1. Elemrendek, számolás $\mathbb{Z}_p$-ben

1.1. Definíció. Legyen $(G, *)$ csoport, az egységelemet jelölje e. Az $a \in G$ elem **rendjén** azt a legkisebb pozitív egész n számot értjük, melyre

$$\overbrace{a * a * \cdots * a}^{n \text{ db}} = e$$

teljesül. Ha egyetlen pozitív n-re sem teljesül ez az egyenlőség, akkor azt mondjuk, hogy a rendje végtelen. Az a elem rendjét $o(a)$ jelöli.

Konkrét csoportok esetén a műveletet általában $+$-szal vagy $\cdot$-tal jelöljük, például $(\mathbb{Z}, +)$, $(\mathbb{R}\backslash\{0\}, \cdot)$. Ha a művelet az összeadás, akkor az egységelemet 0 jelöli. Ha a művelet szorzás, akkor az egységelem 1. (Mint az előbbi két példában.)

Ha a művelet összeadás, és az egységelem 0, akkor itt az a elem rendje az a legkisebb pozitív egész n, melyre $\overbrace{a + a + \cdots + a}^{n \text{ db}} = na = 0$.

Ha a művelet a szorzás, és az egységelem az 1, akkor itt az a elem rendje az a legkisebb pozitív egész n, melyre $\overbrace{a \cdot a \cdot \cdots \cdot a}^{n \text{ db}} = a^n = 0$.

1.2. Példa. Határozzuk meg a $(\mathbb{Z}_8, +)$ csoportban a $\overline{6}$ rendjét!

Megoldás: Kezdjük el a $\overline{6}$-ot összeadni önmagával (modulo 8 számolunk!), és vizsgáljuk mikor kapunk először $\overline{0}$-át:

$\overline{6} = \overline{6}$

$\overline{6} + \overline{6} = \overline{4}$

$\overline{6} + \overline{6} + \overline{6} = \overline{2}$

$\overline{6} + \overline{6} + \overline{6} + \overline{6} = \overline{0}$

Így $o(\overline{6}) = 4$.

1.3. Példa. Határozzuk meg a $(\mathbb{Z}, +)$ csoportban a 3 rendjét!

Megoldás: Akárhány 3-ast adunk össze, sosem fogunk 0-át kapni, így itt $o(3) = \infty$.

1.4. Példa. Határozzuk meg a $(\mathbb{Z}_5\backslash\{\overline{0}\}, \cdot)$ csoportban a 4 rendjét!

Megoldás: $\overline{4} = \overline{4}$

$\overline{4} \cdot \overline{4} = \overline{1}$

Így $o(\overline{4}) = 2$.

Észrevétel: a csoportban az egységelem rendje mindig 1, és minden más elem rendje ennél nagyobb.

Az elemrendre másként is lehet gondolni: az a elem rendje ugyanis nem más, mint az a által generált részcsoport elemszáma. Vizsgáljuk ezt meg a fenti példákon:

1.5. Példa. Határozzuk meg a $(\mathbb{Z}_8, +)$ csoportban a $\overline{6}$ elem által generált részcsoportot!

Megoldás: A generált részcsoport elemei: minden, ami a $\overline{6}$-ból összeadással és kivonással megkapható. Ezek az elemek: $\overline{0}, \overline{2}, \overline{4}, \overline{6}$. (Épp ezeket kaptuk az 1.2-es példában is, mikor $\overline{6}$-osokat 4-nél kevesebbszer adtunk össze. És ez mutatja, hogy miért egyezik meg a generált részcsoport elemszáma az elem rendjével akkor, amikor az elem rendje véges: azok az elemek lesznek a részcsoportban, amiken "végig kell menni", amíg az egységelemig a rend számolásakor eljutunk.) Tehát $[\overline{6}] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$. Ennek az elemszáma valóban 4.

1.6. Példa. Határozzuk meg a $(\mathbb{Z}, +)$ csoportban a 3 által generált részcsoportot!

Megoldás: A részcsoport elemei a 3-ból összeadással, kivonással kapható számok, ezek éppen a 3-al osztható egész számok. Azaz $[3] = \{3k : k \in \mathbb{Z}\}$. Ennek elemszáma valóban végtelen.

1.7. Példa. Határozzuk meg a $(\mathbb{Z}_5\backslash\{\overline{0}\}, \cdot)$ csoportban a 4 által generált részcsoportot!

Megoldás (és egy kis számolás $\mathbb{Z}_5$-ben): A részcsoport elemei megint csak a $\overline{4}$-ből szorzással és inverzképzéssel megkapható elemek. Ennek többféleképp is neki lehet állni:

Először is, gondolhatunk arra, amit az 1.2-es példában láttunk: a részcsoport elemei azok, amiket a rend számolásakor "menet közben" megkaptunk, azaz a $\overline{4}$ és az $\overline{1}$. (Ez egy jó gondolatmenet, de csak akkor működik, ha az elem rendje véges! Azonkívül nem is írtam le pontosan, miért működik.)

Másodszor, csinálhatjuk úgy, ahogyan azt kell: meghatározzuk a $\overline{4}$ inverzét, és megnézzük, mit tudunk kihozni belőle és a $\overline{4}$-ből szorzással. Ez nem olyan egyszerű, mint az összeadás esetén.

$\overline{4}^{-1}$ **meghatározása $\mathbb{Z}_5$-ben:** meg kell találnunk azt a számot, jelölje x, amelyre igaz, hogy $\overline{4}\overline{x} = \overline{1}$. Ezt megintcsak többféleképp tehetjük meg meg.

Először is, a $\overline{4}\overline{x} = \overline{1}$ egyenlőség azzal ekvivalens, hogy $4x \equiv 1 \pmod 5$. Ez egy lineáris kongruencia, meg tudjuk oldani, a megoldás adja meg $\overline{4}^{-1}$-et.

Nem feltétlenül érdemes azonban végigszámolni a kongruenciát, hiszen $\overline{x}$-re eleve nincs túl sok jelölt: a $\mathbb{Z}_5\backslash\{\overline{0}\}$ csoport elemei: $\overline{1}, \overline{2}, \overline{3}, \overline{4}$. egyszerűen az összesre kipróbáljuk, mennyi $\overline{4}\overline{x}$, az lesz az inverz, akire a szorzat eredménye $\overline{1}$.

Sőt, az is eszünkbe juthat, amit néhány sorral följebb már leírtunk a rend számolásánál: $\overline{4} \cdot \overline{4} = \overline{1}$. Hiszen ez épp azt jelenti, hogy a keresett $\overline{x}$, melyre $\overline{4}\overline{x} = \overline{1}$, a $\overline{4}$, így $\overline{4}^{-1} = \overline{4}$. (Általában is, ha a rendje n, akkor $a^{-1} = a^{n-1}$ lesz, hiszen erre teljesül, hogy $a^{n-1} \cdot a = a^n = 1$, mivel n a rend.)

Akárhogy is, a végén erre jutunk: a $\overline{4}$-ből szorzással kapható elemek alkotják a részcsoportot, és ezek csak a $\overline{4}$, és az $\overline{1}$. Tehát $[\overline{4}] = \{\overline{4}, \overline{1}\}$.

És még néhány állítás a végére:

1.8. Tétel. *Véges csoport esetén a részcsoport elemszáma osztja a csoport elemszámát.*

Nézzük meg, hogy ez a példákban is teljesül. Ennek a tételnek egyszerű következménye:

1.9. Tétel. *Véges csoport esetén az elem rendje osztja a csoport elemszámát.*

Hiszen a rend épp a generált részcsoport elemszáma.