

Az egész számok feletti csoportgyűrűk egységcsoportjai

Készítette: Nyilas János

Szak: matematika

Intézmény: II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

Témavezető: Dr. Bódi Béla

Munkahely: II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

2012. október 18.

Tartalomjegyzék

Bevezetés.....	3
1. A csoportgyűrű fogalma.....	4
2. Egységek a csoportgyűrűben.....	8
3. Triviális egységek a csoportgyűrűben.....	9
4. A csoportgyűrű centruma.....	14
5. Példák.....	17
5.1. 8-ad rendű csoportok egész számok feletti csoportgyűrűinek egységei.....	17
5.2. 16-od rendű csoportok egész számok feletti csoportgyűrűinek egységei....	18
Összefoglalás.....	22
Hivatkozások.....	23

BEVEZETÉS

A csoportalgebra fogalmát Frobenius vezette be a múlt század elején, ami különösen hasznosnak bizonyult a véges csoportok reprezentációinak vizsgálatában. Ezt követően, évtizedekig csak alkalmazások szempontjából vizsgálták a csoportgyűrűket. A múlt század 60-as éveiben a végtelen csoportokkal képzett csoportgyűrűkről nagyon sok eredmény született. Néhány év alatt kialakult e terület problematikája, bővültek a tematikai vizsgálatok és több áttekintő cikk is megjelent. A gyűrűelmélet határterületén megszületett az algebra egy új ága - a csoportgyűrűk elmélete. A csoportgyűrűk nagyon érdekes algebrai struktúrák, amelyeket nemcsak a reprezentációelméletben, hanem természetesen a csoport és gyűrűelméleten kívül a homológiában, kohomológiában, a kódelméletben és az algebrai topológiában is alkalmaznak.

A csoportgyűrűk egységcsoportjának vizsgálatát G. Higman kezdeményezte a múlt század 40-es éveiben. Disszertációja hosszú időre meghatározta az egész számok feletti csoportgyűrűk egységcsoportjának problematikáját és további kutatását. Az egységcsoportok iránti érdeklődést fokozta, hogy egyes eredményeit más területeken is sikeresen alkalmazták.

Sajnos jelenleg kevés csoportgyűrű egységcsoportjának a struktúrájára sikerült teljes jellemzést adni, így e terület problematikája a mai napig nyitott. Az egységcsoport csoportelméleti szempontból való vizsgálata azért érdekes mivel ez egy olyan csoport, amelyben explicit számításokat lehet végezni. Munkám célja az egész számok feletti csoportgyűrűk tanulmányozása és egységeinek meghatározása. Munkám első fejezeteiben ismertetem mindazon csoportgyűrű elméleti alapfogalmakat és tételeket melyeket további munkám során felhasználok. Munkám további részében meghatározom az alacsonyabb rendű csoportok egész számok feletti csoportgyűrűinek egységeit, illetve konkrét példákön szemléltetem az erre alkalmas módszerek használatát.

1. A CSOPORTGYŰRŰ FOGALMA

Legyen G véges csoport a szorzásra nézve, illetve $\mathbb{Z}$ az egész számok gyűrűje. Legyen

$$u : G \rightarrow \mathbb{Z}$$

a G csoporton értelmezett függvény, és jelölje

$$\text{Supp}(u) = \{g \in G \mid u(g) \neq 0\}$$

az u függvény **tartóját**.

Jelölje $\mathbb{Z}G$ a G csoportnak a $\mathbb{Z}$ gyűrűre való leképezéseinek a halmazát. Két $u, v \in \mathbb{Z}G$ függvényt akkor tekintünk egyenlőnek, ha tetszőleges $g \in G$ esetén $u(g) = v(g)$. Most definiáljuk következőképpen tetszőleges $u, v \in \mathbb{Z}G$ elemek összeadását

$$(u + v)(g) = u(g) + v(g),$$

illetve szorzását

$$(uv)(g) = \sum_{h \in G} u(h)v(h^{-1}g).$$

A $\mathbb{Z}G$ halmaz a rajta definiált műveletekre nézve gyűrűt alkot, melyet a továbbiakban **csoportgyűrűnek** nevezünk.

A csoportgyűrűk vizsgálatának egyszerűsítése céljából érdemes bevezetnünk a

$$\{\forall g \in G \mid u(g) = u_g\}$$

jelölést. Ekkor az $u \in \mathbb{Z}G$ függvény egy $\sum_{g \in G} u_g g$ alakú formális összeggel egyértelműen meghatározható, így a függvényt a továbbiakban formális összegként tudjuk kezelni. A formális összegek bevezetésével a csoportgyűrűre vonatkozó műveletek a következőképpen definiáltak: ha

$$u = \sum_{g \in G} u_g g \text{ és } v = \sum_{g \in G} v_g g$$

a $\mathbb{Z}G$ elemei, ahol $u_g, v_g \in \mathbb{Z}$, akkor

$$u + v = \sum_{g \in G} (u_g + v_g) g \text{ és}$$
$$uv = \sum_{g \in G} \left(\sum_{h \in G} u_h v_{h^{-1}g} \right) g.$$

Fontos megjegyzés, hogy a $\mathbb{Z}G$ csoportgyűrűben a G csoport elemei és a $\mathbb{Z}$ gyűrű elemei felcserélhetők és a $\mathbb{Z}G$ csoportgyűrű elemeinek formális összeg alakban való felírásánál a nulla együtthatóval rendelkező tagokat elhagyjuk.

1.1. DEFINÍCIÓ. Legyen $u = \sum_{g \in G} u_g g$ a $\mathbb{Z}G$ csoportgyűrű nullától különböző eleme. A G csoport

$$\text{Supp}(u) = \{g \in G \mid u_g \neq 0\}$$

részalmazát az u elem **tartójának**, a $\text{Supp}(u)$ által generált részcsoportot pedig az u elem **tartócsoportjának** nevezzük, és a $\langle \text{Supp}(u) \rangle$ jelölést alkalmazzuk.

A $\mathbb{Z}G$ csoportgyűrű vizsgálatánál kiemelt szerep jut a G csoport részcsoportjai által meghatározott ideáloknak. A továbbiakban ezen ideálok néhány fontosabb tulajdonságával foglalkozunk.

A G csoport H részcsoportja szerinti baloldali mellékosztályok egy teljes reprezentánsrendszerét $R_l(G/H)$ -val, a jobboldali mellékosztályok egy teljes reprezentánsrendszerét $R_r(G/H)$ -val jelöljük. A reprezentánsrendszerek szabad kiválasztása miatt a továbbiakban mindig feltételezzük, hogy azok tartalmazzák a csoport egységelemét.

Legyen $H \leq G$ és jelölje $I_l(H)$ a $\mathbb{Z}G$ csoportgyűrű összes olyan elemének a halmazát amely felírható

$$\sum_{h \in H} u^{(h)}(h - 1)$$

alakban, ahol $u^{(h)} \in \mathbb{Z}G$. Látható, hogy $I_l(H)$ a $\mathbb{Z}G$ csoportgyűrű balideálja, és ennek generátorrendszerét a $\{h - 1 \mid h \in H\}$ elemek adják. Hasonlóképpen határozható meg az $I_r(H)$ jobbideál. Ha $I_l(H)$ kétoldali ideálja $\mathbb{Z}G$ -nek akkor az $I(H)$ jelölést használjuk.

1.2. LEMMA. Ha a $\mathbb{Z}G$ csoportgyűrűben az $I_l(H)$ balideált mint baloldali $\mathbb{Z}$ -modulust tekintjük, akkor ez szabad modulus, és az

$$M = \{x(h - 1) \mid x \in R_l(G/H), 1 \neq h \in H\}$$

halmaz elemei az $I_l(H)$ szabad $\mathbb{Z}$ -modulus bázisát adják.

Bizonyítás: A tételt indirekt módon bizonyítjuk, azaz tegyük fel hogy M elemei lineárisan összefüggőek a $\mathbb{Z}$ gyűrű felett. Válasszunk ki M -ből egy minimális lineárisan összefüggő rendszert. Ennek elemeire érvényes az

$$u_{h_1} x_1 (h_1 - 1) + u_{h_2} x_2 (h_2 - 1) + \dots + u_{h_s} x_s (h_s - 1) = 0 \quad (1.1)$$

összefüggés, ahol $x_i \in R_l(G/H)$, $1 \neq h_i \in H$ és $0 \neq u_{h_i} \in \mathbb{Z}$. Mivel az $x_i (h_i - 1)$ elem tartója részalmazza az $x_i H$ mellékosztálynak, és H különböző mellékosztályai nem tartalmazznak közös elemet, 1.1 csak akkor lehetséges ha $x_1 = x_2 = \dots = x_s$. Mivel a

$h_1, h_2, \dots, h_s$ elemek különbözőek és $h_i \neq 1$, ezért 1.1-ből következik, hogy

$$u_{h_1}h_1 + u_{h_2}h_2 + \dots + u_{h_s}h_s = \sum_{i=1}^s u_{h_i},$$

ami ellentmondás, tehát M elemei lineárisan függetlenek a $\mathbb{Z}$ gyűrű felett.

Most legyen $g \in G$, $h \in H$ és $g = xh_1$ ahol $x \in R_l(G/H)$ és $h_1 \in H$. A

$$g(h-1) = x(h_1h-1) - x(h_1-1)$$

egyenlőség azt bizonyítja, hogy M elemei az $I_l(H)$ ideál bázisát adják. ■

1.3. TÉTEL. Legyen $\varphi : G \rightarrow H$ epimorfizmus, amelynek magja az N normális részcsoporth, és legyen

$$\tilde{\varphi} \left(\sum_{g \in G} u_g g \right) = \sum_{g \in G} u_g \varphi(g) \quad (u_g \in \mathbb{Z}).$$

A $\tilde{\varphi} : \mathbb{Z}G \rightarrow \mathbb{Z}H$ leképezés a $\mathbb{Z}G$ csoportgyűrűt a $\mathbb{Z}H$ csoportgyűrűre képező homomorfizmus, és ennek magja az $I(N)$ ideál.

Bizonyítás: Legyen u és v a $\mathbb{Z}G$ tetszőleges elemei. Az összeadás tulajdonságaiból adódik, hogy

$$\tilde{\varphi}(u+v) = \sum_{g \in G} (u_g + v_g) \varphi(g) = \tilde{\varphi}(u) + \tilde{\varphi}(v).$$

Ha $k, l \in \mathbb{Z}$ és $g, h \in G$, akkor

$$\tilde{\varphi}(kg \cdot lh) = \tilde{\varphi}(klgh) = kl\varphi(gh) = kl\varphi(g)\varphi(h) = \tilde{\varphi}(kg)\tilde{\varphi}(lh).$$

Mivel $\tilde{\varphi}$ a $\mathbb{Z}G$ gyűrű additív csoportjának a $\mathbb{Z}H$ gyűrű additív csoportjára való homomorfizmusa nyilvánvaló, hogy

$$\tilde{\varphi}(u)\tilde{\varphi}(v) = \tilde{\varphi}(uv)$$

tehát ezzel beláttuk, hogy $\tilde{\varphi}$ gyűrű-homomorfizmus.

Ha $x \in R_l(G/N)$ és $n \in N$ akkor

$$\tilde{\varphi}(x(n-1)) = \varphi(x)\tilde{\varphi}(n-1) = 0,$$

és az 1.2 lemmából következik, hogy az $I(N)$ ideál a $\tilde{\varphi}$ homomorfizmus magjában van.

Könnyedén belátható, hogy a G csoport

$$G = \bigcup_{x \in R_l(G/N)} xN$$

diszjunkt halmazokra bontható. Nyilvánvaló, hogy hasonlóképpen igaz az $R_r(G/N)$ jobb-oldali mellékosztályok teljes reprezentáns rendszere esetében is. Legyen az u elem a $\tilde{\varphi}$ homomorfizmus magjában. Belátható, hogy az u elem egyértelműen előáll

$$u = u_1 y_1 + u_2 y_2 + \dots + u_s y_s$$

alakban, ahol $y_i \in R_r(G/N)$ és $u_i \in \mathbb{Z}N = \sum_{n \in N} u_n^{(i)} n$.

Ekkor

$$\begin{aligned} 0 &= \tilde{\varphi}(u) = \tilde{\varphi}(u_1) \tilde{\varphi}(y_1) + \tilde{\varphi}(u_2) \tilde{\varphi}(y_2) + \dots + \tilde{\varphi}(u_s) \tilde{\varphi}(y_s) = \\ &= \left(\sum_{n \in N} u_n^{(1)} \right) \varphi(y_1) + \dots + \left(\sum_{n \in N} u_n^{(s)} \right) \varphi(y_s). \end{aligned}$$

Mivel $\varphi(y_1), \dots, \varphi(y_s)$ páronként különbözőek, így $\sum_{n \in N} u_n^{(i)} = 0$ tetszőleges $1 \leq i \leq s$ esetén,

$$u_i = \sum_{n \in N} u_n^{(i)} (n - 1) + \sum_{n \in N} u_n^{(i)} = \sum_{n \in N} u_n^{(i)} (n - 1) \in I(N).$$

Következtetésképpen $u \in I(N)$. ■

Legyen az $x \rightarrow x^*$ leképezés a $\mathbb{Z}G$ csoportgyűrűnek egy másodrendű anti-automorfizmusa, azaz $\mathbb{Z}G$ -nek olyan kölcsönösen egyértelmű leképezése, melyre tetszőleges $u, v \in \mathbb{Z}G$ esetén, a következő

1. $(u + v)^* = u^* + v^*$,
2. $(uv)^* = v^* u^*$,
3. $(u^*)^* = u$

feltételek teljesülnek. Ezt a leképezést a $\mathbb{Z}G$ csoportgyűrű **involúciójának** nevezzük.

1.4. LEMMA. Az

$$u = \sum_{g \in G} u_g g \rightarrow u^* = \sum_{g \in G} u_g g^{-1} \tag{1.2}$$

leképezés $\mathbb{Z}G$ -nek involúciója.

Bizonyítás: Legyen $\forall u, v \in \mathbb{Z}G$, ekkor

$$(u + v)^* = \sum_{g \in G} (u_g + v_g) g^{-1} = \sum_{g \in G} (u_g g^{-1} + v_g g^{-1}) = \sum_{g \in G} u_g g^{-1} + \sum_{g \in G} v_g g^{-1} = u^* + v^*,$$

$$(uv)^* = \sum_{g \in G} \left(\sum_{x \in G} u_x v_{x^{-1}g} \right) g^{-1} = \sum_{g \in G} \left(\sum_{x, y \in G} u_x v_y \right) g^{-1} = \sum_{y \in G} v_y y^{-1} \sum_{x \in G} u_x x^{-1} = v^* u^*,$$

$$(u^*)^* = \left(\sum_{g \in G} u_g g^{-1} \right)^* = \sum_{g \in G} u_g (g^{-1})^{-1} = \sum_{g \in G} u_g g = u.$$

És ezzel bizonyítottuk a lemma állítását. ■

2. EGYSÉGEK A CSOPORTGYŰRŰBEN

2.1. DEFINÍCIÓ. A $\mathbb{Z}G$ csoportgyűrű u elemére azt mondjuk, hogy **egység**, ha létezik olyan $v \in \mathbb{Z}G$, hogy $uv = vu = 1$.

Nyilvánvaló, hogy a $\mathbb{Z}G$ csoportgyűrű összes egységei csoportot alkotnak, amelyet a $\mathbb{Z}G$ **csoportgyűrű egységcsoportjának** nevezünk, és rá a továbbiakban az $U(\mathbb{Z}G)$ jelölést alkalmazzuk.

Legyen $u = \sum_{g \in G} u_g g$ a $\mathbb{Z}G$ csoportgyűrű eleme és

$$\chi(u) = \sum_{g \in G} u_g.$$

Belátható, hogy a $\chi : \mathbb{Z}G \rightarrow \mathbb{Z}$ a $\mathbb{Z}G$ csoportgyűrűt a $\mathbb{Z}$ gyűrűre képező homomorfizmus.

Ennek alapján

$$V(\mathbb{Z}G) = \left\{ u = \sum_{g \in G} u_g g \in U(\mathbb{Z}G) \mid \sum_{g \in G} u_g = 1 \right\}$$

részcsoportha az $U(\mathbb{Z}G)$ csoportnak, és a $\mathbb{Z}G$ csoportgyűrű **normalizált egységcsoportjának** nevezzük.

Világos, hogy G részcsoportha $V(\mathbb{Z}G)$ -nek, továbbá

$$U(\mathbb{Z}G) = V(\mathbb{Z}G) \times U(\mathbb{Z}) = V(\mathbb{Z}G) \times \{-1, 1\}. \quad (2.1)$$

Az $U(\mathbb{Z})G = \{kg \mid k \in U(\mathbb{Z}), g \in G\}$ halmaz elemei a $\mathbb{Z}G$ csoportgyűrű egységei. Ezeket az egységeket **triviális egységeknek** nevezzük.

2.2. DEFINÍCIÓ. A $V(\mathbb{Z}G) = G$ teljesülésekor a $V(\mathbb{Z}G)$ csoportot **triviálisnak** nevezzük.

3. TRIVIÁLIS EGYSÉGEK A CSOPORTGYŰRŰBEN

A csoportgyűrű egységeinek a vizsgálatánál általában nagyon nehéz feladat annak megállapítása, hogy az adott csoportgyűrű rendelkezik-e valódi egységekkel. Ezen fejezet célja olyan csoportgyűrűk bemutatása amelyek csak triviális egységeket tartalmaznak. A következő tételek bizonyításánál figyelembe vesszük a 2.1 direkt felbontás következményét, azaz ha az egész számok feletti csoportgyűrűben a normalizált egységcsoport triviális, akkor az egységcsoport csak triviális egységeket tartalmaz.

3.1. TÉTEL. *A $\mathbb{Z}C_2$ -nek csak triviális egységei vannak.*

Bizonyítás: Legyen adott tetszőleges $u = \alpha_0 + \alpha_1 a$ eleme a $V(\mathbb{Z}C_2)$ csoportnak, és az inverze legyen $u^{-1} = \beta_0 + \beta_1 a$. Nyilvánvaló, hogy $\alpha_0 + \alpha_1 = 1$ és $\beta_0 + \beta_1 = 1$, illetve

$$uu^{-1} = (\alpha_0 + \alpha_1 a)(\beta_0 + \beta_1 a) = 1.$$

A zárójeleket felbontva

$$\alpha_0\beta_0 + \alpha_0\beta_1 a + \alpha_1\beta_0 a + \alpha_1\beta_1 = 1,$$

majd pedig átrendezve a tagokat,

$$(\alpha_0\beta_0 + \alpha_1\beta_1) + (\alpha_1\beta_0 + \alpha_0\beta_1)a = 1.$$

Mindezekből kapjuk az egységeket meghatározó diofantoszi egyenletrendszert a $\mathbb{Z}$ -ben

$$\begin{cases} \alpha_0 + \alpha_1 = 1 \\ \beta_0 + \beta_1 = 1 \\ \alpha_0\beta_0 + \alpha_1\beta_1 = 1 \\ \alpha_0\beta_1 + \alpha_1\beta_0 = 0. \end{cases} \quad (3.1)$$

A rendszer utolsó előtti egyenletéből kivonva az utolsó egyenletét újabb egyenletet kapunk

$$(\alpha_0 - \alpha_1)\beta_0 + (\alpha_1 - \alpha_0)\beta_1 = 1,$$

és a megfelelő algebrai átalakítás után kapjuk, hogy

$$(\alpha_0 - \alpha_1)(\beta_0 - \beta_1) = 1.$$

A $\mathbb{Z}$ -ben ennek megoldása visszavezetődik az

$$\begin{cases} \alpha_0 + \alpha_1 = 1 \\ \alpha_0 - \alpha_1 = \pm 1 \end{cases} \quad (3.2)$$

egyenletrendszer megoldására. Ebből az egyenletrendszerből következik, hogy

$$\begin{cases} \alpha_0 = 0 \\ \alpha_1 = 1 \end{cases} \text{ vagy } \begin{cases} \alpha_0 = 1 \\ \alpha_1 = 0 \end{cases} \quad (3.3)$$

azaz a $V(\mathbb{Z}C_2)$ csoport triviális. Ezzel a tétel állítását igazoltuk. ■

3.2. TÉTEL. *A $\mathbb{Z}C_3$ -nak csak triviális egységei vannak.*

Bizonyítás: Legyen $u = \alpha_0 + \alpha_1 a + \alpha_2 a^2$ a $V(\mathbb{Z}C_3)$ tetszőleges eleme. Értelmezzünk a C_3 csoporton egy olyan φ leképezést, mely a csoport tetszőleges g elemét az inverzébe viszi át, azaz $\forall g \in C_3 : \varphi(g) = g^{-1}$ és terjesszük ki lineárisan a $\mathbb{Z}C_3$ csoportgyűrűre, azaz $\forall v \in \mathbb{Z}C_3 : \tilde{\varphi}(v) = \sum_{g \in C_3} v_g \varphi(g)$. Az 1.4 lemmából következik, hogy a definiált leképezés involúció a csoportgyűrűben.

Vizsgáljuk meg az $u\tilde{\varphi}(u)$ egység szorzatot:

$$\begin{aligned} u\tilde{\varphi}(u) &= (\alpha_0 + \alpha_1 a + \alpha_2 a^2) (\alpha_0 + \alpha_2 a + \alpha_1 a^2) = \\ &= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + (\alpha_0 \alpha_1 + \alpha_1 \alpha_2 + \alpha_0 \alpha_2) (a + a^2). \end{aligned}$$

Legyen $\gamma_1 = \alpha_0^2 + \alpha_1^2 + \alpha_2^2$ és $\gamma_2 = \alpha_0 \alpha_1 + \alpha_0 \alpha_2 + \alpha_1 \alpha_2$. Az $u\tilde{\varphi}(u) = \gamma_1 + \gamma_2 (a + a^2)$ szorzat egység és legyen inverze $\delta_1 + \delta_2 (a + a^2)$ alakú. Ekkor

$$\begin{aligned} u\tilde{\varphi}(u) (\delta_1 + \delta_2 (a + a^2)) &= \gamma_1 \delta_1 + \gamma_2 \delta_2 (a + a^2)^2 + (\gamma_1 \delta_2 + \gamma_2 \delta_1) (a + a^2) = \\ &= (\gamma_1 \delta_1 + 2\gamma_2 \delta_2) + (\gamma_1 \delta_2 + \gamma_2 \delta_2 + \gamma_2 \delta_1) (a + a^2) = 1. \end{aligned}$$

Az egységeket meghatározó diofantoszi egyenletrendszer a következő:

$$\begin{cases} \gamma_1 \delta_1 + 2\gamma_2 \delta_2 = 1 \\ \gamma_1 \delta_2 + \gamma_2 \delta_2 + \gamma_2 \delta_1 = 0. \end{cases} \quad (3.4)$$

Könnyedén belátható, hogy $u\tilde{\varphi}(u)$ és inverze normalizált egységek ezért $\gamma_1 + 2\gamma_2 = 1$ és $\delta_1 + 2\delta_2 = 1$. Behelyettesítve a 3.4 rendszerbe, hogy $\gamma_1 = 1 - 2\gamma_2$ és $\delta_1 = 1 - 2\delta_2$ az

$$\begin{cases} (1 - 2\gamma_2) (1 - 2\delta_2) + 2\gamma_2 \delta_2 = 1 \\ (1 - 2\gamma_2) \delta_2 + \gamma_2 \delta_2 + \gamma_2 (1 - 2\delta_2) = 0 \end{cases}$$

egyenletrendszerhez jutunk, melyből azt kapjuk, hogy

$$\delta_2 = \frac{\gamma_2}{3\gamma_2 - 1}. \quad (3.5)$$

Ennek $\mathbb{Z}$ feletti megoldása a $\gamma_2 = \delta_2 = 0$. Ezt a 3.4 rendszer első egyenletébe helyettesítve kapjuk, hogy $\gamma_1 \delta_1 = 1$ melyből pedig következik, hogy $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 = 1$ azaz $\mathbb{Z}C_3$ -ban csak triviális egységek vannak. ■

3.3. TÉTEL. A $\mathbb{Z}C_4$ -nek csak triviális egységei vannak.

Bizonyítás: Legyen $u = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3$ tetszőleges $V(\mathbb{Z}C_4)$ elem. Legyen φ leképezés olyan, hogy tetszőleges $g \in C_4$ elemre $\varphi(g) = g^2$. Könnyedén igazolható, hogy a φ homomorfizmus és képe izomorf a C_2 csoporttal. Terjesszük ki a φ leképezést lineárisan a $\mathbb{Z}C_4$ csoportgyűrűre. Belátható, hogy a kiterjesztett $\tilde{\varphi}$ leképezés homomorfizmus és képe izomorf a $\mathbb{Z}C_2$ csoportgyűrűvel. Ekkor azt kapjuk, hogy

$$\tilde{\varphi}(u) = \alpha_0 + \alpha_1 a^2 + \alpha_2 + \alpha_3 a^2 = (\alpha_0 + \alpha_2) + (\alpha_1 + \alpha_3) a^2$$

egység a $\mathbb{Z}C_2$ -ben. Mivel $\mathbb{Z}C_2$ -ben csak triviális egységek vannak, így két esetet kapunk:

1. $\alpha_0 + \alpha_2 = \pm 1, \alpha_1 + \alpha_3 = 0$ és $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = 1$;
2. $\alpha_0 + \alpha_2 = 0, \alpha_1 + \alpha_3 = \pm 1$ és $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = 1$.

Most vizsgáljuk meg az első esetet. Kifejezve az α_0 és α_1 tagokat és visszahelyettesítve azt kapjuk, hogy

$$u = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 = 1 - \alpha_2 - \alpha_3 a + \alpha_2 a^2 + \alpha_3 a^3 = 1 + (\alpha_2 + \alpha_3 a)(a^2 - 1).$$

Ennek inverze legyen $u^{-1} = 1 + (\beta_2 + \beta_3 a)(a^2 - 1)$ alakú. Ekkor

$$\begin{aligned} uu^{-1} &= 1 + (\alpha_2 + \beta_2 - 2\alpha_2\beta_2 + 2\alpha_3\beta_3)(a^2 - 1) + \\ &\quad + (\alpha_3 + \beta_3 - 2\alpha_2\beta_3 - 2\alpha_3\beta_2)(a^2 - 1)a = 1. \end{aligned}$$

Ez csak akkor teljesül ha

$$\begin{cases} (1 - 2\alpha_2)\beta_2 + 2\alpha_3\beta_3 = -\alpha_2 \\ -2\alpha_3\beta_2 + (1 - 2\alpha_2)\beta_3 = -\alpha_3. \end{cases} \quad (3.6)$$

A 3.6 egyenletrendszert megoldva

$$\beta_3 = \frac{(1 - 2\alpha_2)(-\alpha_3) - 2\alpha_2\alpha_3}{(1 - 2\alpha_2)^2 + 4\alpha_3^2} = \frac{-\alpha_3}{(1 - 2\alpha_2)^2 + 4\alpha_3^2}.$$

A kapott képlet $\mathbb{Z}$ feletti értékeket csak akkor vesz fel ha $\alpha_3 = \beta_3 = 0$. Ezeket visszahelyettesítve a 3.6 rendszerbe azt kapjuk, hogy $(1 - 2\alpha_2)\beta_2 = -\alpha_2$ melyből kifejezve a β_2 -t

$$\beta_2 = \frac{-\alpha_2}{1 - 2\alpha_2},$$

innen pedig α_2 vagy 1 vagy 0. Tehát az első eset teljesülésekor megkapjuk a 1 és a^2 elemeket.

Most vizsgáljuk meg a második esetet. Ekkor

$$u = -\alpha_2 + a - \alpha_3 a + \alpha_2 a^2 + \alpha_3 a^3 = a(1 + (\alpha_3 - \alpha_2 a)(a^2 - 1)).$$

Belátható, hogy a második esetben az előzővel szimmetrikus esetet kapunk melyben a diofantikus egyenletrendszerből azt kapjuk, hogy $\alpha_2 = 0$ és α_3 vagy 1 vagy 0. Így a második eset teljesülésekor megkapjuk a a és a^3 elemeket. Ezzel beláttuk, hogy az összes lehetséges egység triviális. ■

3.4. TÉTEL. *A $\mathbb{Z}C_6$ -nak csak triviális egységei vannak.*

Bizonyítás: Legyen $u = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 + \alpha_4 a^4 + \alpha_5 a^5$ a $\mathbb{Z}C_6$ csoportgyűrű normalizált egysége. Legyen φ olyan, hogy $\varphi(g) = g^3$ tetszőleges $g \in C_6$ elemre. Könnyen belátható, hogy φ a C_6 csoport C_2 csoportra képező csoport - homomorfizmus, és lineárisan kiterjesztve $\tilde{\varphi}$ a $\mathbb{Z}C_6$ csoportgyűrű $\mathbb{Z}C_2$ csoportgyűrűre képező gyűrű - homomorfizmus. Ekkor

$$\tilde{\varphi}(u) = \alpha_0 + \alpha_1 a^3 + \alpha_2 + \alpha_3 a^3 + \alpha_4 + \alpha_5 a^3 = (\alpha_0 + \alpha_2 + \alpha_4) + (\alpha_1 + \alpha_3 + \alpha_5) a^3$$

egység a $\mathbb{Z}C_2$ -ben. Az előző tételekből tudjuk, hogy $\mathbb{Z}C_2$ -ben csak triviális egységek vannak így két esetet kapunk:

1. $\alpha_0 + \alpha_2 + \alpha_4 = 1, \alpha_1 + \alpha_3 + \alpha_5 = 0$ és $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 1$;
2. $\alpha_0 + \alpha_2 + \alpha_4 = 0, \alpha_1 + \alpha_3 + \alpha_5 = 1$ és $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 1$.

Hasonlóképpen definiálhatunk egy $\lambda : C_6 \rightarrow C_3$ homomorfizmust, ahol $\lambda(g) = g^2$ tetszőleges $g \in C_6$ elemre. Ezt a homomorfizmust lineárisan kiterjesztve a $\tilde{\lambda} : \mathbb{Z}C_6 \rightarrow \mathbb{Z}C_3$ gyűrű - homomorfizmust kapjuk. Az előzőekhez hasonló módon

$$\tilde{\lambda}(u) = \alpha_0 + \alpha_1 a^2 + \alpha_2 a^4 + \alpha_3 + \alpha_4 a^2 + \alpha_5 a^4 = (\alpha_0 + \alpha_3) + (\alpha_1 + \alpha_4) a^2 + (\alpha_2 + \alpha_5) a^4$$

a $\mathbb{Z}C_3$ triviális egysége, így három esetet kapunk:

- a. $\alpha_0 + \alpha_3 = 1, \alpha_1 + \alpha_4 = 0, \alpha_2 + \alpha_5 = 0$;
- b. $\alpha_0 + \alpha_3 = 0, \alpha_1 + \alpha_4 = 1, \alpha_2 + \alpha_5 = 0$;
- c. $\alpha_0 + \alpha_3 = 0, \alpha_1 + \alpha_4 = 0, \alpha_2 + \alpha_5 = 1$.

Az 1. és az a. eset teljesülésekor

$$\begin{cases} \alpha_0 = 1 - \alpha_4 + \alpha_5 \\ \alpha_1 = -\alpha_4 \\ \alpha_2 = -\alpha_5 \\ \alpha_3 = \alpha_4 - \alpha_5. \end{cases} \quad (3.7)$$

Ezt visszahelyettesítve és a megfelelő algebrai átalakítások elvégzése után kapjuk, hogy

$$u = 1 + (\alpha_5 - \alpha_4 - \alpha_4 a - \alpha_5 a^2) (1 - a^3), \quad (3.8)$$

és legyen ennek inverze

$$u^{-1} = 1 + (\beta_5 - \beta_4 - \beta_4 a - \beta_5 a^2) (1 - a^3).$$

Ekkor

$$\begin{aligned} uu^{-1} = & 1 + (\alpha_5 - \alpha_4 + \beta_5 - \beta_4 - \alpha_4 a - \beta_4 a - \alpha_5 a^2 - \beta_5 a^2) (1 - a^3) + \\ & + (\alpha_5 \beta_5 - \alpha_5 \beta_4 - \alpha_5 \beta_4 a - \alpha_5 \beta_5 a^2 - \alpha_4 \beta_5 + \alpha_4 \beta_4 + \alpha_4 \beta_4 a + \alpha_4 \beta_5 a^2 - \alpha_4 \beta_5 a + \\ & + \alpha_4 \beta_4 a + \alpha_4 \beta_4 a^2 + \alpha_4 \beta_5 a^3 - \alpha_5 \beta_5 a^2 + \alpha_5 \beta_4 a^2 + \alpha_5 \beta_4 a^3 + \alpha_5 \beta_5 a^4) (1 - a^3)^2. \end{aligned}$$

Elvégezve a megfelelő algebrai átalakításokat, illetve összevonva az egynemű tagokat

$$\begin{aligned} uu^{-1} = & 1 + ((-1 + 2\alpha_4 - 4\alpha_5) \beta_4 + (1 - 4\alpha_4 + 2\alpha_5) \beta_5 - \alpha_4 + \alpha_5) + \\ & + ((-1 + 4\alpha_4 - 2\alpha_5) \beta_4 + (-2\alpha_4 - 2\alpha_5) \beta_5 - \alpha_4) a + \\ & + ((2\alpha_4 + 2\alpha_5) \beta_4 + (-1 + 2\alpha_4 - 4\alpha_5) \beta_5 - \alpha_5) a^2 = 1, \end{aligned}$$

és ebből pedig megkapjuk a

$$\begin{cases} (-1 + 2\alpha_4 - 4\alpha_5) \beta_4 + (1 - 4\alpha_4 + 2\alpha_5) \beta_5 = \alpha_4 - \alpha_5 \\ (-1 + 4\alpha_4 - 2\alpha_5) \beta_4 + (-2\alpha_4 - 2\alpha_5) \beta_5 = \alpha_4 \\ (2\alpha_4 + 2\alpha_5) \beta_4 + (-1 + 2\alpha_4 - 4\alpha_5) \beta_5 = \alpha_5 \end{cases}$$

diofantoszi egyenletrendszer. Könnyen látható, hogy az első egyenlet előáll a másik kettő lineáris kombinációjaként tehát a rendszer első egyenletét kivéve a

$$\begin{cases} (-1 + 4\alpha_4 - 2\alpha_5) \beta_4 + (-2\alpha_4 - 2\alpha_5) \beta_5 = \alpha_4 \\ (2\alpha_4 + 2\alpha_5) \beta_4 + (-1 + 2\alpha_4 - 4\alpha_5) \beta_5 = \alpha_5 \end{cases} \quad (3.9)$$

egyenletrendszert kapjuk. Az előző tételhez hasonló módon igazolható, hogy $\mathbb{Z}$ felett csak akkor van megoldása ha $\alpha_4 = \alpha_5 = 0$.

Ezzel megkaptuk a C_6 csoport egységelemét és az előző tételhez hasonlóan itt is igazolható, hogy a további 5 lehetséges eset az előbbivel szimmetrikus és belőlük megkapjuk az összes többi triviális egységet. Ezzel beláttuk, hogy az összes lehetséges egység triviális. ■

Megjegyezném, hogy ezen tételekhez hasonló módon bizonyítható:

3.5. TÉTEL. *Legyen G véges Abel csoport. Ha a G elemeinek rendje osztója 4-nek vagy 6-nak, akkor $\mathbb{Z}G$ egységei triviálisak.*

4. A CSOPORTGYŰRŰ CENTRUMA

Az előző fejezetben láthattuk, hogy vannak olyan csoportgyűrűk, amelyek csak triviális egységeket tartalmaznak. Ennek a fejezetnek a célja olyan módszer felépítése, amely segítségével előállíthatunk nem triviális egységeket.

Legyen G véges csoport a szorzásra nézve. A $g, h \in G$ elemeket felcserélhetőeknek mondjuk, ha $g \cdot h = h \cdot g$. A csoport minden elemével felcserélhető elemek

$$Z(G) = \{g \in G \mid \forall h \in G: gh = hg\} \quad (4.1)$$

halmazát a G csoport **centrumának** hívjuk.

Legyen $g, h \in G$ és jelölje $(g, h) = g^{-1}h^{-1}gh$ ezen elemek **kommutátorát**. A g és h elemek pontosan akkor felcserélhetőek, ha $(g, h) = 1$. A G összes kommutátora által generált

$$G' = \langle (g, h) \mid g, h \in G \rangle \quad (4.2)$$

részcsoporthat a G derivált csoportjának vagy **kommutátor részcsoporthatjának** nevezzük.

Legyen G véges csoport és $G/Z(G)$ rendje 4 ekkor két eset lehetséges:

1. $G/Z(G) \cong C_4 = \langle a \rangle$;
2. $G/Z(G) \cong C_2 \times C_2 = \langle a, b \rangle$.

Az első eset teljesülésekor

$$\forall g_1, g_2 \in G : g_1 = z_1 a^i \text{ és } g_2 = z_2 a^j$$

ahol $z_1, z_2 \in Z(G)$ és $i, j \in \{0, 1, 2, 3\}$. Azonnal látható, hogy

$$g_1 g_2 = z_1 a^i z_2 a^j = z_1 z_2 a^{i+j} = z_2 z_1 a^{i+j} = z_2 a^j z_1 a^i = g_2 g_1$$

ami ellentmondás. Ezzel beláttuk hogy az első eset lehetetlen.

Legyen G véges csoport és $G/Z(G) \cong C_2 \times C_2 = \langle a, b \rangle$. Ekkor tetszőleges $g \in G$ elemre $g^2 \in Z(G)$. Emiatt $a^2, b^2 \in Z(G)$ és

$$ab = zba, z \in Z(G).$$

Ezért a G csoport bármely eleme felírható x, ax, bx vagy abx alakban, ahol x a centrum eleme. A kommutátorok

$$(ax_1, bx_2) = a^{-1}x_1^{-1}b^{-1}x_2^{-1}ax_1bx_2 = (a, b) \text{ és}$$

$$(ax_1, abx_2) = a^{-1} (ab)^{-1} aab = a^{-1}b^{-1}a^{-1}a^2b = (a, b)$$

ezzel beláttuk, hogy csak egy nem triviális kommutátor létezik. Ebből azonnal arra juthatunk, hogy $G' = \{1, z\}$ és ennek következménye, hogy ha g és h a G tetszőleges elemei akkor $hg = gh$ vagy $hg = zgh$. Mivel G kommutátorai részcsoporthat alkotnak nyilvánvaló, hogy $z^2 = 1$.

Definiáljunk egy új involúciót, legyen $g \in G$ és

$$g^{\oplus} = \begin{cases} g, & \text{ha } g \text{ centrum elem} \\ gz, & \text{ha } g \text{ nem centrum elem} \end{cases} \quad (4.3)$$

illetve lineárisan kiterjesztve

$$u = \sum_{g \in G} \alpha_i g_i \rightarrow u^{\oplus} = \sum_{g \in G} \alpha_i g_i^{\oplus}.$$

4.1. LEMMA. *Legyen G véges csoport mely elemeinek rendje osztója 4-nek vagy 6-nak és $G/Z(G) \cong C_2 \times C_2$. Az $u \rightarrow u^{\oplus}$ leképezés involúció, és a következő tulajdonságokkal:*

$$1. \quad uu^{\oplus} = u^{\oplus}u$$

$$2. \quad uu^{\oplus} \text{ centrális elem és ha } u \text{ egység, akkor } (\pm G \text{ pontossággal}) uu^{\oplus} = 1$$

Bizonyítás: Legyen $G' = \langle z \rangle$. Jelölje $I(G') = (1 - z)\mathbb{Z}G$, amely nem más mint a $z - 1$ -el generált ideál. Az 1.3 tételből következik, hogy mivel G' normális részcsoporthat G -nek, akkor a G/G' faktorcsoporthat $\mathbb{Z}(G/G')$ csoportgyűrűje izomorf a $\mathbb{Z}G/I(G')$ faktorgyűrűvel. Nyilvánvaló, hogy G/G' -ben minden kommutátor triviális így G/G' kommutatív. Könnyen látható, hogy G/G' elemeinek rendje osztója 4-nek vagy 6-nak így a 3.5 tétel alapján minden egység a $\mathbb{Z}[G/G']$ csoportgyűrűben triviális. Nyilvánvaló, hogy ha

$$G = \bigcup_{x \in R_l(G/G')} xG',$$

akkor az $x + I(G')$ (ahol $x \in R_l(G/G')$) alakú elemek a $\mathbb{Z}G/I(G')$ faktorgyűrűben multiplikatív csoportot alkotnak, amely izomorf a G/G' faktorcsoporthat, és ezek az elemek a $\mathbb{Z}G/I(G')$ faktorgyűrűnek - mint baloldali $\mathbb{Z}$ -modulusnak - egy $\mathbb{Z}$ -bázisát alkotják. Mivel

$$u + I(G') = g + I(G'), \text{ esetén}$$

$$ug^{-1} + I(G') = 1 + I(G')$$

ezért az u egység felírható ($\pm G$ pontossággal)

$$u = 1 + (1 - z)\alpha,$$

alakban ahol α a $\mathbb{Z}G$ eleme. Hassunk az u -ra a $\oplus$ involúcióval ekkor belátható, hogy $uu^\oplus$ a centrum eleme és triviális azaz ($\pm G$ pontossággal) $uu^\oplus = 1$. ■

Most mindezek alapján képesek vagyunk olyan eljárást készíteni melyekkel nem triviális egységek hozhatóak létre. Legyen G olyan csoport mely a 4.1 lemma feltételeinek megfelelő, ekkor a csoportgyűrű tetszőleges u egységére ($\pm G$ pontossággal)

$$uu^\oplus = (1 + (1 - z)\alpha)(1 + (1 - z)\alpha^\oplus) = 1.$$

Mivel $(1 - z)^2 = 2(1 - z)$ ezért a megfelelő algebrai átalakítások és összevonások után azt kapjuk, hogy

$$1 + (1 - z)(\alpha + \alpha^\oplus + 2\alpha\alpha^\oplus) = 1.$$

Tehát u akkor és csakis akkor egység ha

$$(1 - z)(\alpha + \alpha^\oplus + 2\alpha\alpha^\oplus) = 0 \tag{4.4}$$

teljesül, így ennek segítségével ($\pm G$ pontossággal) meghatározhatók a csoportgyűrűbeli egységek.

5. PÉLDÁK

Legyen G olyan véges csoport melyben $|G/Z(G)| = 4$. Jelölje a és b a G csoport két egymástól különböző nem centrális elemét. Igazolható, hogy

$$G = Z(G) \cup aZ(G) \cup bZ(G) \cup abZ(G),$$

és az előző fejezet alapján tetszőleges $u \in \mathbb{Z}G$ egység előáll $1 + (1 - z)\alpha$ alakban, ahol $\alpha \in \mathbb{Z}G$. Legyen

$$Z(G) = \{z, z_1, z_2, \dots, z_n\},$$

akkor

$$\begin{aligned} \alpha &= (\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + (\alpha_4 + \alpha_5 a + \alpha_6 b + \alpha_7 ab) z_1 + \\ &+ (\alpha_8 + \alpha_9 a + \alpha_{10} b + \alpha_{11} ab) z_2 + \dots = (\alpha_0 + \alpha_4 z_1 + \alpha_8 z_2 + \dots) + \\ &+ (\alpha_1 + \alpha_5 z_1 + \alpha_9 z_2 + \dots) a + (\alpha_2 + \alpha_6 z_1 + \alpha_{10} z_2 + \dots) b + \\ &+ (\alpha_3 + \alpha_7 z_1 + \alpha_{11} z_2 + \dots) ab. \end{aligned} \quad (5.1)$$

A könnyebb átláthatóság érdekében jelölje

$$\{x_i = \alpha_i + \alpha_{i+4} z_1 + \dots + \alpha_{i+4n} z_n\} \in Z(\mathbb{Z}G). \quad (5.2)$$

Az 5.1 és a 5.2 képletekből kapjuk, hogy $u = 1 + (1 - z)(x_0 + x_1 a + x_2 b + x_3 ab)$. Az előző fejezetben ismertettet módszer alapján $u^\oplus = 1 + (1 - z)(x_0 - x_1 a - x_2 b - x_3 ab)$ és mivel $(1 - z)^2 = 2(1 - z)$, illetve $ba = abz$ ezért

$$uu^\oplus = 1 + (1 - z)(2x_0 + 2x_0^2 - 2(x_1 a)^2 - 2(x_2 b)^2 - 2(x_3 ab)^2). \quad (5.3)$$

Könnyedén igazolható, hogy

$$x_i^2 = \alpha_i^2 + 2\alpha_i \alpha_{i+4} z_1 + \alpha_{i+4}^2 z_1^2 + 2\alpha_i \alpha_{i+8} z_2 + 2\alpha_{i+4} \alpha_{i+8} z_1 z_2 + \alpha_{i+8}^2 z_2^2 + \dots \quad (5.4)$$

Most mindezek segítségével az előző fejezetbe leírt módszer használata sokkal egyszerűbbé válik.

5.1. 8-ad rendű csoportok egész számok feletti csoportgyűrűinek egységei

Legyen $|G| = 8$ és $|G/Z(G)| = 4$, ekkor

$$\begin{aligned} uu^\oplus &= 1 + (1 - z)(2\alpha_0 + 2\alpha_0^2 - 2(\alpha_1 a)^2 - 2(\alpha_2 b)^2 - 2(\alpha_3 ab)^2) = \\ &= 1 + 2(1 - a^2)(\alpha_0 + \alpha_0^2 + \alpha_1^2 - (\alpha_2^2 + \alpha_3^2) b^2). \end{aligned} \quad (5.5)$$

Mivel a^2 és b^2 centrálisak és $a^2 = b^2 = 1$ nem lehetséges, így közülük az egyik biztosan z és (izomorfia erejéig) feltételezhetjük, hogy $z = a^2$. Mindezekből $uu^\oplus = 1$ ha

$$(1 - a^2) (\alpha_0 + \alpha_0^2 + \alpha_1^2 - (\alpha_2^2 + \alpha_3^2) b^2) = 0.$$

Mivel b^2 centrális, így két eset lehetséges:

- $b^2 = 1$ esetén 8-ad rendű diéder csoportot kapunk és az egységeket meghatározó diofantoszi egyenletünk $\alpha_0 + \alpha_0^2 + \alpha_1^2 - \alpha_2^2 - \alpha_3^2 = 0$;
- $b^2 = z$ esetén 8-ad rendű kvaternió csoportot kapunk és a diofantoszi egyenletünk $\alpha_0 + \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0$. A megfelelő algebrai átalakítások után az egyenlet $(1 + 2\alpha_0)^2 + (2\alpha_0)^2 + (2\alpha_1)^2 + (2\alpha_2)^2 + (2\alpha_3)^2 = 1$ alakú melyből következik, hogy ebben a csoportban csak triviális egységek vannak.

5.2. 16-od rendű csoportok egész számok feletti csoportgyűrűinek egységei

Munkám utolsó részében olyan 16-od rendű csoportokat mutatok be melyek a módszerünk használati feltételeinek eleget tesznek. A módszer használatát a következő négy csoporton szemléltetem:

1. $\langle a, b, c | a^2 = b^2 = (ab)^2 = c^2, c^4 = (a, c) = (b, c) = 1 \rangle$,
2. $\langle a, b | a^4 = b^4 = 1, ba = a^3b \rangle$,
3. $\langle a, b | a^4 = b^4 = (ab)^2 = (a^2, b) = 1, \rangle$,
4. $\langle a, b | a^8 = (ab)^2 = 1, b^2 = a^2 \rangle$.

1. Legyen $G = \langle a, b, c | a^2 = b^2 = (ab)^2 = c^2, c^4 = (a, c) = (b, c) = 1 \rangle$. Könnyedén igazolható, hogy $z = (a, b) = (ab)^2 = c^2$ és $z_1 = c$.

A 5.4 képlet alapján $x_i^2 = \alpha_i^2 + 2\alpha_i\alpha_{i+4}c + \alpha_{i+4}^2c^2$ és a 5.3 képlet alapján

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - c^2) (x_0 + x_0^2 - (x_1a)^2 - (x_2b)^2 - (x_3ab)^2) = \\ &= 1 + 2(1 - c^2) (x_0 + x_0^2 + x_1^2 + x_2^2 + x_3^2). \end{aligned} \quad (5.6)$$

Az eredeti jelölésekhez visszatérve és a megfelelő algebrai átalakítások elvégzése után

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - c^2) (\alpha_0 + \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_4^2 - \alpha_5^2 - \alpha_6^2 - \alpha_7^2) + \\ &+ 2c(1 - c^2) (\alpha_4 + 2\alpha_0\alpha_4 + 2\alpha_1\alpha_5 + 2\alpha_2\alpha_6 + 2\alpha_3\alpha_7). \end{aligned}$$

Innen kapjuk az

$$\begin{cases} \alpha_0 + \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_4^2 - \alpha_5^2 - \alpha_6^2 - \alpha_7^2 = 0 \\ \alpha_4 + 2\alpha_0\alpha_4 + 2\alpha_1\alpha_5 + 2\alpha_2\alpha_6 + 2\alpha_3\alpha_7 = 0 \end{cases} \quad (5.7)$$

diofantoszi egyenletrendszer, amely megadja az egységeket ($\pm G$ pontossággal).

2. Legyen $G = \langle a, b | a^4 = b^4 = 1, ba = a^3b \rangle$. Az előzőhöz hasonlóan itt is igazolható, hogy $z = (a, b) = a^2$ és $z_1 = b^2$. A 5.3 és a 5.4 képletek alapján $x_i^2 = \alpha_i^2 + 2\alpha_i\alpha_{i+4}b^2 + \alpha_{i+4}^2$ és

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - a^2)(x_0 + x_0^2 + x_1^2 - x_2^2b^2 - x_3^2b^2) = \\ &= 1 + 2(1 - a^2)(x_0 + x_0^2 + x_1^2 - (x_2^2 + x_3^2)b^2). \end{aligned}$$

Az eredeti jelölésekhez visszatérve és a megfelelő algebrai átalakítások elvégzése után

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - a^2)(\alpha_0 + \alpha_0^2 + \alpha_4^2 + \alpha_1^2 + \alpha_5^2 - 2\alpha_2\alpha_6 - 2\alpha_3\alpha_7) + \\ &+ 2b^2(1 - a^2)(\alpha_4 + 2\alpha_0\alpha_4 + 2\alpha_1\alpha_5 - \alpha_2^2 - \alpha_6^2 - \alpha_3^2 - \alpha_7^2). \end{aligned}$$

Ebből megkapjuk a

$$\begin{cases} 2\alpha_0 + 2\alpha_0^2 + 2\alpha_4^2 + 2\alpha_1^2 + 2\alpha_5^2 - 4\alpha_2\alpha_6 - 4\alpha_3\alpha_7 = 0 \\ 2\alpha_4 + 4\alpha_0\alpha_4 + 4\alpha_1\alpha_5 - 2\alpha_2^2 - 2\alpha_6^2 - 2\alpha_3^2 - 2\alpha_7^2 = 0 \end{cases} \quad (5.8)$$

diofantoszi egyenletrendszer. A rendszer egyenleteit egymásból kivonva a

$$2(\alpha_0 - \alpha_4) + 2(\alpha_0 - \alpha_4)^2 + 2(\alpha_1 - \alpha_5)^2 + 2(\alpha_2 - \alpha_6)^2 + 2(\alpha_3 - \alpha_7)^2 = 0$$

egyenlethez jutunk. Ezt 2-vel szorozva és egyet hozzáadva mindkét oldalához a megfelelő algebrai átalakítások után az

$$(1 + 2(\alpha_0 - \alpha_4))^2 + (2(\alpha_1 - \alpha_5))^2 + (2(\alpha_2 - \alpha_6))^2 + (2(\alpha_3 - \alpha_7))^2 = 1$$

egyenletet kapjuk, melynek megoldása

$$\begin{cases} \alpha_1 = \alpha_5, \alpha_2 = \alpha_6, \alpha_3 = \alpha_7 \\ 1 + 2(\alpha_0 - \alpha_4) = \pm 1. \end{cases} \quad (5.9)$$

Két esetet tárgyalunk

$$\text{I. } \alpha_0 = \alpha_4, \alpha_1 = \alpha_5, \alpha_2 = \alpha_6, \alpha_3 = \alpha_7,$$

$$\text{II. } \alpha_0 = \alpha_4 - 1, \alpha_1 = \alpha_5, \alpha_2 = \alpha_6, \alpha_3 = \alpha_7.$$

Az I. esetben

$$u = 1 + (1 - a^2) (1 + b^2) (\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab),$$

ekkor újra elvégezve a konjugálttal való szorzást arra juthatunk, hogy $uu^\oplus = 1$ ha

$$2\alpha_0 + 4\alpha_0^2 + 4\alpha_1^2 - 4\alpha_2^2 - 4\alpha_3^2 = 0.$$

Az egyenlet mindkét oldalához $1 + 2\alpha_0$ -t adva és a megfelelő algebrai átalakítások után megkapjuk az

$$(1 + 2\alpha_0)^2 + (2\alpha_1)^2 - (2\alpha_2)^2 - (2\alpha_3)^2 = 1 + 2\alpha_0$$

alakú diofantoszi egyenletet.

A II. eset teljesülésekor azt kapjuk, hogy

$$\begin{aligned} u &= 1 + (1 - z) (1 + b^2) (\alpha_4 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) - (1 - z) = \\ &= z + (1 - z) (1 + b^2) (\alpha_4 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) = zv \end{aligned}$$

ahol v egység az I. eset szerint.

3. Legyen $G = \langle a, b | a^4 = b^4 = (ab)^2 = (a^2, b) = 1, \rangle$. Ebben az esetben

$$z = (a, b) = a^{-1}b^{-1}ab = baab = a^2b^2$$

és $z_1 = a^2$. A 5.3 és a 5.4 képletek alapján $x_i^2 = \alpha_i^2 + 2\alpha_i\alpha_{i+4}a^2 + \alpha_{i+4}$ és

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - a^2b^2) (x_0 + x_0^2 - x_1^2a^2 - x_2^2b^2 - x_3^2(ab)^2) = \\ &= 1 + 2(1 - a^2b^2) (x_0 + x_0^2 - x_1^2a^2 + x_2^2a^2 - x_3^2). \end{aligned} \quad (5.10)$$

Az eredeti jelölésekhez visszatérve és a megfelelő algebrai átalakítások elvégzése után

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - a^2b^2) (\alpha_0 + \alpha_0^2 + \alpha_4^2 - 2\alpha_1\alpha_5 + 2\alpha_2\alpha_6 - \alpha_3^2 - \alpha_7^2) + \\ &+ 2a^2(1 - a^2b^2) (\alpha_4 + 2\alpha_0\alpha_4 - \alpha_1^2 - \alpha_5^2 + \alpha_2^2 + \alpha_6^2 - 2\alpha_3\alpha_7) = 0. \end{aligned}$$

alakú és ebből megkapjuk az

$$\begin{cases} \alpha_0 + \alpha_0^2 + \alpha_4^2 - 2\alpha_1\alpha_5 + 2\alpha_2\alpha_6 - \alpha_3^2 - \alpha_7^2 = 0 \\ \alpha_4 + 2\alpha_0\alpha_4 - \alpha_1^2 - \alpha_5^2 + \alpha_2^2 + \alpha_6^2 - 2\alpha_3\alpha_7 = 0 \end{cases} \quad (5.11)$$

diofantoszi egyenletrendszer.

4. Legyen $G = \langle a, b | a^8 = (ab)^2 = 1, b^2 = a^2 \rangle$. A nem triviális kommutátor

$$z = (a, b) = a^{-1}b^{-1}ab = baab = a^2b^2 = a^4$$

és könnyen belátható, hogy $z_1 = a^2$.

Az előző példákhoz hasonlóan $x_i^2 = \alpha_i^2 + 2\alpha_i\alpha_{i+4}a^2 + \alpha_{i+4}^2a^4$ és

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - a^4)(x_0 + x_0^2 - x_1^2a^2 - x_2^2b^2 - x_3^2(ab)^2) = \\ &= 1 + 2(1 - a^4)(x_0 + x_0^2 - x_1^2a^2 - x_2^2a^2 - x_3^2). \end{aligned}$$

Az eredeti jelölésekhez visszatérve és a megfelelő algebrai átalakítások után

$$\begin{aligned} uu^\oplus &= 1 + 2(1 - a^4)(\alpha_0 + \alpha_0^2 - \alpha_4^2 + 2\alpha_1\alpha_5 + 2\alpha_2\alpha_6 - \alpha_3^2 + \alpha_7^2) + \\ &\quad + 2a^2(1 - a^4)(\alpha_4 + 2\alpha_0\alpha_4 - \alpha_1^2 + \alpha_5^2 - \alpha_2^2 + \alpha_6^2 - 2\alpha_3\alpha_7) \end{aligned}$$

alakú és ebből megkapjuk a

$$\begin{cases} \alpha_0 + \alpha_0^2 - \alpha_4^2 + 2\alpha_1\alpha_5 + 2\alpha_2\alpha_6 - \alpha_3^2 + \alpha_7^2 = 0 \\ \alpha_4 + 2\alpha_0\alpha_4 - \alpha_1^2 + \alpha_5^2 - \alpha_2^2 + \alpha_6^2 - 2\alpha_3\alpha_7 = 0 \end{cases} \quad (5.12)$$

diofantoszi egyenletrendszer.

Ezzel együtt sikeresen meghatároztuk mindazon diofantoszi egyenleteket melyek segítségével megállapíthatjuk az adott csoportgyűrűbeli elem invertálhatóságát.

ÖSSZEFOGLALÁS

A $\mathbb{Z}G$ csoportgyűrű invertálható elemeit egységeknek nevezzük. A csoportgyűrű összes egysége csoportot alkot, amelyet csoportgyűrű egységcsoportjának nevezünk, és rá az $U(\mathbb{Z}G)$ jelölést használjuk. Az $U(\mathbb{Z})G = \{kg \mid k \in U(\mathbb{Z}), g \in G\}$ halmaz elemei a $\mathbb{Z}G$ csoportgyűrű egységei melyeket triviális egységeknek nevezzük.

Munkám során kiderült, hogy a csoportgyűrűk egységeinek meghatározása nagyon bonyolult feladat, mivel az egész számok feletti csoportgyűrűkben egy elem nem csak attól lesz invertálhatatlan, hogy nullosztó hanem attól is, hogy az egész számok halmaza nem test azaz nem tartalmazza minden elemének inverzét. Ezáltal szinte minden probléma diofantoszi egyenletek, illetve nagyobb csoportok esetén diofantoszi egyenletrendszerek megoldását igényli mely egy nagyon nehéz és nagy odafigyelést igénylő feladat.

Munkám során sikeresen igazoltam, hogy $\mathbb{Z}C_2$, $\mathbb{Z}C_3$, $\mathbb{Z}C_4$, $\mathbb{Z}C_6$ és $\mathbb{Z}Q_8$ csoportgyűrűk csak triviális egységeket tartalmaznak. Rengeteg számítást tett egyszerűbbé a normalizált egységcsoport

$$V(\mathbb{Z}G) = \left\{ u = \sum_{g \in G} u_g g \in U(\mathbb{Z}G) \mid \sum_{g \in G} u_g = 1 \right\}$$

használata és az a tény, hogy az egész számok feletti csoportgyűrűkben ha a normalizált egységcsoport csak triviális egységeket tartalmaz akkor maga az egységcsoport is. Munkámban bemutattam egy olyan eljárást mely segítségével a megfelelő feltételeknek eleget tevő csoportok egész számok feletti csoportgyűrűiben meghatározhatók a nem triviális egységek, illetve sikeresen alkalmaztam nem triviális egységek meghatározására.

Hivatkozások

- [1] **Bódi Béla:** *A csoportelmélet alapjai*, Kossuth Egyetemi Kiadó, Debrecen, 1999
- [2] **Bódi Béla:** *A gyűrűelmélet alapjai*, Kossuth Egyetemi Kiadó, Debrecen, 2006
- [3] **Bódi Béla:** *Bevezetés a csoportgyűrűk elméletébe*, KLTE, Debrecen, 1996
- [4] **Bódi Béla:** *Unitarity of the Units group of group algebra*, 1992
- [5] **E.G. Goodaire, E. Jespers, M. M. Parmenter:** *Determining Units in Some Integral Group Rings*, Memorial University of Newfoundland, St. John's, Canada
- [6] **G. Higman:** *The units of group rings*, *Proceedings of the London Mathematical Society*, (2) 46: 231 - 248, 1940
- [7] **S.K. Sehgal:** *Topics in Group Rings*, Marcel Dekker, New York, 1978