

A CIKLIKUS CSOPORTOK FAKTORIZÁCIÓJÁNAK PROBLÉMÁJÁHOZ

HAJÓS GYÖRGY lev. tag

Előadta az 1950. február 16-án tartott felolvasó ülésen

1. Legyen C egy Abel-féle csoport, A és B e csoport elemeinek egy-egy részhalmaza (komplexusa). Azt mondjuk, hogy C az A és B részhalmaz szorzata:

$$C = AB,$$

ha bármely $c \in C$ elemhez található $a \in A$ és $b \in B$ úgy, hogy $c = ab$, és e feltételt kielégítő a és b elemek csak egyféleképpen határozhatók meg. A $C = AB$ előállítás a C csoportnak egy *szorzatelőállítás* (faktorizációja). Nem könnyű egy C csoport valamennyi szorzatelőállítását megadni. Ez e csoport *faktorizációjának problémája*¹.

Ha A alcsoportja C -nek, akkor A mellékosztályainak egy-egy eleméből alakított B részhalmaz AB szorzatelőállítást szolgáltat. Tehát csak azok a szorzatelőállítások érdekesek, amelyeknek egyik tényezője sem alcsoport. Ilyen szorzatelőállítások is vannak, amit a következő példa mutat: Legyen C az $a^8 = 1$ által definiált ciklikus csoport, $A = (1, a^2)$, $B = (1, a, a^4, a^5)$; utóbbiak egyike sem alcsoport és $C = AB$.

Azt mondjuk, hogy a C csoportnak A részhalmaza *periodikus*, ha van C -nek olyan, egységelemétől különböző a eleme, melyre $aA = A$. Ebben az esetben A előállítható az a által generált ciklikus alcsoport s egy részhalmaz szorzataként. Egy részhalmaz tehát akkor és csak akkor periodikus, ha van olyan szorzatelőállítása, melynek egyik tényezője alcsoport. Minden alcsoport periodikus. Fentebbi példánkban B periodikus, mert $a^4B = B$.

Felmerül a kérdés, hogy vajjon egy Abel-féle csoport szorzatelőállításában mindig periodikus-e a két tényező valamelyike. Ez általában nem következik be, amit *Szele T.* következő példája mutat: Legyen C végtelen ciklikus csoport s generátoreleme a ; az $(1, a^2), (1, a^8), (1, a^{32}), \dots$ részhalmazok szorzatát A -val, az $(1, a^{-1}), (1, a^{-4}), (1, a^{-16}), \dots$ részhalmazok szorzatát B -vel jelölve, $C = AB$ szorzatelőállításhoz jutunk, melynek egyik tényezője sem periodikus.

Nehezebb véges Abel-féle csoportra találni nem-periodikus tényezőkre való felbontást. Sőt még a véges ciklikus csoportokra sem könnyű eldönteni, hogy vajjon van-e ilyen szorzatelőállításunk². Ha a csoport rendszáma prímszámhatvány, akkor nincs ily előállítás³. *Rédei L.* kimutatta⁴, hogy akkor sincs, ha a ciklikus csoport rendszáma két vagy három prímszám szorzata. E dolgozat

célja annak a kimutatása, hogy vannak véges ciklikus csoportok, amelyek előállíthatók nem-periodikus részhalmazaik szorzataként. Pontosabban a következő tételt bizonyítjuk:

Ha egy véges ciklikus csoport rendszáma felírható három olyan, egymáshoz relatív prím egészszám szorzataként, amelyek között van legalább két összetett-szám, akkor e csoport előállítható két nem-periodikus részhalmazának szorzataként.

Nyílt kérdés, hogy vajon e tétel állítása más ciklikus csoportokra is teljesül-e. Eldöntetlen a kérdés, ha a rendszám $pq^3, p^2q^3, pqr^2, pqrs$ alakú, ahol p, q, r, s prímszámok és α, β, γ pozitív egészszámok.

2. Tételünk bizonyításához geometriai megfontolás vezetett. Ezt az utat ismertetjük. Ha φ geometriai alakzatoknak és F tranzlációknak (esetleg egyetlen tranzlációból álló halmaz, akkor $F\varphi$ azoknak az alakzatoknak egyesített halmazát fogja jelölni, amelyek A tranzlációval keletkeznek az α alakzataból, ahol $\alpha \in \varphi$ és $A \in F$. Ha $A\alpha = \alpha'$, akkor az $A = (\alpha \rightarrow \alpha')$ jelölést is használjuk.

Tekintsük az n -dimenziós euklideszi teret s azt n darab ekvidisztans, párhuzamos hipersíksorral kongruens paralelotopokra bontjuk. Ezeknek a paralelotopoknak egyikét π -vel s e paralelotopok összességét (π) -vel jelöljük. P -vel jelöljük azoknak a T tranzlációknak csoportját, amelyekre $T(\pi) = (\pi)$.

Olyan φ paralelotopot választunk, mely tartalmazza π -t és (π) paralelotopjaiból épül fel, azaz (π) egyes paralelotopjait vagy egészben tartalmazza, vagy pedig nincs közös belső pontjuk. A teret egyszeresen befedjük olyan φ -val kongruens és párhuzamos helyzetű paralelotopokkal, melyeknek mindegyike (π) paralelotopjaiból épül fel. E paralelotopok összességét (φ) -val jelöljük. (π) -nek minden egyes elemét (φ) -nak egy és csak egy eleme tartalmazza. Jelölje R azoknak a T tranzlációknak csoportját, amelyekre $R(\varphi) = (\varphi)$.

P és R Abel-féle csoportok. R alcsoportja P -nek. A P/R faktorcsoporthoz C -vel jelöljük. Ha a (φ) paralelotop-halmazt megfelelően választjuk, akkor C lehet véges csoport és lehet ciklikus is. A $C = P/R$ csoport elemeinek, azaz R mellékosztályainak két részhalmazát értelmezzük.

Tekintjük először P azon T elemelt, amelyekre $T\pi \subset \varphi$. Ezeknek a T tranzlációknak mindegyike R -nek egy-egy mellékosztályához tartozik* s ezek összességét A -val jelöljük. Erre tehát $A\pi \subset R\varphi$.

Tekintjük másodszor azokat a T tranzlációkat, amelyekre $T\varphi \in (\varphi)$. E tranzlációk összessége R -nek mellékosztályaiból áll. Ha ugyanis a T_1 és T_2 tranzláció R -nek ugyanahhoz a mellékosztályához tartozik, akkor $T_1 T_2^{-1} \in R$ s így $T_2\varphi \in (\varphi)$ esetén

$$T_1\varphi = (T_1 T_2^{-1})(T_2\varphi) \in R(\varphi) = (\varphi),$$

* Mindannyian más-más mellékosztályhoz tartoznak, amit könnyű igazolni, de ezt a tényt nem használjuk fel.

azaz egy mellékosztálynak egy elemével együtt valamennyi eleme a kiszemelt tranzlációk közé tartozik. R ama mellékosztályainak összességét, amelyekhez így jutottunk, B -vel jelöljük.

Bizonyítjuk, hogy $C = AB$. Legyen T egy a $c \in C$ mellékosztályhoz tartozó tranzláció, legyen továbbá $T\pi = \pi'$ és $\pi' \subset \varrho' \in (\varrho)$. Legyen $\pi^* \in (\pi)$ az a paralelotop, melyre $(\varrho \rightarrow \varrho')\pi^* = \pi'$, melyre tehát $\pi^* \subset \varrho$. Ha $U = (\pi \rightarrow \pi^*)$ és $V = (\varrho \rightarrow \varrho')$, akkor $T = UV$ és $U \in a \in A$, $V \in b \in B$. Tehát $c = ab$.

Ha viszont $a_1 b_1 = a_2 b_2$, ahol $a_i \in A$ és $b_i \in B$ ($i = 1, 2$), akkor legyenek U_i és V_i olyan tranzlációk, melyekre $T = U_1 V_1 = U_2 V_2$ és

$$\begin{aligned} U_i \in a_i, \quad U_i \pi = \pi_i \subset \varrho, \\ V_i \in b_i, \quad V_i \varrho = \varrho_i \subset (\varrho). \end{aligned} \quad (i = 1, 2)$$

Minthogy $T\pi = V_i(U_i\pi) = V_i\pi_i \subset V_i\varrho = \varrho_i$, azért $\varrho_1 = \varrho_2$. Ebből következik, hogy $V_1 = (\varrho \rightarrow \varrho_1) = (\varrho \rightarrow \varrho_2) = V_2$ és $U_1 = TV_1^{-1} = TV_2^{-1} = U_2$, tehát $a_1 = a_2$ és $b_1 = b_2$. Ezzel befejeztük $C = AB$ bizonyítását.

A B részhalmaz nem periodikus. Legyen ugyanis $aB = B$ és $a \in C$, továbbá a T tranzlációra $T \in a$. Állításunkat $T(\varrho) = (\varrho)$ kimutatásával bizonyítjuk, mert ebből $T \in R$ és így az következik, hogy a a C csoport egységeleme. Legyen $\varrho_1 \in (\varrho)$, $(\varrho \rightarrow \varrho_1) \in b_1 \in B$ és $ab_1 = b_2 \in B$, tehát $T(\varrho \rightarrow \varrho_1) \in b_2$. Ekkor

$$T\varrho_1 = [T(\varrho \rightarrow \varrho_1)]\varrho \in b_2\varrho \subset (\varrho),$$

s mivel ez minden $\varrho_1 \in (\varrho)$ paralelotopra áll, valóban $T(\varrho) = (\varrho)$.

Ha $aA = A$, ahol $a \in C$, és $T \in a$, akkor $T(R\varrho) = R\varrho$. Legyen ugyanis $\pi_1 \subset \varrho_1 \in R\varrho$, $(\varrho \rightarrow \varrho_1)\pi^* = \pi_1$ és így $\pi^* \subset \varrho$. Ekkor

$$\begin{aligned} T\pi_1 &= T(\varrho \rightarrow \varrho_1)\pi^* = (\varrho \rightarrow \varrho_1)T(\pi \rightarrow \pi^*)\pi \in \\ &\in (\varrho \rightarrow \varrho_1)aA\pi = (\varrho \rightarrow \varrho_1)A\pi \subset R \cdot R\varrho = R\varrho. \end{aligned}$$

Minthogy ez minden $\pi_1 \subset R\varrho$ paralelotopra áll, valóban $T(R\varrho) = R\varrho$.

Ha az $R\varrho$ paralelotop-halmaz izolált paralelotopokból áll, akkor $T(R\varrho) = R\varrho$ csak $T \in R$ esetében állhat fenn. Ebben az esetben tehát A nem periodikus, mert $aA = A$, $T \in a$ relációknak $T \in R$ a folyománya s így a a C csoport egységeleme.

Egy módszert dolgoztunk ki olyan C csoportok megalkotására, amelyek nem-periodikus részhalmazaik szorzataként előállíthatók. Ha a (π) paralelotop-halmazból megfelelően építjük fel a (ϱ) paralelotop-halmazt, akkor az előírásainkkal definiált C csoport ciklikus, ennek A, B részhalmazaira $C = AB$, és e tényezőknek egyike sem periodikus, ha $R\varrho$ izolált paralelotopokból áll.

3. Tételünk bizonyítására a mondottaknak megfelelő paralelotop-halmazt szerkesztünk. Legyen a ciklikus C csoport rendszáma $n = m_1 m_2 m_3$, ahol m_1, m_2, m_3 relatív prím egészszámok, s legyen $m_1 = u_1 v_1$, $m_2 = u_2 v_2$, ahol u_1, u_2, v_1, v_2 egyménél nagyobb egészszámok.

A bizonyítást háromdimenziós térben végezzük. A tranzlációkat vektoraikkal jellemezzük s azokkal jelöljük. Legyen i, j, k három páronként merőleges

egységvektor és π egy ezekkel párhuzamos helyzetű, egységélű kocka. Az ebből megszerkesztett (π) kocka-rendszerhez az i, j, k tranzlációkkal generált P csoport tartozik.

A ϱ paralelepipedont (π) ama kockái alkossák, amelyek π -ből

$$\alpha i + \beta j \quad (\alpha = 0, 1, 2, \dots, u_1 - 1; \beta = 0, 1, 2, \dots, u_2 - 1)$$

tranzlációkkal keletkeznek. Legyen R az $m_1 i, m_2 j, m_3 k$ tranzlációkkal generált csoport. Így P/R az m_1, m_2, m_3 rendű ciklikus csoportok külső szorzata és, mivel ezek a rendszámok relatív prímek, P/R valóban $n = m_1 m_2 m_3$ rendszámú ciklikus csoport.

Ha most még a (ϱ) halmazt úgy definiáljuk, hogy ehhez valóban a mondott R tranzláció-csoport tartozzék, akkor az adott C csoportnak nem-periodikus tényezőkre való felbontásához jutunk, mert a definiált $R\varrho$ halmaz izolált paralelepipedonokból áll.

Tekintjük evégből először azt a $(\varrho)'$ paralelepipedon-halmazt, amelyik ϱ -ból az $u_1 i, u_2 j, k$ tranzlációkkal generált csoport elemeinek alkalmazásával áll elő. E $(\varrho)'$ halmaz a teret egyszeresen betölti.

$(\varrho)'$ -nek ama paralelepipedonjai, amelyek $R\varrho$ paralelepipedonjaiból

$$k + \mu u_1 i, \text{ ill. } u_1 i + \nu u_2 j \quad (\mu, \nu \text{ egész})$$

eltolásokkal állanak elő, i ill. j irányú oszlopokat alkotnak. Ez pontosabban azt jelenti, hogy $(\varrho)'$ -nek így kiválasztott részhalmazaira i , ill. j tranzlációt alkalmazva a térnek változatlanul ugyanazt a részét egyszeresen betöltő paralelepipedon-halmazt kapunk. Hagyjuk el $(\varrho)'$ -ből a mondott két részhalmazt s pótoljuk ezeket azokkal a paralelepipedon-halmazokkal, amelyek az elhagyottakból i , ill. j tranzláció alkalmazásával keletkeznek. Az így definiált paralelepipedon-halmaz a teret egyszeresen betölti s ezt választjuk (ϱ) halmaznak.

(ϱ) definíciójából következik, hogy $R\varrho$ paralelepipedonjai (ϱ) -hoz tartoznak és $R(\varrho) = (\varrho)$. Megállapíthatjuk továbbá, hogy ha $R\varrho$ paralelepipedonjaira akár k , akár $u_1 i$ tranzlációt alkalmazunk, olyan paralelepipedonhoz jutunk, amelyik nem tartozik (ϱ) -hoz. Minthogy a (ϱ) halmaznak $R\varrho$ -hoz nem tartozó paralelepipedonjai a mondott tulajdonságokkal nem rendelkeznek, azért $T(\varrho) = (\varrho)$ esetében a T tranzláció csak olyan lehet, hogy $T(R\varrho) = R\varrho$ is fennáll, azaz $T \in R$. Így a (ϱ) halmazhoz valóban az R tranzláció-csoport tartozik.

4. Ha geometriai megfontolásainkból kiolvassuk egy adott C csoporthoz a talált nem-periodikus tényezőket, eredményünk tiszta csoportelméleti alakban jelentkezik s ezt az eredményt már könnyű lesz tiszta csoportelméleti úton is verifikálni. Ezáltal azt érjük el, hogy e dolgozat 2 és 3 kihagyásával is logikailag hiánytalan marad.

Legyenek az additív Abel-féle C csoport generátorelemei a, b, c , definiáló relációi pedig

$$m_1 a = 0, \quad m_2 b = 0, \quad m_3 c = 0,$$

ahol m_1, m_2, m_3 relatív prím egészs számok s így a C csoport $n = m_1 m_2 m_3$ rendszámú ciklikus csoport. Legyen továbbá $m_1 = u_1 v_1, m_2 = u_2 v_2$, ahol u_1, v_1, u_2, v_2 egynél nagyobb egészs számok. A C csoportnak két részhalmazát adjuk meg.

Az A részhalmaz elemei:

$$\alpha a + \beta b \quad (\alpha = 0, 1, 2, \dots, u_1 - 1; \beta = 0, 1, 2, \dots, u_2 - 1).$$

Ez a részhalmaz nem periodikus. Ha ugyanis $x + A = A$, akkor

$$x + 0 \text{ és } x + (u_1 - 1)a + (u_2 - 1)b$$

A -hoz tartozik, x tehát közös eleme az

$$A \text{ és } A - (u_1 - 1)a - (u_2 - 1)b$$

halmazoknak. Ezeknek viszont egyetlen közös elemük 0 és ezért csak $x = 0$ lehetséges.

A B részhalmaz elemei:

$$\alpha u_1 a + \beta u_2 b \quad (\alpha \neq 1),$$

$$u_1 a + (1 + \beta u_2) b,$$

$$\alpha u_1 a + \beta u_2 b + c, \quad (\beta \neq 0),$$

$$(1 + \alpha u_1) a + c,$$

$$\alpha u_1 a + \beta u_2 b + \gamma c,$$

ahol α, β, γ olyan egészs számok, amelyekre (a már tett megszorításokon kívül)

$$0 \leq \alpha < v_1, \quad 0 \leq \beta < v_2, \quad 2 \leq \gamma < m_3.$$

Ez a részhalmaz nem periodikus, hiszen 0 az egyetlen olyan eleme, amelyből $u_1 a$ vagy c hozzáadásával B -hez nem tartozó elemet kapunk.

A C csoport az A és B részhalmazok összege. Ezt a következőképpen láthatjuk be. C nyilván előáll A és az $\alpha u_1 a + \beta u_2 b + \gamma c$ elemekből ($0 \leq \alpha < v_1, 0 \leq \beta < v_2, 0 \leq \gamma < m_3$) álló B' halmaz összegeként. B abban különbözik a B' halmaztól, hogy

$$u_1 a + \beta u_2 b \text{ helyett } u_1 a + (1 + \beta u_2) b,$$

$$\alpha u_1 a + c \text{ helyett } (1 + \alpha u_1) a + c$$

elemeket tartalmazza. Viszont e halmazpárokhoz a $(0, b, 2b, \dots, (u_2 - 1)b)$, ill. $(0, a, 2a, \dots, (u_1 - 1)a)$ halmazok elemeit hozzáadva azonos összeghalmazokhoz jutunk s így mindkét halmazpár azonos összeget eredményez, ha az A halmazt adjuk hozzájuk, hiszen A a mondott két halmaz összege. Ezért $A + B = A + B' = C$.

5. A legkisebb n szám, amelyik tételünk feltételét kielégíti, 180. Álljon itt e rendszámra a talált nem-periodikus szorzatelállításnak egy példája. E példát az egészs számok mod 180 additív csoportjára fogalmazzuk.

A elemei

$$0, 20, 45, 65, 100, 145.$$

B elemei

0, 6, 10, 12, 18, 24, 42, 48, 54, 60, 66, 70, 72, 78, 81,
84, 96, 102, 108, 114, 120, 130, 132, 138, 144, 156, 162, 168, 171, 174.

E halmazok elemeit páronként mod 180 összeadva teljes maradékrendszeret kapunk.

6. A véges Abel-féle csoportokra eddig ismert minden szorzatelőállítás kváziperiodikus a szó következő értelmében: Azt mondjuk, hogy a $C = AB$ szorzatelőállítás kváziperiodikus, ha az A és B részhalmazok egyike, pl. B felbontható oly módon $B_1, B_2, \dots, B_k$ halmazokra, hogy az $AB_1, AB_2, \dots, AB_k$ részhalmazok egyiküknek egy periodikus részhalmaz elemeivel való szorzataiként állíthatók elő. Azaz található olyan periodikus $(b_1, b_2, \dots, b_k)$ részhalmaz, hogy az AB_i és $AB_1 b_i$ részhalmazok sorrendjüktől eltekintve, azonosak. Nyílt kérdés, hogy vajon a véges Abel-féle csoportoknak minden szorzatelőállítása kváziperiodikus-e. Még véges ciklikus csoportok esetére sem sikerült e kérdésre feleletet adni.

*Budapesti Eötvös Loránd Tudományegyetem
Matematikai Intézete.*

IRODALOM

- ¹ G. Hajós, Sur la factorisation des groupes abéliens, Časopis 74, (1950), 157–162.
- ² Lásd i. m.¹
- ³ Lásd i. m.¹ és L. Rédei i. m.⁴
- ⁴ L. Rédei Ein Beitrag zum Problem der Faktorisierung von endlichen Abelschen Gruppen, Acta Math. Hung. 1 (1950), 197.