van egy b ellentettje, akkor legyen $(-n)a = nb$.

Értelmeztük az *egész kitevőjű* hatvány (többszörös) fogalmát.

A hatványozás tulajdonságai.

2.2.20. Állítás
Legyenek a és b elemek egy G csoportban, ahol a művelet jele egymás mellé írás, és m, n egész számok. Ekkor a következők teljesülnek.

(1) a^{-n} az a^n inverze.

(2) $a^m a^n = a^{m+n}$.

(3) $(a^m)^n = a^{mn}$.

(4) Ha a és b *felcserélhetők* ($ab = ba$), akkor $(ab)^n = a^n b^n$.

Bizonyítás
Pozitív kitevőkre egyszerű leszámlálás. A többi esetben esetszétválasztás (HF).

Ismétlés.

Kiss-jegyzet, 1.5. szakasz
Egy z komplex szám *rendje* a különböző hatványainak száma. Jele: $o(z)$. Az n *jó kitevője* z-nek, ha $z^n = 1$.

(1) A z-nek vagy bármely két egész kitevőjű hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periodikusan ismétlődnek.

(2) A rend a legkisebb pozitív jó kitevő (véges rendű számra).

(3) Tetszőleges k és ℓ egészekre, $o(z) \neq \infty$ esetén $z^k = z^\ell \iff o(z) \mid k - \ell$, speciálisan $z^k = 1 \iff o(z) \mid k$. A jó kitevők tehát pontosan a rend többszörösei.

(4) A hatvány rendjének képlete: $o(z^k) = \dfrac{o(z)}{(o(z), k)}$.

(5) A $z = 1$ az egyetlen olyan szám, melynek a rendje 1.

Csoportelem rendje.

4.3.9. Definíció, 4.3.10. Gyakorlat
Egy g csoportelem *rendje* a különböző hatványainak száma. Jele: $o(g)$. Az n *jó kitevője* g-nek, ha $g^n = 1$.

(1) A g-nek vagy bármely két egész kitevőjű hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periodikusan ismétlődnek.

(2) A rend a legkisebb pozitív jó kitevő (véges rendű elemre).

(3) Tetszőleges k és ℓ egészekre, $o(g) \neq \infty$ esetén $g^k = g^\ell \iff o(g) \mid k - \ell$, speciálisan $g^k = 1 \iff o(g) \mid k$. A jó kitevők tehát pontosan a rend többszörösei.

(4) A hatvány rendjének képlete: $o(g^k) = \dfrac{o(g)}{(o(g), k)}$.

(5) A $g = 1$ az egyetlen olyan elem, melynek a rendje 1.

Példák elemrendre.

(1) $G = \mathbb{Z}_5^\times$. Ekkor $o(2) = 4$, mert $2^1 = 2 \neq 1$, $\quad 2^2 = 4 \neq 1$,
$2^3 = 4 \cdot 2 = 3 \neq 1$, $\quad$ de $2^4 = 3 \cdot 2 = 1$.

(2) $G = \mathbb{Z}_8^\times$. Az 1-től különböző elemek rendje 2, mert $3^2 = 5^2 = 7^2 = 1$.

(3) $G = \mathbb{Z}_6^+$. Ekkor $o(4) = 3$, mert $2 \cdot 4 = 8 \neq 0$, de $3 \cdot 4 = 0$. Általában $\mathbb{Z}_n^+$-ban $o(k) = n/(n, k)$ (alkalmazzuk a hatvány rendjének képletét a $g = 1$ elemre).

(4) Tükrözés rendje 2, eltolás rendje ∞ (kivéve az identitást).
$k360°$-os forgatás rendje akkor véges, ha k racionális. Ha $k = p/q$ egyszerűsíthetetlen tört, akkor a rend q.

HF (4.3.16): Ha $\psi : G \to H$ izomorfizmus, akkor *megőrzi az elemrendet*, azaz minden $g \in G$-re g és $\psi(g)$ rendje ugyanaz. Ezért $\mathbb{Z}_5^\times$ nem izomorf $\mathbb{Z}_8^\times$-cal, mert $\mathbb{Z}_5^\times$-ben csak egy másodrendű elem van, $\mathbb{Z}_8^\times$-ban pedig három.

Permutáció rendjének leolvasása.

4.3.12. Állítás
Az $f = (x_1, \ldots, x_k)$ *ciklus rendje* k, vagyis *a hossza*. Permutáció rendje a diszjunkt ciklushosszak legkisebb közös többszöröse.

Példa: $(23)(15)(45)(42)(13) = (12)(354)$ rendje $[2, 3] = 6$. *FONTOS*: a ciklusok diszjunktak kell, hogy legyenek!

Bizonyítás
Ha $\ell < k$, akkor f^ℓ az x_1-et $x_{\ell+1} \neq x_1$-be viszi, így $f^\ell \neq id$. De $f^k = id$, mert a ciklus minden eleme egyszer „körbemegy”. Legyen $g = g_1 \ldots g_m$, ahol $g_1, \ldots, g_m$ diszjunkt ciklusok. Ekkor $g^\ell = id \iff g_j^\ell = id$ minden j-re, mert ezek a ciklusok diszjunkt halmazokat mozgatnak. De $g_j^\ell = id \iff g_j$ rendje (vagyis a hossza) osztója ℓ-nek. Tehát g jó kitevői a g_j ciklusok hosszainak közös többszörösei.

Ciklikus csoportok.

4.3.17. Definíció
A G csoport *ciklikus*, ha egy eleme hatványaiból áll.
Az ilyen elem neve G egy *generátora*.

$\mathbb{Z}_5^\times$ ciklikus, generátorai 2 és 3, vagyis a negyedrendű elemek.
$\mathbb{Z}_8^\times$ nem ciklikus, mert minden eleme legfeljebb másodrendű.
$\mathbb{Z}^+$ ciklikus, az 1 és a -1 generálja (egész többszörösök!).
$\mathbb{Z}_n^+$ ciklikus, például az 1 generálja.

4.3.20. Tétel
G ciklikus $\iff$ $G \cong \mathbb{Z}^+$ vagy $G \cong \mathbb{Z}_n^+$.

Valóban: ha G ciklikus és g generálja, akkor legyen $n = o(g)$.
Ha $n < \infty$, akkor $\psi : \mathbb{Z}_n^+ \to G$, $\psi(k) = g^k$ izomorfizmus.
Ha $n = \infty$, akkor $\psi : \mathbb{Z}^+ \to G$, $\psi(k) = g^k$ izomorfizmus. □

Elemrend és generátorok ciklikus csoportban.

4.3.24. Állítás
Egy n elemű ciklikus csoportban $\varphi(n)$ generátorelem van. Minden csoportelem rendje osztója n-nek. Minden $d \mid n$-re $\varphi(d)$ darab d rendű elem van.

Bizonyítás
Ha g egy generátor, akkor $o(g) = n$, így $o(g^k) = n/(n,k) \mid n$ a hatvány rendjének képlete miatt. De g^d akkor generátor, ha rendje n, azaz ha $(n,k) = 1$. Az ilyenek száma $\varphi(n)$. A harmadik állítás következik egy későbbi tételből.

4.3.22. Tétel (nehéz)
Véges test multiplikatív csoportja ciklikus. Így $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}^+$.