Ismerkedés az Abel-csoportokkal

- Szakdolgozat -

Készítette: **Takács Mária**
(Matematika BSc, Tanári szakirány)

Témavezető: **Kiss Emil**
(Algebra és Számelmélet Tanszék, Matematikai Intézet)

Eötvös Loránd Tudományegyetem
Természettudományi Kar
Budapest, 2015

Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Dr. Kiss Emilnek, észrevételeiért, ötleteiért. Az útmutatásaival a választott témámat mélyebben megismerhettem. Hálás vagyok türelméért, a LaTeX használatában nyújtott segítségéért, amely hozzájárult ahhoz, hogy megszülethessen szakdolgozatom.

Tartalomjegyzék

1. Előszó

Az egyetemi algebra előadások során bepillantást nyerhettünk a csoportelméletbe. Az előadások felkeltették az érdeklődésemet, ezért is választottam olyan témát, amely a széleskörűen alkalmazható csoportelmélettel foglalkozik. A csoportelmélet kialakulásában jelentős szerepe volt Niels Henrik Abel norvég matematikusnak, aki kimagasló eredményeket ért el sorok, az algebrai egyenletek, valamint az elliptikus és hiperbolikus függvények elmélete terén. Róla nevezték el a legrangosabb matematikai kitüntetést, sőt ő a névadója az olyan csoportoknak is, ahol a csoportművelet kommutatív. Szakdolgozatomban az Abel-csoportok tulajdonságait vizsgálom.

Dolgozatom második fejezetében ismertetem az Abel-csoportokat és a hozzá kapcsolódó legfontosabb fogalmakat. A következő fejezetben példákat mutatok direkt felbonthatatlan csoportokra. A negyedik fejezetben a csoportelmélet egyik legfontosabb tételét ismertetem és bizonyítom. Végül az utolsó fejezetben bemutatom példák segítségével az osztható csoportokat.

2. Az Abel-csoportok és a direkt szorzat

2.1. Kommutatív csoportok

Az Abel-csoportokkal való megismerkedés első lépéseként definiáljuk az Abel-csoport fogalmát. A meghatározást a csoport definíciójából kiindulva kapjuk meg úgy, hogy hozzáadunk még egy feltételt.

2.1. Definíció. Legyen G nem üres halmaz Abel-csoport, ha értelmezett rajta egy $+$ művelet a következő tulajdonságokkal:

1. Az $+$ művelet asszociatív.
2. Az $+$ művelet kommutatív.
3. Létezik olyan $e \in G$ elem, hogy minden $g \in G$ elemre $e + g = g$. A halmaznak van neutrális eleme.
4. Minden $g \in G$ elemhez létezik olyan $-g \in G$ elem , hogy $g + (-g) = e$. Minden elemnek van inverze.

Az e neutrális elemet 0-val fogjuk jelölni. Mivel a műveletet összeadásnak írjuk általában, ezért az inverzet is ellentettnek fogjuk nevezni.

Az Abel-csoportokat kommutatív csoportnak is szokták nevezni, mert ha elhagyjuk a definícióban szereplő 2. feltételt, a művelet kommutativitását, akkor a csoport definícióját kapjuk.

A komplex számok műveleti tulajdonságaiból következnek az alábbi állítások.

2.2. Állítás. *A komplex számok additív csoportja Abel-csoport.*

2.3. Állítás. *A komplex számok multiplikatív csoportja, azaz a nem nulla komplex számok csoportja a szorzásra Abel-csoport.*

A komplex számok additív csoportjának részcsoportjai a valós számok-, a racionális számok-, az egész számok additív csoportja. A komplex számok multiplikatív csoportjának részcsoportjai a valós számok-, a racionális számok multiplikatív csoportja. Mivel ezek részcsoportok, ezért öröklődnek a $\mathbb{C}^+$, illetve $\mathbb{C}^\times$ csoportbeli műveletek, és zárt csoportok ezekre a műveletekre.

2.4. Állítás. *([1], 2.2.14. Állítás) Az $\mathbb{R}^+$, $\mathbb{R}^\times$, $\mathbb{Q}^+$, $\mathbb{Q}^\times$, $\mathbb{Z}^+$ kommutatív csoportok.*

2.5. Állítás. *Az $\{0, 1, 2, \ldots, m-1\}$ halmaz kommutatív csoport a modulo m összeadásra: $\mathbb{Z}_m^+$*

Bizonyítás. A modulo m összeadás asszociatív és kommutatív. Az 1 inverze az $m-1$, a 2 inverze az $m-2$, és így tovább. Ha az m páros szám akkor az $\frac{m}{2}$ inverze az $\frac{m}{2}$ elem. Ha az m páratlan szám, akkor az $\frac{m-1}{2}$ inverze az $\frac{m-1}{2}+1$ elem. □

2.6. Példa. Tekintsük egy 4 rendű csoportot: $\mathbb{Z}_4^+ = \{0, 1, 2, 3\}$! A modulo m összeadás asszociatív és kommutatív. A $\mathbb{Z}_4^+$ neutrális eleme a 0. Az 1 inverze a 3 és a 2 inverze önmaga.

2.2. Direkt szorzat és direkt összeg

Az Abel-csoportok felbonthatósága az elkövetkezendő fejezetekben fontos szerepet kap. Ez okból elengedhetetlen, hogy ismertessük a direkt szorzat és a direkt összeg fogalmát, és így eljussunk az Abel-csoportok felbonthatóságáig. Ezeket a fogalmakat a [1] alapján építjük fel.

2.7. Definíció. Legyen A és B két csoport. Azt a csoportot, amelynek elemei (a, b) alakú párok, ahol az $a \in A$ és $b \in B$ az A és B csoportok direkt szorzatának nevezzük. A műveletet komponensenként végezzük el:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

Az első komponenst úgy kapjuk, hogy A csoportbeli műveltet végzünk, a második komponenst pedig úgy, hogy B csoportbeli műveletet végzünk. Jelölése: $A \times B$.

Vizsgáljuk meg az $A \times B$ csoportot. Tekintsük $A \times B$-ben az A^* részcsoportot, amelynek elemei olyan $(a, 0)$ párok, ahol a $a \in A$ és a $0 \in B$ a B csoport egységeleme. Az $A^* \leftrightarrow A : (a, 0) \leftrightarrow a$ megfeleltetés bijektív és művelettartó. Hasonlóan B^* csoport az $A \times B$ azon részcsoportja, amelynek elemei olyan $(0, b)$ párok, ahol a $b \in B$ és a 0 az A csoport egységeleme és a $B^* \leftrightarrow B : (0, b) \leftrightarrow b$ megfeleltetés bijektív és művelettartó. Az $A^* \cap B^* = (0, 0)$ az $A \times B$ csoport egységeleme.

2.8. Állítás. *([1], 4.9.11 Állítás). Minden $c \in A \times B$ csoportelemhez létezik $a^* \in A^*$ és $b^* \in B^*$ úgy, hogy $a^* + b^* = c$, azaz*

$$A^* + B^* = A \times B.$$

Bizonyítás. Legyen $c = (a, b)$. A c két csoportelem összege, ahol az első tényező A^* csoportbeli, míg a második tényező B^* csoportbeli elem:

$$(a, b) = (a, 0) + (0, b)$$

□

2.9. Tétel. *([1], 4.9.12 Tétel). Legyen G csoport, és tegyük fel, hogy G-ben van 2 részcsoport úgy, hogy $A \cap B = \{0\}$ és $A + B = G$. Ekkor $G \cong A \times B$.*

Bizonyítás. A tételben megfogalmazott A-ra és B-re vonatkozó feltételek pontosan azok a feltételek, amelyek a korábban definiált A^*-ra és B^*-re vonatkoztak.
Ha A és B ilyen részcsoportok, akkor G minden eleme egyértelműen áll elő $a + b$ alakban, ahol $a \in A$ és $b \in B$. Mert ha $a + b = a^* + b^*$, ahol $a^* \in A$ és $b^* \in B$, akkor $a - a^* = b^* - b$ az $A \cap B$-ben van, ezért nulla, tehát $a = a^*$ és $b = b^*$. Feleltessük meg az $a + b$ elemet az (a, b) párnak. Ez a leképezés kölcsönösen egyértelmű és művelettartó G és $A \times B$ között. □

A direkt szorzat fogalmát kiterjeszthetjük véges és végtelen sok csoportra is. Most véges sok csoport direkt szorzatát fogjuk definiálni.

2.10. Definíció. Legyen $A_1, A_2, \ldots, A_n$ véges sok csoport. Az $A_1, A_2, \ldots, A_n$ csoportok direkt szorzatán az olyan $(a_1, a_2, \ldots, a_n)$ alakú n komponensű sorozatokat értjük, amelyeknél az $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$. Az i. komponensben A_i csoportbeli műveletet végzünk. Jelölése: $A_1 \times A_2 \times \cdots \times A_n$.

A definíciót megelőző tétel és állítás öröklődik véges sok csoport direkt szorzatára. Nézzünk meg, hogyan öröklődik a 2 tényezőre vonatkozó tétel!

2.11. Állítás. *Ha az A_i-k részcsoportok az A csoportban úgy, hogy teljesülnek rá a következő feltételek:*

1. *Az A csoport minden eleme előáll véges sok A_i-beli elem összegeként.*

2. Minden A_i-t elmetszve véges sok másik A_j összegével, csak a 0-t kapjuk.

akkor $A \cong A_1 \times A_2 \times \dots A_n$.

Az Abel-csoportok esetében a direkt szorzatot direkt összegnek is nevezzük, mivel a műveletet nem csak asszociatív, hanem kommutatív is, és a kommutatív művelet jele: $+$. A direkt összeg jele: $\oplus$. A megfeleltetés: $a_1 + \dots + a_n \leftrightarrow (a_1, \dots, a_n)$.

2.12. Állítás. *Az Abel-csoportok esetében:* $A \oplus B \cong A \times B$*, ahol a* A *és* B *az Abel-csoport részcsoportjai a 2.11-beli feltételekkel.*

A direkt összeg kiterjeszthető végtelen sok csoportra.

2.13. Definíció. A 2.10. Definíció mintájára végtelen sok A_i Abel-csoport direkt szorzatát is definiálhatjuk, ennek jele $\prod_i A_i$. Jelölje A ennek azt a részcsoportját, amelyben mindegyik elem komponensei véges sok kivétellel nullával egyenlőek. Ezt az A_i csoportok direkt összegének nevezzük, jele $\sum_i A_i$. A 2.11 Állításban megadott jellemzés végtelen sok Abel-csoport direkt összegére is érvényes.

2.3. Példák véges Abel-csoportok direkt felbontásaira

A fejezet elkövetkezendő részében véges Abel-csoportok direkt összegre való felbontásaira láthatunk példákat.

2.14. Példa. Vegyük azt a négyelemű csoportot, amelyben az egységelemen kívül minden elem rendje 2, és egy nem egységeleme megkapható a másik két elem szorzataként. A Klein csoport szorzótáblája ezek szerint:

$\cdot$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

A Klein-csoport nem triviális részcsoportjai: $X = \{e, x\}$, $Y = \{e, y\}$, $Z = \{e, z\}$. A felbontások: $X \oplus Y$, $X \oplus Z$, $Y \oplus Z$. A $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$ a Klein-csoporttal izomorf .

2.15. Példa. Adott a hatelemű ciklikus csoport: $\mathbb{Z}_2^+ = \{0, 1, 2, 3, 4, 5\}$. Ennek nem triviális részcsoportjai: $G = \{0, 3\}$ és $H = \{0, 2, 4\}$. A hatelemű ciklikus csoportnak egy felbontása van, a két nem triviális részcsoportjának direkt összege: $\mathbb{Z}_6^+ = G \oplus H$.

2.16. Példa. Nézzük a százrendű ciklikus csoportot! $\mathbb{Z}_{100}^+ = \{0, 1, 2, \ldots, 97, 98, 99\}$. A $\mathbb{Z}_{100}^+$ nem triviális részcsoportjai:

- A=$\{$0,50$\}$
- B=$\{$0,25,50,75$\}$
- C=$\{$0,20,40,60,80$\}$
- D=$\{$0,10,20,30,40,50,60,70,80,90$\}$
- E=$\{$0,5,10,15, $\ldots$,90,95$\}$
- F=$\{$0,4,8,12, $\ldots$,88,92,96$\}$
- G=$\{$0,2,4, $\ldots$,94,96,98$\}$.

A százrendű ciklikus csoport egyik felbontása: $B \oplus F$.

Az utolsó példa előtt még szükséges ismertetnünk egy tételt.

2.17. Tétel. *Véges test multiplikatív csoportja ciklikus.*

2.18. Példa. Vizsgáljuk meg a 16 elemű test multiplikatív csoportját! Ez a csoport izomorf a $\mathbb{Z}_{15}^+$ ciklikus csoporttal $\mathbb{F}_{16}^\times \cong \mathbb{Z}_{15}^+$. Ezért nem triviális részcsoportjai a következők: $A = \{0, 5, 10\}, B = \{0, 3, 6, 9, 12\}$. Az $\mathbb{F}_{16}^\times$ felbontása: $A \oplus B$.

3. Példák direkt felbonthatatlan csoportokra

Az előző fejezet végén direkt összegre való felbontásokra mutattunk példákat. De nem minden csoport felbontható csoport. Itt az ideje, hogy megismerjünk néhány direkt felbonthatatlan csoportot.

3.1. Az egész és racionális számok additív csoportja

3.1. Állítás. *Az egész számok additív csoportja direkt felbonthatatlan csoport.*

Bizonyítás. Az egész számok additív csoportjának részcsoportjai az egyelemű részcsoporton és az egész halmazon kívül a 2-vel, 3-mal, 4-gyel, stb. osztható egész számok. Ezek közül a részhalmazok közül nem tudunk kiválasztani kettőt úgy, hogy azok metszete csak a 0 legyen. Ugyanis ha például kiválasztjuk a p-vel, illetve a q-val osztható egész számok csoportját, ahol $p \neq 0$ és $q \neq 0$, akkor mindkettő csoportban megtalálható a pq egész szám és azok többszörösei. □

3.2. Állítás. *A racionális számok additív csoportja direkt felbonthatatlan csoport.*

Bizonyítás. Vegyük a csoportjának nem triviális részhalmazait. Ezek közül kiválasztunk két tetszőleges csoportot. Ha $\frac{p}{q}$ benne van az egyik részcsoportban és $\frac{r}{s}$ a másik részcsoportban, ahol $\frac{p}{q} \neq 0$ és $\frac{r}{s} \neq 0$, akkor metszetükben benne lesz a nullán kívül a

$$\frac{p}{q} \cdot q \cdot r = \frac{r}{s} \cdot s \cdot p = p \cdot r$$

racionális szám és többszörösei. □

3.2. Torziócsoport

A fejezetben még két példát mutatunk direkt felbonthatatlan csoportokra. E példák előtt elengedhetetlen két fogalom bevezetése.

3.3. Definíció. Egy csoportot torziócsoportnak nevezünk, ha minden eleme véges rendű.

Az elemrend definíciójából következik, hogy minden véges csoport torziócsoport.

Vizsgáljuk meg egy adott b elem által generált véges csoport elemeinek rendjét! A b elem rendje: n, azaz $o(b) = n$. A csoport: $\{0, b, 2b, 3, \ldots, (n-1)b\}$. Ez a csoport ciklikus csoport, amely izomorf $\mathbb{Z}_n^+$-el. Lagrange-tételének következménye, hogy egy véges csoport tetszőleges elemének rendje a csoport rendjének osztója, azaz minden kb-re $o(kb)$ osztója lesz n-nek. Ez a rend a hatvány rendjének képletéből kiszámolható:

$$o(kb) = \frac{n}{(n,k)}.$$

Nem csak véges, hanem végtelen rendű torziócsoportok is léteznek.

3.4. Definíció. Legyen p prím. A p-hatványadik komplex egységgyökök multiplikatív csoportját p-Prüfer-csoportnak nevezzük. Ezt a csoportot $\mathbb{Z}_{p^\infty}$-nel jelöljük.

Véges rendű elemek esetén ahhoz, hogy ellenőrizzük, hogy egy részhalmaz részcsoport-e, elég ellenőrizni, hogy zárt-e az összeadásra. Ugyanis, ha b rendje n, akkor $-b$ megkapható úgy, hogy $(n-1)b$. Emiatt a Prüfer-csoportban elég ellenőrizni, hogy 2-hatvány rendű elemek szorzata is 2-hatvány rendű, és ezért az inverzzel már nem kell foglalkozni.
A 2-hatványadik egységgyökök szorzata is 2-hatványadik egységgyök:

$$u_1 = \cos(\frac{2\pi \cdot m}{2^k}) + i \cdot \sin(\frac{2\pi \cdot m}{2^k})$$
$$u_2 = \cos(\frac{2\pi \cdot n}{2^l}) + i \cdot \sin(\frac{2\pi \cdot n}{2^l})$$

$$u_1 \cdot u_2 = \cos(\frac{2\pi \cdot m \cdot 2^l + 2\pi \cdot n \cdot 2^k}{2^k \cdot 2^l}) + i \cdot \sin(\frac{2\pi \cdot m \cdot 2^l + 2\pi \cdot n \cdot 2^k}{2^k \cdot 2^l})$$

$$u_1 \cdot u_2 = \cos(\frac{2\pi(m \cdot 2^l + n \cdot 2^k)}{2^{k+l}}) + i \cdot \sin(\frac{2\pi(m \cdot 2^l + n \cdot 2^k)}{2^{k+l}})$$

Azaz ha u_1 egy 2^k. egységgyök, az u_2 egy 2^l. egységgyök, ezek szorzata, az $u_1 \cdot u_2$ egy 2^{k+l}. egységgyök. Azaz szorzatuk mindig 2-hatványadik egységgyök marad. Ha $z^{2^n} = 1$, akkor z rendje osztója a 2^n-nek, vagyis z rendje 2-hatvány.

3.5. Állítás. *A p-Prüfer-csoportok nem triviális részcsoportjai p^k-adik komplex egységgyökök, ahol k befutja az összes pozitív egész számot.*

Az állítást a $p = 2$ esetre bizonyítjuk. Tekintsük azt a G csoportot, amely azon komplex számokból áll, amelyek rendje 2-hatvány.

Bizonyítás. A Prüfer-csoport részcsoportjai: a 2.-, a 4.-, a 8. egységgyökök, és így tovább, azaz a 2-hatványadik egységgyökök.
2. egységgyökök $\subseteq$ 4. egységgyökök $\subseteq$ 8. egységgyökök, stb.
Nincs más részcsoport a 2-hatványadik egységgyökökön kívül a G-ben.
Vegyünk egy H részcsoportot. 2 esetet vizsgálunk:

1. A H részcsoportban a legnagyobb elemrend: 2^n.

   $$z^{2^n} = 1.$$

   Ha a legnagyobb elemrend 1 lenne, azaz $n = 0$, akkor $z^1 = 1 \to z = 1$.
   Ha $n = 1$, akkor $z^2 = 1 \to z = \pm 1$. $\to$ 2 db elem
   Ha $n = 2$, akkor $z^4 = 1 \to z = \pm 1, \pm i$. $\to$ 4 db elem
   Ha $n = 3$, akkor $z^8 = 1 \to z = \pm 1, \pm i, \pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}$. $\to$ 8 db elem, stb.
   Ugyanis, ha egy részcsoportban van egy olyan a elem, amely 2^k rendű, akkor benne van az a által generált csoport, az $\langle a \rangle = \{1, a, a^2, a^3, \ldots, a^{2^{k-1}}\}$.
   Az a^s rendje:

   $$o(a^s) = \frac{o(a)}{(o(a), s)} = \frac{2^k}{(2^k, s)}$$

   Az s-re teljesül, hogy $1 \leq s \leq 2^{k-1}$. Amikor az s és a 2^k relatív prímek, akkor egy újabb 2^k rendű elemet kapunk, és így megkapjuk az összes 2^k rendű elemet. Mivel az a rendje 2^k, így 2^k darab különböző hatványa van és ezek mindegyike 2^k. egységgyök. Összesen 2^k darab 2^k. egységgyök van, így megkaptuk az összes 2^k-adik egységgyököt. Tudjuk, hogy n adott, ekkor $z^{2^n} = 1$. Vagyis ennek a részcsoportnak 2^n db eleme van, ebből 2^{n-1} db rendje 2^n, a többi elem rendje $1, 2, 4, \ldots, 2^{n-1}$. Ez egy véges csoport, amely a 2^n-edik egységgyökökből áll.

2. A H részcsoportban akármilyen nagy rendű elemek vannak.
   Az 1. eset alapján tudjuk, hogy ha H-ban van 2^k rendű elem, akkor H-ban benne van az összes 2^k-adik egységgyök, és ezek között ott vannak, azok a 2^m-edik egységgyökök, amelyeknél $m \leq k$. De k is akármilyen nagy lehet, ezért ez a H részcsoport tartalmaz minden 2-hatványadik egységgyököt, és ezért H az egész csoporttal egyezik meg.

□

A 2-Prüfer-csoport egy olyan csoport, amely végtelen csoport, de minden valódi részcsoportja véges csoport.

3.6. Definíció. Torziómentes csoport: Egy csoportot torziómentes nevezünk, ha az egységelemen kívüli összes elemének rendje végtelen.

3.7. Példa. Komplex számok az összeadásra nézve.
Legyen az $a + bi$ komplex szám rendje: n. Ekkor:

$$n(a + bi) = 0$$
$$na + nbi = 0 + 0i$$

Azaz $na = 0$ és $nb = 0$. De az n nem lehet 0, mert az a $a + bi$ komplex szám rendje, de ekkor az a-nak és a b-nek kell 0-nak lenni, így az egységet kaptuk. Vagyis a komplex számok additív csoportjában az egységen kívül minden elem rendje végtelen.

3.8. Definíció. Egy véges csoportot p-csoportnak nevezünk, ha a csoport rendje p hatványa, ahol p prím. Minden p-re p-csoportnak tekintjük az egyelemű csoportot.

A p-csoport fogalmát kiterjeszthetjük végtelen csoportokra is.

3.9. Definíció. Legyen p prím. Egy végtelen csoportot p-csoportnak nevezünk, ha minden elemének rendje a p-hatványa.

A végtelen torziócsoportra mutatott utóbbi példában is egy p-csoporttal találkoztunk, amely a Prüfer-csoport volt.

Lagrange-tételéből következik, hogy egy p-hatvány rendű csoport minden eleme p-hatvány rendű.

Miután definiáltuk a szükséges fogalmakat, itt az ideje, hogy mutassunk egy újabb direkt felbonthatatlan torziócsoportot.

3.10. Állítás. *A p-Prüfer csoport direkt felbonthatatlan csoport.*

Bizonyítás. A 3.5. Állításban leírtuk a 2-Prüfer-csoport részcsoportjait:
2. egységgyökök $\subseteq$ 4. egységgyökök $\subseteq$ 8. egységgyökök, stb.

Ugyanígy igaz minden p-re, hogy a p-Prüfer-csoport részhalmazai:
p. egységgyökök $\subseteq p^2$. egységgyökök $\subseteq p^3$. egységgyökök, stb.
A nem triviális részcsoportok közül egyik sem egyelemű, és bármely két részcsoport közül az egyik tartalmazza a másikat, ezért nem tudunk kiválasztani két részcsoportot úgy, hogy azok metszete csak a $\{0\}$ legyen. □

3.11. Állítás. *A prímhatvány rendű ciklikus csoportok direkt felbonthatatlanok.*

Bizonyítás. Legyen A a p^k-adik egységgyökök csoportja a szorzásra. Ez ciklikus, mert p^k-adik primitív egységgyök generálja. Ezért elég megmutatni, hogy ez direkt felbonthatatlan.
Ha H részcsoportja A-nak, akkor legyen n a legnagyobb egész, amelyre H-ban van p^n rendű elem. Ekkor az n által generált részcsoport az összes p^n-edik egységgyökökből áll. Láttuk, hogy mely részcsoportok a Prüfer-csoportok részcsoportja. Ezek alapján felírhatjuk a prímhatvány rendű ciklikus csoport részcsoportjait. A nem triviális részcsoportok közül egyik sem egyelemű, és nincs két olyan, amik csak a nullában metszik egymást. □

3.12. Példa. A 2.14. Példában mutattunk egy olyan 4 elemű csoportot, amely direkt felbontható. De vannak olyan 4 elemű csoport is, amelyek nem izomorfak a $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$ direkt szorzattal. Ezek a $\mathbb{Z}_4^+$ csoporttal, másképpen felírva: a $\mathbb{Z}_{2^2}^+$ csoporttal izomorfak.

4. A véges Abel-csoportok alaptétele

Az Abel-csoportokkal való megismerkedés során a legfontosabb tétel a véges Abel-csoportok alaptétele. Az alaptétel bizonyítása számos lépésből áll. A bizonyítás első lépésében a komponensekre bontást végtelen csoportokra is bizonyítani fogjuk.

4.1. Tétel. *([1], 4.9.15). [Véges Abel-csoportok alaptétele]: Minden véges Abel-csoport egyértelműen felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. Képlettel:*

$$A \cong \mathbb{Z}^+_{p_1^{\alpha_1}} \times \mathbb{Z}^+_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}^+_{p_m^{\alpha_m}},$$

ahol A jelöli a véges Abel-csoportot és minden i-re p_i prím, ahol $1 \leq i \leq m$.

4.1. Torziócsoport felbontása p-komponensekre

Az alaposabb megértéshez nézzük először a torziócsoportok felbontását. A következőkben [2] 8.4 Tételt és bizonyítását ismertetem.

4.2. Állítás. *Minden torziócsoport felbontható p-csoportok direkt összegére.*

De mégis hogyan? A következő állításban választ kaphatunk erre a kérdésre.

4.3. Állítás. *Egy A torziócsoport olyan A_p p-csoportok direkt összege, ahol a p befutja az összes prímet. Az A az A_p-ket egyértelműen meghatározza.*

Bizonyítás. Az A_p p-csoport olyan A csoportbeli elemekből áll, amelyek rendje p prím hatványa. Az A egységeleme, amelyet most 0-val jelölök, az A_p-nek is eleme, így A_p nem üres. Ha a és b két A csoportbeli elem, azaz ha

$$p^m a = p^n b = 0$$

az m és n pozitív egész számokra, akkor $p^{max(m,n)}(a-b) = 0$, tehát A_p csoportbeli elem $a-b$ is, és így A_p egy részcsoport. Ha a rendje $p_1^{r_1}$, b rendje $p_2^{r_2}$, c rendje $p_3^{r_3}$, akkor $a = b + c$ egyenletből következik, hogy $a = 0$. Ugyanis, ha

az egyenletet megszorozzuk a következő számmal: $p_2^{r_2}p_3^{r_3}$, akkor a jobboldalon 0-t kapunk, mivel

$$bp_2^{r_2}p_3^{r_3} = (bp_2^{r_2})p_3^{r_3} = 0p_3^{r_3} = 0 \qquad p_2^{r_2}p_3^{r_3}c = p_2^{r_2}(p_3^{r_3}c) = p_2^{r_2}0 = 0.$$

Mivel a jobboldalon 0 van, ezért a baloldalon is 0-nak kell lennie, azaz $p_2^{r_2}p_3^{r_3}a = 0$. Ekkor a rendje osztója $p_2^{r_2}p_3^{r_3}$-nak, de osztója $p_1^{r_1}$-nek is, ezért a rendje 1, azaz $a = 0$. Tehát

$$A_p \cap (A_{p_1} + A_{p_2} + \cdots + A_{p_k}) = 0,$$

amikor a $p \neq p_1, p_2, \ldots, p_k$-val. Ezért a A_p-k által generált összeg direkt összeg: $\oplus_p A_p$. Azért, hogy megmutassuk, hogy minden $a \in A$ elem benne van a direkt összegben, tekintsük $a \in A$ rendjét. Az $o(a) = m = p_1^{r_1} \cdot \cdots \cdot p_n^{r_n}$, ahol p_i-k különböző prímek. Az $m_i = mp_i^{-r_i}$ (ahol $i = 1, \ldots, n$)-k relatív prímek, ezért vannak $s_1, s_2, \ldots, s_k$ egészek úgy, hogy $s_1m_1 + s_2m_2 + \cdots + s_nm_n = 1$ (diofantoszi egyenlet megoldhatósága). Így

$$a = s_1m_1a + s_2m_2a + \cdots + s_nm_na,$$

ahol $m_ia \in A_{p_i}$, mert $p_i^{r_i}m_ia = ma = 0$, és így $a \in A_{p_1} + A_{p_2} + \cdots + A_{p_n} \subseteq \oplus_p A_p$.

Ha $A = \oplus_p B_p$ az A-nak egy másik direkt felbontása, ahol a B_p-k p-csoportok különböző prímekkel. A $B_p \subseteq A_p$ minden p-re. Ha $a \in A_p$, akkor a felírható $a_1 + a_2 + \cdots + a_n$ alakban, ahol $a_1 \in B_p$ és az a_i-k mindegyike valamely másik B_{p_i}-ben van. Átrendezés után azt kapjuk, hogy $a - a_1 = a_2 + a_3 + \cdots + a_n$. De előzőleg már beláttuk, hogy ez csak akkor lehetséges, ha $a - a_1$ és az $a_2 + a_3 + \cdots + a_n$ is 0. Azaz $a = a_1$, vagyis $a \in B_p$. Ezért $B_p = A_p$. $\square$

Mivel minden véges Abel-csoport torziócsoport, ezért minden véges Abel-csoport egyértelműen felbontható A_p p-csoportok direkt összegére, ahol az A_p-khez tartozó p-k különböző prímek. Felbontásnak vesszük a triviális felbontást is, amikor az egyik p-csoport az egyelemű csoport, amely egyetlen eleme a 0, a másik csoport maga a csoport.

4.4. Példa. Ha A az összes komplex egységgyökök csoportja, akkor $A_p = \mathbb{Z}_{p^\infty}$, vagyis A_p pontosan a Prüfer-csoport lesz.

4.5. Példa. Ha m pozitív egész kanonikus alakja $p_1^{r_1}p_2^{r_2} \cdot \cdots \cdot p_n^{r_n}$, akkor

$$\mathbb{Z}_m^+ = \mathbb{Z}_{p_1^{r_1}}^+ \oplus Z_{p_2^{r_2}}^+ \oplus \cdots \oplus Z_{p_n^{r_n}}^+.$$

Bizonyítás. A $\mathbb{Z}_m^+$ felbontása. A p_1-csoport elemei a p_1-hatvány rendű elemek. Így n darab részcsoportot kapunk: $A_{p_1}, A_{p_2}, \ldots, A_{p_n}$. A $\mathbb{Z}_m^+$ csoportban $p_1^{r_1}$ darab p_1-hatvány rendű elem van, ezért A_{p_1} rendje $p_1^{r_1}$. Hasonlóan járunk el a többi p-csoport esetében is. Az A_{p_1} ciklikus, és ezért izomorf $\mathbb{Z}^+_{p_1^{r_1}}$-gyel, ugyanis ha a $\mathbb{Z}_m^+$ generátoreleme a, akkor az a-t megszorozva $p_2^{r_2} \ldots p_n^{r_n}$-el $p_1^{r_1}$ rendű elemet kapunk a hatvány rendjének képlete miatt. Hasonlóan járunk a többi izomorfia bizonyítása során. Tudjuk, hogy az $A = \oplus_i A_{p_i}$, az izomorfia miatt $A = \oplus_i \mathbb{Z}^+_{p_i^{r_i}}$. Tehát $A = \mathbb{Z}^+_{p_1^{r_1}} \oplus Z^+_{p_2^{r_2}} \oplus \cdots \oplus Z^+_{p_n^{r_n}}$. $\square$

4.2. Az alaptétel bizonyítása

A véges Abel-csoportok alaptételének kimondásával nem elégszünk meg. Szükségünk van egy konstrukcióra is a felbontáshoz. A konstrukció megalkotásához [1] 4.9.34., illetve 4.9.39. feladatokat és megoldásaikat használtam fel.

4.6. Állítás. *Legyen A Abel-csoport és p prím. Tegyük föl, hogy $pa=0$ minden $a \in A$ esetén. Legyen $\lambda \in \mathbb{Z}_p$ esetén a λa szorzat, az a egész többszöröse. Ezzel a szorzással A vektortérré válik $\mathbb{Z}_p$ fölött.*

Bizonyítás. Ha a $pa = 0$ csak néhány $a \in A$ esetén áll fent, akkor nem kapunk vektorteret. Tegyük fel, hogy $pa = 0$ minden $a \in A$ esetén. Ha $\lambda \in \mathbb{Z}_p$, akkor λ egy egész, mivel a $0, 1, 2, \ldots, p-1$ valamelyike, ezért beszélhetünk a $\lambda a \in A$ elemről, mint az a egész többszöröséről. Tetszőleges $\lambda, \mu \in \mathbb{Z}_p$ és $a \in A$ esetén teljesülnek a következő vektortér-axiómák a hatványozás azonosságai miatt:

- $(\lambda + \mu)a = \lambda a + \mu a$, ugyanis $a^{(\lambda+\mu)} = a^\lambda a^\mu$
- $\lambda(a + b) = \lambda a + \lambda b$, ugyanis $(ab)^\lambda = a^\lambda b^\lambda$
- $(\lambda\mu)a = \lambda(\mu a)$, ugyanis $a^{\lambda\mu} = (a^\lambda)^\mu$
- $1a = a$, ugyanis $a^1 = a$.

A többi vektortér-axióma teljesül az Abel-csoport definíciója miatt. De vegyük észre, az előbb felsorolt axiómák nem a $\mathbb{Z}_p$ fölötti vektortér-axiómák!
A $\mathbb{Z}_p$ fölötti vektortér-axiómáknál a tetszőleges $\lambda, \mu \in \mathbb{Z}_p$ skalárok közötti összeadásnál az egész számok összeadása és szorzása helyett a modulo p összeadást és szorzást alkalmazzuk. Csak két vektortér axióma változik. Azt akarjuk

belátni, hogy $(\lambda +_p \mu)a = \lambda a + \mu a$ és $(\lambda \cdot_p \mu)a = \lambda(\mu a)$. Mivel $\lambda + \mu \equiv \lambda +_p \mu$ (modulo p) és $\lambda \cdot \mu \equiv \lambda \cdot_p \mu$ (modulo p), ezért $(\lambda + \mu) - (\lambda +_p \mu)$ és $(\lambda \cdot \mu) - (\lambda \cdot_p \mu)$ osztható p-vel. Most kell felhasználni, hogy $pa = 0$, ugyanis, ha a $(\lambda + \mu) - (\lambda +_p \mu)$ és $(\lambda \cdot \mu) - (\lambda \cdot_p \mu)$ p-vel osztható egész számokat megszorozzuk a-val, akkor 0-t kapunk. Átrendezés után azt kapjuk, hogy $(\lambda +_p \mu)a = \lambda a + \mu a$ és $(\lambda \cdot_p \mu)a = \lambda(\mu a)$. □

4.7. Megjegyzés. Ha valamelyik állításban lévő feltétel nem teljesül, akkor nem kapunk vektorteret. Nézzük meg a $A = \mathbb{Z}_4^+$ és $p = 2$ esetét! Legyen a 0-val és 1-gyel való szorzás a következő: $0a = 0$ és $1a = a$. Legyen $\lambda, \mu \in \mathbb{Z}_2$ és $a \in \mathbb{Z}_4^+$. A $(\lambda + \mu)a = \lambda a + \mu a$ vektortér-axióma nem teljesül. Ugyanis $(1 +_2 1)a = 0a = 0$. De $1a + 1a = a + a = 2a$. A $2a$ nem minden esetben 0. Ha $a = 0$ vagy $a = 2$, akkor $2a = 0$, de ha $a = 1$ vagy $a = 3$, akkor $2a = 2$, azaz a disztributivitás nem teljesül. Vagyis a $\mathbb{Z}_4^+$ nem vektortér a $\mathbb{Z}_2$ fölött.

Az olyan A Abel-csoportra, amelyekre teljesül az állításban megfogalmazott feltételek, azaz $pa = 0$ minden $a \in A$ esetén, ahol p prím, és a többszöröse is értelmes, akkor A vektortér $\mathbb{Z}_p$ fölött. Ha az A vektortér n-dimenziós, akkor A izomorf $(\mathbb{Z}_p)^n$-nel, mert ha $b_1, b_2, \ldots, b_n$ bázis, akkor a egyértelműen felírható $\lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n$ alakban. Az $a \to (\lambda_1, \lambda_2, \ldots, \lambda_n)$ megfeleltetés pedig izomorfizmus.

4.8. Állítás. *Legyen A Abel-csoport és p prímosztója A rendjének. Ha $a \in A$ maximális rendű az A csoport p-hatványrendű elemei között, akkor A felbomlik az $\langle a \rangle$ részcsoport és egy másik alkalmas részcsoport direkt szorzatára.*

Bizonyítás. Legyen M maximális az A Abel-csoport azon részcsoportjai között, melyekre $M \cap \langle a \rangle = 0$. Azt szeretnénk belátni, hogy $M + \langle a \rangle = A$.

Az A csoport a elemének rendje p^n, és az A csoportban nincs ennél nagyobb p-hatványrendű elem. Ahhoz, hogy belássuk, hogy $M + \langle a \rangle = A$, először külön vizsgáljuk meg az $M + \langle a \rangle$-t. Legyen $K = M + \langle a \rangle$. Az $\langle a \rangle$ részcsoport elemei : $\{0, a, 2a, \ldots, (p^n - 1)a\}$, tehát ua alakúak, ahol u-ra teljesül, hogy $1 \leq u \leq p^n - 1$. A K részcsoport elemei $ua + b$ alakúak, ahol u egész és $b \in M$.

Legyen $g \in A$ és m olyan egész, amelyre $mg \in M$. Ha olyan A csoportbeli g-t választunk, amely nincs benne az M-ben, akkor az m legyen a g jó kitevője, hiszen ha a g-t a jó kitevőjével megszorozzuk, akkor 0-t kapunk, és persze $0 \in M$. Tehát ilyen m mindig van, de az is lehetséges, hogy a jó kitevő valamely

osztója is jó választás az m-re. Legyen $m = tp^e$, ahol t már nem osztható p-vel, azaz a t relatív prím p-hez. Belátjuk, hogy $p^e g \in M$. Legyen $h = p^e g$. Ekkor $th \in M$, mivel $th = tp^e g = mg$ és mg-ről már tudjuk, hogy M csoportbeli.

Indirekt tegyük fel, hogy $h = p^e g$ nem M csoportbeli. Tekintsük az M és h által generált részcsoportot. A h által generált részcsoport elemei kh alakúak, ahol k egész. Így az M és h által generált részcsoport elemei $kh+b$ alakúak, ahol k egész és $b \in M$. Mivel az M-et maximálisnak választottuk, ezért az M és h által generált részcsoport már nem csak a 0-ban metszi $\langle a \rangle$-t. Tehát van olyan u egész, ahol $kh + b = ua$ és $ua \neq 0$. Innen $tkh + tb = tua$. De $tua \in M$, ugyanis $tua = tkp^e g + tb$ és $tp^e g \in M$ és $b \in M$, így a többszöröseik összege is M csoportbeli. De M csak a 0-ban metszi $\langle a \rangle$-t, így $tua = 0$. Ezért a rendje, azaz p^n, osztója tu-nak. De t és p relatív prímek, ezért p^n osztója u-nak is, azaz $ua = 0$, ami ellentmondás. Tehát $p^e g \in M$.

Indirekt tegyük fel, hogy $\langle a \rangle + M \neq A$, azaz van olyan $g \in A$, ami nincs benne K-ban. Legyen g rendje tp^e, ahol t már nem osztható p-vel. Ekkor tg rendje p^e, ugyanis

$$o(tg) = \frac{o(g)}{(o(g), t)} = \frac{tp^e}{(tp^e, t)} = \frac{tp^e}{t} = p^e$$

Ezért $e \leq n$, ugyanis a maximális p-hatványrendű elem. Az imént beláttuk, hogy $p^e g \in M$. Ha pg nincs K-ban, akkor g-ről áttérhetünk pg-re, és ekkor a rendben a kitevő 1-gyel csökken, mivel hogy

$$o(pg) = \frac{o(g)}{(o(g), p)} = \frac{tp^e}{(tp^e, p)} = \frac{tp^e}{p} = tp^{e-1}$$

Ezt az eljárás folytatva végül egy olyan g elemet kapunk, amelyre $pg \in K$. Ennek az új g-nek a rendjét jelölje újra tp^e, és tudjuk, hogy $e \leq n$. Tehát $pg = ka + b$, ahol k egész és b pedig egy M csoportbeli elem. Ezt az egyenletet szorozzuk meg tp^{e-1}-gyel.

$$tp^{e-1}pg = tp^{e-1}ka + tp^{e-1}b$$
$$tp^e g = tp^{e-1}ka + tp^{e-1}b$$

és $tp^e g = 0$, hiszen az új g rendje tp^e. Tudjuk, hogy az M és $\langle a \rangle$ csak a 0-ban metszik egymást. Tehát $tp^{e-1}ka = 0$ és $tp^{e-1}b = 0$, vagyis a rendje, azaz p^n osztója $tp^{e-1}k$-nak. Mivel $e \leq n$ és p nem osztója t-nek, ezért p osztója k-nak. Legyen $k = pv$. Tehát $pg = pva + b$, vagyis $pg - pva = b$. Tudjuk, hogy a b egy M csoportbeli elem, ezért a $pg - pva$ is M csoportbeli elem, azaz

$p(g - va) \in M$. Legyen $h = g - va$, és ez sincs K-ban. Ha h K-ban lenne és tudjuk, hogy $va \in K$, akkor az összegük is K csoportbeli elem lenne. Az összegük $h + va = g$, de a g-ről tudjuk, hogy nem K csoportbeli, ezért a h sem lehet K-ban. Tudjuk, hogy $ph \in M$. Tekintsük az M és a h által generált részcsoportot. Ez nagyobb M-nél, tehát M maximalitása miatt metszi $\langle a \rangle$-t nem csak a 0-ban. Vagyis vannak olyan s, w egészek, amelyre $sa = wh + c$, ahol $c \in M$. Itt w nem lehet p-vel osztható, mert akkor $wh = 0$ lenne és $c = sa$ egyenletet kapnánk. De tudjuk, hogy $M \cap \langle a \rangle = 0$, tehát $c = sa$ ellentmondás. Vagyis w nem lehet p-vel osztható, így p és w relatív prímek, és ezért vannak olyan x, y egészek, melyekre teljesül, hogy $wx + py = 1$. Ezért

$$xsa = xwh + xc = (1 - py)h + xc = h - pyh + xc.$$

Itt $ph \in M$, és ezért h benne van K-ban. Ellentmondáshoz jutottunk. Ezek szerint $A{=}\langle a \rangle + M$. Az M is Abel-csoport, és elemszáma már kisebb, mint A elemszáma. Ezért A elemszáma szerinti indukcióval bizonyítva feltehető, hogy M már prímhatványrendű ciklikus csoportok direkt összege. Mivel $\langle a \rangle$ is prímhatványrendű ciklikus csoport, ezért készen vagyunk. $\square$

Ezzel a bizonyítással beláttuk a véges Abel-csoportok alaptételében foglaltakat a felbonthatóságról, miszerint minden véges Abel-csoport felbomlik prímhatványrendű ciklikus csoportok direkt szorzatára, és konstrukciót is adtunk a felbontásra.

5. Osztható csoportok

Az előző fejezetben a bizonyítások során többször előfordult, hogy egy csoport elemét megszoroztuk egy egész számmal, azaz egy többszörösét vettük. Ezek után bevezethetjük az elem oszthatóságának definícióját, hiszen az oszthatóság a többszörösség inverz relációja.

5.1. Definíció. Legyen A Abel-csoport. Azt mondjuk, hogy az $a \in A$ elem osztható az n pozitív egésszel, ha az $nx = a$ egyenlet megoldható az A-ban, vagyis van olyan $b \in A$, amelyre teljesül, hogy $nb = a$. Ezt másképp úgy is megfogalmazhatjuk, hogy az $a \in A$ elem osztható az n pozitív egésszel, akkor ha $a \in nA$ teljesül.

5.2. Példa. Legyen $A = \mathbb{Z}_8^+$, azaz $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Vegyük a $3 \in A$ 8-adrendű elemet. Mely n-ekre lesz megoldható az $nx = 3$ egyenlet az A-ban? Az $n = 1$-re természetesen megoldható lesz. Ha $n = 3$, akkor $x = 1$, ha $n = 5$, akkor $x = 7$ és ha $n = 7$, akkor $x = 5$. Az $n = 2, 4, 6$-ra nem oldható meg az $nx = 3$ egyenlet. Észrevehetjük, hogy ha n páratlan szám, akkor a 3 osztható n-nel, és ha n páros, akkor nem.

5.3. Állítás. *([1], 7.7.15) Ha az $a \in A$ rendje n, ahol n véges, akkor az a osztható az n-hez relatív prím számokkal.*

Bizonyítás. Vizsgáljuk az A részcsoportjai közül azt a részcsoportot, amelyet az a elem generált. Az $\langle a \rangle = \{1, a, 2a, \ldots, (n-1)a\}$ részcsoport rendje: n. Azt szeretnénk belátni, hogy az $a \in k\langle a \rangle$ teljesül az olyan k egészekre, amelyek n-hez relatív prímek, és ebből következik az $a \in kA$ is. Vagyis azt szeretnénk igazolni, hogy minden olyan k-ra, amikor k relatív prím az n-hez, létezik olyan $\langle a \rangle$ részcsoportbeli elem, amelynek k-szorosa a. Ez akkor teljesül, ha az $\langle a \rangle$ és $k\langle a \rangle$ elemszáma megegyezik és ekkor az elemek is megegyeznek. Mivel a eleme volt az $\langle a \rangle$-nak, így a $k\langle a \rangle$-nak is eleme lesz, amikor k relatív prím az n-hez. Lássuk be, hogy az $\langle a \rangle = k\langle a \rangle$ minden olyan k-ra, amikor k relatív prím az n-hez. Az a többszöröse a ka-nak akkor és csak akkor, ha az a rendje és k relatív prímek. Ugyanis ekkor

$$o(ka) = \frac{o(a)}{(o(a), k)} = o(a),$$

vagyis a ka és a rendje egyenlők.

A ka többszörösei a-nak is többszörösei, és mivel tudjuk, hogy $o(a) = o(ka)$, ezért $\langle a \rangle = k\langle a \rangle$. Ekkor az a eleme a $k\langle a \rangle$-nak is. □

A csoportelemek oszthatósága után rátérhetünk a csoport oszthatóságára.

5.4. Definíció. Az A Abel-csoport osztható csoport, ha minden $a \in A$ csoportelem minden nem 0 egész számmal osztható. Másképpen fogalmazva, ha minden elemére teljesül, hogy $a \in nA$ minden nem 0 n egész számra, tehát $A = nA$ minden n egészre, ahol az n nem 0.

5.1. Példák osztható csoportokra

5.5. Állítás. *A racionális számok additív csoportja osztható.*

Bizonyítás. Vegyük a racionális számok additív csoportjának egy tetszőleges elemét: $\frac{p}{q}$. Ha erre belátjuk, hogy osztható minden nem 0 egész számmal, akkor beláttuk, hogy az egész csoport osztható, ugyanis tetszőleges elemet választottunk a $\mathbb{Q}^+$ csoportból. Tekintsük az $nx = \frac{p}{q}$ egyenletet. Legyen n nem 0 egész szám, ekkor oszthatunk n-nel. Az

$$x = \frac{\frac{p}{q}}{n} = \frac{p}{nq}$$

kapjuk. A $\frac{p}{nq}$ egy racionális szám, ahol nq nem 0, mivel a p és az nq is egy egész szám. Tehát az $nx = \frac{p}{q}$ egyenlet megoldható a racionális számok additív csoportjában minden nem 0 n-re és minden $\frac{p}{q}$ racionális számra. □

Az előző fejezetben már definiáltuk a Prüfer-csoportot, mint a p-hatványadik komplex egységgyökök multiplikatív csoportját. Ezt a csoportot kváziciklikus csoportnak is szokták nevezni.

5.6. Állítás. *A kváziciklikus csoportok osztható csoportok.*

Bizonyítás. A bizonyításban azt látjuk be, hogy a csoport minden eleme osztható minden prímszámmal. Ha ezt megtettük, akkor készen is vagyunk a bizonyítással, hiszen minden egész számot megkapunk prímszámok szorzataként. Először azt látjuk be, hogy a p-hatványadik komplex egységgyökök multiplikatív csoportjának minden eleme osztható a p prímszámmal. Ebben a

csoportban minden elem rendje p-hatvány. Legyen z egy tetszőleges elem ebből a csoportból. A $\sqrt[p]{z}$ is benne van a csoportban, hiszen:

$$z = \cos(\frac{2\pi \cdot m}{p^k}) + i \cdot \sin(\frac{2\pi \cdot m}{p^k})$$

$$\sqrt[p]{z} = \cos(\frac{\frac{2\pi \cdot m}{2^k} + 2k\pi}{p}) + i \cdot \sin(\frac{\frac{2\pi \cdot m}{2^k} + 2k\pi}{p})$$

$$\sqrt[p]{z} = \cos(\frac{2\pi(m + k \cdot p^k)}{p^{k+1}}) + i \cdot \sin(\frac{2\pi(m + k \cdot p^k)}{p^{k+1}})$$

Tehát minden csoportelem osztható a p prímmel. Most pedig azt látjuk be, hogy minden elem osztható a többi prímszámmal is. Tudjuk azt, hogy ha az $a \in A$ rendje n, ahol n véges, akkor az a osztható az n-hez relatív prím számokkal. Ebben a csoportban minden elem rendje p-hatvány, ezért minden elem osztható az adott p-hatványhoz relatív prímszámokkal. A p-hatványhoz relatív prím az összes többi prím, ezért minden elem osztható minden prímszámmal. □

5.7. Állítás. *A valós számok additív csoportja is osztható csoport.*

5.2. Az osztható csoportok alaptétele

Mit mondhatunk el két osztható csoport direkt összegéről? Vajon így osztható csoportot kapunk?

5.8. Állítás. *([3], 6.18.11) Osztható részcsoportok direkt összege is osztható.*

Bizonyítás. Legyen A és B két osztható csoport. Az A és B direkt összege C. Minden A és B csoportbeli elem osztható minden nem 0 n egész számmal. Másképp fogalmazva minden $a \in A$ elemre az $nx = a$ egyenlet megoldható az A csoportban és minden $b \in B$ elemre az $ny = b$ egyenlet megoldható a B csoportban. A C csoportbeli $a + b$ elemre $nx + ny = a + b$, ahol x egy A csoportbeli, illetve y egy B csoportbeli elem, ezért az $n(x+y) = a+b$ egyenlet megoldható a C csoportban minden nem 0 n-re. Tehát a C csoport osztható. □

5.9. Állítás. *([2], 21.3. Tétel) Minden G csoport egy H osztható csoport és egy olyan K csoport direkt összege, amelynek nincs osztható részcsoportja, azaz $G = H \oplus K$.*

Tekintsük a G csoport minden osztható részcsoportját. Ezen részcsoportok összege legyen H. Tudjuk, hogy a H is osztható csoport, mivel osztható részcsoportok direkt összege, ezt az utóbbi bizonyításban láttuk be.

5.10. Állítás. *([3], 6.18.13. Tétel) Ha B osztható részcsoport az A Abel-csoportban, akkor $A = B \oplus C$, alkalmas C részcsoporttal.*

Ha a C is osztható csoport, akkor az A is az, illetve ha a C nem osztatható, akkor az A sem az.

Az Abel-csoportok közül nem mindegyik csoport osztható csoport. Az egyelemű csoport kivételével egyetlen véges Abel-csoport sem osztható csoport. A következő tétel a végtelen osztható Abel-csoportokra vonatkozik és az egyelemű Abel-csoportra is.

5.11. Tétel. *([1], 7.7.20. Tétel) Egy Abel-csoport akkor és csak akkor osztható csoport, ha a racionális számok additív csoportja példányainak és a $\mathbb{Z}_{p^\infty}$ csoport példányainak direkt összegével izomorf. A $\mathbb{Q}^+$ csoportból és a $\mathbb{Z}_{p^\infty}$ csoportból is tetszőleges sokat vehetünk.*

5.12. Állítás. *A valós és a komplex számok additív csoportja izomorf.*

Ez az állítás halmazelméleti megfontolások miatt következik az előző tételből.

Hivatkozások

[1] Kiss Emil, *Bevezetés az algebrába*, Typotex, Budapest, 2007.

[2] László Fuchs, *Infinite Abelian groups I-II*, Academic Press, 1970, 1973.

[3] Pelikán József, Gröller Ákos *Algebra jegyzet*, 2010
`http://www.cs.elte.hu/~pelikan/algebra.html`