Eötvös Loránd Tudományegyetem
Természettudományi Kar

Csoportok a matematika különböző területein

Szakdolgozat

Harkai Alexandra Dóra
Matematika B.Sc., Matematikai elemző szakirány

Témavezető: **Károlyi Gyula**, egyetemi docens
Algebra és Számelmélet Tanszék

Budapest
2010

Tartalomjegyzék

Bevezetés

> *„A csoportelmélet a matematika azon ága, amely megválaszolja azt a kérdést, hogy 'Mi a szimmetria?' ”* – Nathan C. Carter

Nem csak a matematikában, hanem a fizika, a kémia, sőt a művészetek különféle területein is találkozhatunk csoportokkal. Megjelennek a relativitáselméletben, kristályszerkezetek leírásakor, a sík vagy a tér „csempékkel” történő kirakásánál, a Rubik-kocka mozgatásai is kifejezhetők a csoportok nyelvén, sőt a zenében a kvintkör is egy ciklikus csoporttal írható le [6]. A csoportelmélet segítségével feltárható egy halmaz működése, felépítése és megérthetjük a bennük rejlő rendszert, szabályosságokat.

A csoportok tanulmányozása alapvető fontosságú az absztrakt algebrában, ugyanis a különböző algebrai struktúrák (gyűrűk, testek, vektorterek) tulajdonképpen maguk is mind alapvetően csoportok, a további műveleti sajátosságok különböztetik meg őket, ezek jelentik azokat a plusz tulajdonságokat, amelyek külön érdekessé és nem utolsó sorban hasznossá teszik őket.

Már az elsőéves algebrában és számelméletben is találkozunk olyan tételekkel, melyek csoport- és gyűrűelméleti háttérrel rendelkeznek. Ilyenek az Euler-Fermat-tétel, a Lagrange-tétel, valamint modulo p primitív gyök létezése, ami annak speciális esete, hogy minden véges test multiplikatív csoportja ciklikus. A kriptográfiában alkalmazott diszkrét logaritumus pedig úgy is megfogalmazható, hogy a modulo p maradékosztályok a szorzásra nézve ciklikus csoportot alkotnak.

Dolgozatomban kifejezetten maguknak a csoportoknak a hasznosságára, széles körű alkalmazásaira szeretnék rávilágítani néhány konkrét példa segítségével. Megoldásukon keresztül mélyebben bemutatom, hogyan jelennek meg a csoportok a matematika legkülönbözőbb területein és segítenek megérteni, átlátni a problémák felépítését, működését.

Az első fejezetben bemutatom azokat a csoportelméleti fogalmakat, melyeket a későbbiek során fel fogok használni, illetve melyeknek ismerete alapvető fontosságú

a továbbiak megértéséhez. Az itt részletezett tételek és definíciók nagyrészt Szabó Endre, Pelikán József, Ágoston István, Pálfy Péter Pál, Károlyi Gyula és Szabó Csaba óráin hangzottak el.

A második fejezetben a nevezetes Pell-egyenletek megoldásain keresztül ismertetem az ideálok és az egységcsoport egy alkalmazását, a harmadik fejezet a Cayley-gráfok tulajdonságait felhasználva egy mélyebb absztrakt algebrai tétel következményeit mutatja be. A negyedik fejezetben egy, az elliptikus görbéken értelmezett csoport tulajdonságaival foglalkozom.

A dolgozatban felhasznált ábrák a Wikipedia szabadon felhasználható képei közül és a Wolfram MathWorld oldaláról származnak, az általam rajzolt ábrákat pedig a KmPlot nyílt forráskódú programmal készítettem.

1. fejezet

Csoportelméleti bevezető

Számos algebrai, illetve leginkább speciálisan csoportelméleti ismeretre fogok építeni a dolgozatban, ezért a bevezető fejezetben ősszefoglalom azokat a fogalmakat, amiket a későbbiek során felhasználok. Ezek döntő többségben szigorúan csoportelméleti tételek és definíciók, melyek ugyan mind menynyiségükben, mind mélységükben csak kis részét képezik a csoportelméleti alapismereteknek [15], azonban a bemutatott problémák már így is megoldhatóak lesznek. Mivel a példák a matematika különböző területeiről származnak, egy kevés gyűrűelméleti, geometriai ismeretre is szükség lesz.
A legfontosabbak természetesen maga a csoport a fogalma, valamint a hozzá szorosan kapcsolódó definíciók lesznek:

1. Definíció. *[csoport] Csoportnak nevezünk egy olyan nemüres G halmazt, amelyen értelmezve van egy bináris művelet $(\cdot)$ a következő tulajdonságokkal:*

- *bármely két $a, b \in G$ esetén $ab \in G$ (műveleti zártság)*
- *minden $a, b, c \in G$ elemekre $(ab)c=a(bc)$ (a művelet asszociatív)*
- *egyértelműen létezik egy kitüntetett $e \in G$ elem, amelyre igaz, hogy $\forall\ a \in G$ elemre $ea = a = ae$ (kétoldali egységelem létezése)*
- *$\forall\ a \in G$ elemhez egyértelműen létezik egy $b = a^{-1}$ elem, amelyre igaz, hogy $aa^{-1} = e = a^{-1}a$, ahol e a csoport fent definiált egységeleme (kétoldali inverz létezése)*

2. Definíció. *[rend] Egy G csoport $|G|$ rendje a csoport elemeinek száma, egy $g \in G$ elem rendje pedig az a legkisebb $n \in \mathbb{N}$, amelyre $g^n = e$.*

3. Definíció. *[Abel-csoport] Egy G csoport Abel-csoport, ha kommutatív, vagyis $\forall\ a, b \in G$ esetén $ab = ba$.*

Egy csoportnak nevezetes részhalmazai lehetnek, külön fontosak azok, amelyek „öröklik" az eredeti csoport struktúráját, esetleg következtetni lehet belőlük az egész csoport szerkezetére.

4. Definíció. *[komplexus] Komplexusnak nevezzük egy csoport részhalmazait. A komplexusokon definiálunk egy szorzást a következőképpen: $K^{-1} = \{k^{-1} \mid k \in K\}$, valamint $K_1K_2 = \{k_1k_2 \mid k_1 \in K_1, k_2 \in K_2\}$.*
Komplexusokat elemmel is szorozhatunk, ez egyelmű komplexussal való szorzást jelent: $gK = \{g\}K = \{gk \mid g \in G, k \in K\}$. (Hasonlóan definiálható Kg is.)

5. Definíció. *[részcsoport] Egy G csoportnak részcsoportja $\emptyset \neq H \subset G$, ha ugyanarra a csoportműveletre és az inverzképzésre nézve is zárt, ezt $H < G$-vel jelöljük.*

1. Példa. *[részcsoport] Az egész számok $(\mathbb{Z}, +)$ csoportjában részcsoportot alkotnak a k nemnulla egésszel osztható számok.*

6. Definíció. *[generátor] Egy $S \subset G$ részhalmaz által generált $\langle S \rangle$ csoport az a legszűkebb részcsoportja G-nek, amely tartalmazza S-t. Egy G csoport generátora az az $S \subset G$ halmaz, melyre $\langle S \rangle = G$, ahol $\langle S \rangle$ jelöli a generátorelemek és inverzeik kombinációiból előállítható elemek halmazát.*

7. Definíció. *[végesen generált Abel-csoport] Egy $(G, +)$ Abel-csoport végesen generált, ha létezik véges számú $g_1, \ldots, g_s \in G$, melyeksegítségével $\forall g \in G$ elem egyértelműen felírható*

$$\forall g \in G : g = n_1g_1 + \ldots + n_sg_s$$

alakban, ahol $n_1, \ldots, n_s \in \mathbb{Z}$. Ekkor $\{g_1, \ldots, g_s\}$ a G csoport egy generátorhalmaza.

Könnyen látható, hogy minden véges Abel-csoport végesen generált, de fordítva nem igaz.

8. Definíció. *[ciklikus csoport] Ciklikusnak nevezzük azokat a csoportokat, melyek egy elemmel generálhatók.*

2. Példa. *[ciklikus csoport] Az egész számok $(\mathbb{Z}, +)$ csoportja, valamint m egészekre $a \pmod m$ maradékosztályok csoportjai.*

9. Definíció. *[szabad csoport] Szabad csoportnak nevezünk egy G csoportot, ha létezik olyan S generátora, hogy a generátorelemek és inverzeik szozataként G minden eleme pontosan egyféleképpen írható fel.*

10. Definíció. *[mellékosztály] Egy $H < G$ részcsoport mellékosztályai G-ben azok a komplexusok, melyeket a G-beli g elemekkel való szorzással kapunk: gH és Hg a H részcsoport g szerinti bal-, illetve jobboldali mellékosztálya.*

11. Definíció. *[normálosztó] A G csoport egy N részcsoportja normálosztó ($N \triangleleft G$), ha $\forall g \in G$-re teljesül, hogy $gN = Ng$. A G csoport egy N normálosztóját normális részcsoportnak is szokás nevezni.*

3. Példa. *[normálosztó] A D_n diédercsoportokban normálosztókat alkotnak az irányítástartó transzformációk részcsoportjai.*

12. Definíció. *[direkt összeg] A G Abel-csoport a $G_1, \ldots, G_n$ részcsoportjainak direkt összege azt a G , ha G minden eleme egyértelműen felírható a G_i csoportok elemeinek szorzataként $g_1, \ldots, g_n$ alakban, ahol $g_i \in G_i$. (Nem kommutatív esetben a G_i részcsoportoknak normális részcsoportok kell lenniük.)*

4. Példa. *[direkt összeg] A C_{12} ciklikus csoport felbontható két csoport direkt összegére: $C_{12} \cong C_3 \bigoplus C_4$.*

13. Definíció. *[faktorcsoport] Egy G csoport N normálosztójának mellékosztályaiból alkotott csoport a $(gN)(hN) = (gh)n$ műveletre nézve, amit G/N-nel jelölünk.*

Bizonyos csoportok struktúrái között lehet hasonlóság:

14. Definíció. *[homomorfizmus] Homomorfizmus egy olyan $\varphi : G \to H$ leképezés, amely művelettartó, vagyis minden $\forall a, b \in G$ elemre $\varphi(a) \cdot \varphi(b) = \varphi(ab)$.*

15. Definíció. *[izomorfizmus] Egy φ homomorfizmus izomorfizmus, ha bijektív. Ekkor létezik hozzá egy $\varphi^{-1} = \psi$ inverz homomorfizmus: $\varphi(\psi(a)) = a = \psi(\varphi(a))$.*

5. Példa. *[homomorfizmus, izomorfizmus] A nemnegatív számok $(\mathbb{R}, \cdot)$ csoportja izomorf a valós számok $(\mathbb{R}, +)$ csoportjával, az izomorfizmus pedig a logaritmálás: $\ln ab = \ln a + \ln b$.*

16. Definíció. *[automorfizmus] Egy csoport önmagára való izomorfizmusát automorfizmusnak nevezzük.*

17. Definíció. *[gráfizomorfizmus] $G_1 = (V_1, E_1)$ és $G_1 = (V_1, E_1)$ gráfokra a bijektív $\phi : V_1 \to V_2$ leképezés gráfizomorfizmus, ha megőrzi a szomszédsági relációt, vagyis $\forall\{u, v\} \in E_1 \iff \{\phi(u), \phi(v)\} \in E_2$.*

18. Definíció. *[gráfautomorfizmus] Egy gráf önmagára való izomorfizmusa gráfautomorfizmus.*

A csoportokhoz hasonló struktúrákkal is fogunk dolgozni:

19. Definíció. *[félcsoport] A félcsoport egy olyan nemüres halmaz, amelyen definiálva van egy asszociatív, kétváltozós művelet, vagyis: $\forall a, b \in G$ esetén $ab \in G$ és $(ab)c = a(bc)$.*

20. Definíció. *[gyűrű] Egy $(R, +, \cdot)$ struktúrát gyűrűnek nevezünk, ha $(R, +)$ Abel-csoport, $(R, \cdot)$ pedig félcsoport, valamint ha a szorzás disztributív az összeadásra nézve, azaz $a, b, c \in R$ elemekre $a(b + c) = ab + ac$ és $(a + b)c = ac + bc$. Az R kommutatív, ha $(R, \cdot)$ kommutatív.*

21. Definíció. *[ideál] Az $(R, +, \cdot)$ kommutatív gyűrű $I \subset R$ részhalmaza ideál, ha:*

- $(I, +) < (R, +)$
- $\forall i \in I, \forall r \in R$ *esetén* $ri \in I$

6. Példa. *[ideál] Az egész számok gyűrűjében a k nemnulla egésszel osztható számok ideált alkotnak.*

22. Definíció. *[test] Az R gyűrű test, ha kommutatív és $(R, \cdot)$ csoport.*

23. Definíció. *[testbővítés] Ha K részteste a L testnek, akkor L-t K bővítésének nevezzük, $K < L$ pedig egy testbővítés, amit $L \mid K$-val is jelölünk.*

7. Példa. *[testbővítés] Egy test véges bővítése a $\mathbb{Q}$ számtest egy n-edfokú α algebrai számmal való bővítése, $\mathbb{Q}(\alpha) = \{r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1} \mid r_i \in \mathbb{Q}\}$.*

24. Definíció. *[algebrai egész(1)] Egy K számtestben $\alpha \in K$ algebrai egész, ha létezik olyan 1 főegyüttható̊ju $f(x) \in \mathbb{Z}[x]$ polinom, melynek gyöke, vagyis $f(\alpha) = 0$.*

25. Definíció. *[algebrai egész(2)] Egy K számtestben $\alpha \in K$ algebrai egész, ha az 1 főegyüttható̊ju, $\mathbb{Q}$ fölötti minimálpolinomja $\mathbb{Z}[x]$-ben van.*

26. Definíció. *[monomorfizmus] Egy injektív homomorfizmust monomorfizmusnak nevezünk.*

Legyen K egy n-fokú algebrai számtest és legyenek $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ a $\mathbb{Q}$-monomorfizmusok.

27. Definíció. *[konjugált] $\alpha \in K$ szám konjugáltjai a $\sigma_i(\alpha)$ számok.*

8. Példa. *[bővítés] Ha α nem valós, másodfokú algebrai szám, akkor a $\mathbb{Q}(\alpha)$ bővítés komplex számokat ad.*

28. Definíció. *[algebrai számtest] Algebrai számtestnek nevezzük $\mathbb{C}$nek egy K résztestét, amely $\mathbb{Q}$-nak véges fokú bővítése.*

29. Definíció. *[egyszerű bővítés] Egy K test egy elemmel való bővítését egyszerű bővítésének nevezzük.*

30. Definíció. *[bővítés foka] Egy K fölötti L bővítés foka a K fölötti L vektortér n dimenziója, ezt $[L : K] = n$-nel jelöljük.*

1. Tétel. *[végesen generált Abel-csoportok alaptétele] [22, 25]*

- *Minden végesen generált Abel-csoport izomorf ciklikus prímhatványrendű csoportok és végtelen ciklikus csoportok direkt összegével. Vagyis minden ilyen G csoportra:*

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_t}$$

  ahol az $n, q_1, \cdots, q_t$ számok értékei a sorrendtől eltekintve egyértelműen meghatározottak és a $q_1, \cdots, q_t$ számok (nem feltétlenül különböző) prímek hatványai.

- *Minden végesen generált G Abel-csoportra:*

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_u}$$

  ahol a $k_i | k_{i+1}$ ($\forall i = 1, \cdots, u-1$-re). Itt n és $k_1, \cdots, k_u$ értékei és sorrendje is G által egyértelműen meghatározottak.

2. fejezet

A Pell-egyenletek és az egységcsoport

Néhány egyszerűbb példa, ami először eszünkbe juthat, amikor az említett algebrai stuktúrákról beszélünk:

- félcsoportok: $(\mathbb{N}, +), (\mathbb{Z}, \cdot), (\mathbb{Z}^{n\times n}, \cdot)$
- csoportok: $(\mathbb{Z}, +), (\mathbb{Z}^n, +), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot), (\mathbb{H}, \cdot)$, $(A \in \mathbb{R}^{n\times n} \mid \det(A) \neq 0, \cdot)$
- gyűrűk: $(\mathbb{Z}, +, \cdot), (\mathbb{H}, +, \cdot), (\mathbb{Z}^{n\times n}, +, \cdot), (\mathbb{R}^{n\times n}, +, \cdot)$

Most egy hasonlóan egyszerű struktúra segítségével fogjuk megmutatni, hogy menynyire jól használhatók az absztrakt algebrai módszerek jelen esetben egy nevezetes probléma, nevezetesen a Pell-egyenletek megoldására.

2.1. A Pell-egyenlet

A „Pell-egyenlet" elnevezés Leonhard Eulertől származik, aki Lord Brouncker munkáját tanulmányozta a nevezetes diophantoszi egyenletről, de véletlenül összekeverte Brouncker és John Pell nevét.

Már az ókori görögöket és indiaiakat is érdekelték a Pell-egyenletek, különösen az $x^2 - 2y^2 = 1$ alakú, ugyanis ennek megoldásai nagyon szoros kapcsolatban vannak a $\sqrt{2}$ racionális közelítésével. Ha az egyenlet egy megoldása x és y, akkor $\frac{x}{y}$ nagyon jó racionális közelítése lesz $\sqrt{2}$-nek. Diophantoszról kapták a nevüket azok a

többváltozós polinomiális egyenletek, melyekben csak egész megoldásokat engedünk meg.

Indiában Brahmagupta már 628-ban készített módszert a Pell-egyenlet és más kvadratikus egyenletek megoldására, de Lord Brouncker volt az első európai matematikus, aki általános megoldást talált a nevezetes egyenletre. A XII. és XIV. században két, szintén indiai matematikus, Bhaskara és Narayana is talált általános megoldást az egyenletre.

31. Definíció. *[Pell-egyenlet] Pell-egyenletnek nevezzük az*

$$x^2 - dy^2 = 1$$

alakú diophantoszi egyenletet, illetve általánosabb formában az

$$x^2 - dy^2 = c$$

alakú egyenleteket, ahol $d \in \mathbb{Z}^+$, $c \in \mathbb{Z}$, $\sqrt{d} \notin \mathbb{Q}$. *Az* (x, y) *megoldásokat tehát az egészek között keressük.*

Jelen dolgozatban azonban csak az $x^2 - 2y^2 = 1$ alakú egyenlettel fogok mélyebben foglalkozni.

A Pell-egyenlet gyökeinek meghatározására számos módszer létezik: lánctörtekkel, faktorizáció kvadratikus szitával, sőt, kvantumszámítógéppel is kereshetünk megoldásokat. Ha van egy nemtriviális x_1, y_1 kiinduló megoldásunk ($y_1 \neq 0$), akkor végtelen sok további megoldást állíthatunk elő egy egyszerű képlettel:

$$x_i + y_i\sqrt{d} = (x_1 + y_1\sqrt{d})^i$$

Ezzel ekvivalens a következő rekurzió [8]:

$$\begin{aligned} x_{i+1} &= x_1 x_i + d y_1 y_i \\ y_{i+1} &= x_1 y_i + y_1 x_i \end{aligned}$$

Érdekesség továbbá, hogy az első- és másodfajú Csebisev-polinomok (T_i és U_i) is a megoldásai lehetnek a $p^2 - nq^2 = 1$ Pell-egyenletnek a $\mathbb{Q}[x]$ egyváltozós polinomgyűrű felett, ha $n = x^2 - 1$, mégpedig a következőképpen:

$$T_i^2 - (x^2 - 1)U_{i-1}^2 = 1$$

Továbbá hasonló képletet is kapunk a többi megoldás előállítsára:

$$T_i + U_{i-1}\sqrt{x^2-1} = (x+\sqrt{x^2-1})^i$$

Ez a megfigyelés is sugallja, hogy a Pell-egyenlet megoldása során érdemes támaszkodni az algebrai számelmélet eszköztárára, ezért most olyan megközelítést fogunk alkalmazni, ami felhasználja a számgyűrűkkel kapcsolatos ismereteinket.

2.2. Megközelítés az algebrai számelmélet segítségével

A $x^2 - dy^2 = 1$ egyenletet szorzattá alakítva az

$$(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$$

alakú egyenletet kapjuk. Ennek a faktorizációnak a célja az, hogy a megfelelő számgyűrűben dolgozhassunk, így szorzatként előállíthassuk az egyenlet jobb oldalán álló 1-et.

Mivel $x, y \in \mathbb{Z}$, ezért $x - \sqrt{d}y$ és $x + \sqrt{d}y$ számokkal a $\mathbb{Z}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{d})$ gyűrűben szeretnénk és fogunk számolni. A későbbiekben fontos lesz az a megfigyelés, hogy ennek a bővítésnek a foka $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$.

32. Definíció. *[norma(1)] Egy $\mathbb{Q}(\sqrt{d})$-beli $z = a + b\sqrt{d}$ szám konjugáltja $\overline{z} = a - b\sqrt{d}$ és normája:*

$$N(z) = z\overline{z} = a^2 - db^2$$

Az így bevezetett norma definíciója egyébként nem más, mint az algebrai számtestekben általában használt norma [9] speciális esete:

33. Definíció. *[norma(2)] Ha K algebrai test $\mathbb{Q}$ fölött és α egy K-beli egész, akkor α-nak n konjugáltja létezik $\mathbb{C}$-ben, az α szám normája ekkor $N(\alpha) = \alpha_1 \cdots \alpha_n$.*

Természetesen a definícióból következik, hogy α normája függ a K testtől, hiszen például míg a 2 normája a racionális számtest fölött 2, addig a Gauss-racionális számok körében 4 lesz.

2. Tétel. *[multiplikativitás] A norma képzése és a konjugálás is multiplikatív:*

$$\begin{aligned} N(z)N(w) &= N(zw) \\ \overline{zw} &= \overline{z} \cdot \overline{w} \end{aligned}$$

Az így definiált norma és konjugálás tehát kulcsfontosságú lesz a Pell-egyenlet gyökeinek meghatározásánál, hiszen ekkor az x, y megoldások egyértelműen megfeleltethetők egy $\mathbb{Z}(\sqrt{d})$-beli számnak: $z = x + \sqrt{d}y$. Ez azt jelenti, hogy az eredeti egyenlet a bevezetett számgyűrűben a következő egyenletté alakítható: $N(z) = 1$.
Vegyük észre, hogy bármely z megoldásra, vagyis ha $N(z) = 1$, akkor $\overline{z}$ is megoldás és $\overline{z} = \frac{1}{z}$, hiszen $N(\overline{z}) = \overline{z} \cdot \overline{\overline{z}} = \overline{z}z = z\overline{z} = N(z)$.
Hasonlóan $N(-z) = (-z) \cdot \overline{-z} = (-1) \cdot z \cdot \overline{(-1) \cdot z} = (-1) \cdot z \cdot \overline{(-1)} \cdot \overline{z} = (-1) \cdot z \cdot (-1) \cdot \overline{z} = z\overline{z} = N(z)$.
Ezek alapján tehát megállapíthatjuk, hogy ha találunk egy z_0 megoldást, akkor abból előállíthatjuk a $z_n = \pm z_0^n, n \in \mathbb{Z}$ megoldásokat, ezeknek megfelelő x, y számok megoldásai lesznek Pell-egyenletnek [6].

2.3. A Dirichlet-egységtétel

Egy gyűrűben fontos speciális elemek azok, melyek invertálhatóak, az $(R, \cdot)$ multiplikatív félcsoport esetében ugyanis nem követeltük meg az invertálhatóságot:

34. Definíció. *[egység] Egy R gyűrű $(R, \cdot)$ multiplikatív félcsoportjában egységnek nevezzük azokat az elemeket, amelyeknek létezik inverze, vagyis azon $u \in R$ elemek, melyekre $\exists v = u^{-1} : uv = vu = 1_R$, ahol 1_R a multiplikatív egységelem.*

3. Tétel. *[egységcsoport] Egy R gyűrű egységeinek $U(R)$ halmaza (multiplikatív) csoportot alkot az R-beli szorzásra nézve.*

Bizonyítás.

- asszociativitás: triviális, hiszen magára az R gyűrűre is igaz
- műveleti zártság:
  $u_1 \in U(R), u_2 \in U(R) \implies \exists u_1^{-1}, u_2^{-1} \implies \exists (u_1u_2)^{-1} = u_2^{-1}u_1^{-1} :$
  $(u_1u_2)(u_1u_2)^{-1} = (u_1u_2)u_2^{-1}u_1^{-1} = u_1(u_2u_2^{-1})u_1^{-1} = u_1 1_R u_1^{-1} = u_1u_1^{-1} = 1_R$
- egységelem: triviális, hiszen 1_R az eredeti gyűrűben is multiplikatív egységelem

- inverz elem: triviálisan létezik, hiszen pontosan az invertálható elemeket vettük be a csoportba

□

9. Példa. *[egységek] A $\mathbb{Z}(\sqrt{d})$ egészeinek gyűrűjében:*

- *$d = 2$ esetén $z = \sqrt{2} + 1$ számra:* $(\sqrt{2}+1)(\sqrt{2}-1) = 2 - 1 = 1$
- *$d = 5$ esetén $z = \sqrt{5} + 2$ számra:* $(\sqrt{5}+2)(\sqrt{5}-2) = 5 - 4 = 1$

Mint látni fogjuk, végtelen sok egység van.

4. Tétel. *[egységek normája] Egy R algebrai számgyűrű r eleme akkor és csak akkor tartozik az $U(R)$ egységcsoportba, ha normája $N(r) = \pm 1$.*

Bizonyítás. Itt csak azt mutatjuk meg, hogy egységcsoport elemeinek normája ± 1.
Az r gyűrűelem pontosan akkor eleme $U(R)$-nek, ha $\exists r^{-1} : rr^{-1} = 1$. Ekkor a norma multiplikativitása miatt $N(r)N(r^{-1}) = N(rr^{-1}) = N(1) = 1$. Mivel az a norma az egész számokra képez, az r szám $N(r)$ normája csak ± 1 lehet. □

Jegyezzük meg, hogy az eredeti számgyűrűnk ($\mathbb{Z}(\sqrt{d})$) kommutatív! Ebből következik, hogy az $U(\mathbb{Z}(\sqrt{d}))$ egységcsoport, amivel most dolgozni fogunk, Abel-csoport lesz. Egy Abel-csoport torziómentes rangjára több, ekvivalens definíció létezik [27], ezek közül praktikus és elegendő is most a legegyszerűbb:

35. Definíció. *[egységcsoport rangja] Egy G Abel-csoport rangja az az n szám, amely a maximális $\mathbb{Z}$-lineárisan független, G-beli részhalmazok számossága.*

Ez az n szám invariáns a vektorterek dimentziójához hasonlóan, amit a kicserélési tétel mond ki.

A Pell-egyenletből származtatott algebrai probléma a $\mathbb{Z}(\sqrt{d})$ gyűrűvel dolgozik. Alapvetően a $\mathbb{Q}(\sqrt{d})$ számtesttel dolgoznánk, de mi csak az egyenlet egész megoldásait keressük. A számtestek algebrai egészeivel juthatunk el a megfelelő számgyűrűhöz.

A továbbiakban a rövidség kedvéért a K algebrai számtest algebrai egészeinek gyűrűjét O_K-vel fogjuk jelölni.

A $\mathbb{Q}(\sqrt{d})$ számtest algebrai egészei $d \equiv 2, 3 \pmod 4$ esetén pontosan a $\mathbb{Z}(\sqrt{d})$-beli számok lesznek. A $d \equiv 0 \pmod 4$ esetben d nem négyzetmentes, ekkor az

egyenlet visszavezethető egy négyzetmentes d számra. A $d \equiv 1 \pmod 4$ esetben a $\mathbb{Z}(\frac{\sqrt{d}+1}{2})$-beli számokkal kell számolnunk. Mindezek miatt a továbbiakban a $\mathbb{Q}(\sqrt{2})$ test algebrai egészeinek tárgyalásánál dolgozhatunk a $\mathbb{Z}(\sqrt{2})$ számokkal.

36. Definíció. *[kvadratikus test] Kvadratikus számtest egy olyan K algebrai számtest, amely másodfokú $\mathbb{Q}$ fölött. $\mathbb{Q}(\sqrt{d})$ esetében, ha $\sqrt{d} \notin \mathbb{Z}$, $d > 0$ esetében valós kvadratikus testről beszélünk, $d < 0$ esetén képzetes vagy imaginárius kvadratikus testről.*

Arra a kérdésre, hogy milyen a tárgyalt egységcsoport szerkezete (és általában tetszőleges számtestben az egységcsoporté), a Dirichlet-egységtétel fog választ adni.

37. Definíció. *[beágyazás] Ha $\sigma_i : K \to \mathbb{R}$, akkor valós beágyazásnak nevezzük, egyébként komplex beágyazásnak.*

A valós beágyazások számát r_1, a komplexekét r_2 jelöli. Így kapjuk a következő kanonikus beágyazást:

$$\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R}^n$$

Ez a kanonikus beágyazás egy injektív gyűrűhomomorfizmus, melyre

$$\sigma(x) = (\sigma_1(x), \cdots, \sigma_{r_1+r_2}(x)).$$

5. Tétel. *[Dirichlet-egységtétel(1)] Egy O_K gyűrű $U(O_K)$ egységcsoportja végesen generált és a rangja $r = r_1 + r_2 - 1$, ahol r_1 a valós beágyazások, r_2 pedig a komplex beágyazások konjugált párjainak száma.*

6. Tétel. *[Dirichlet-egységtétel(2)] [5] Egy K test $U(K)$ egységcsoportja izomorf a $G \times \mathbb{Z}^r$ csoporttal, ahol G az 1-nek K gyűrűbeli gyökeit tartalmazó ciklikus csoport, és $r = r_1 + r_2 - 1$. (Másképp: G a K-ba eső komplex egységgyökök véges ciklikus csoportja.)*

Mivel egy $\mathbb{Q}$-monomorfizmus komplex konjugáltja is $\mathbb{Q}$-monomorfizmus, a σ_i-k et átszámozva párba állíthatjuk őket a következőképpen:
Legyenek a valós beágyazások $\sigma_1, \cdots, \sigma_{r_1}$, a komplexek pedig $\sigma_{r_1+1}, \cdots, \sigma_n$ úgy, hogy $j = 1, \cdots, r_2$-re minden σ_{r_1+j}-t a komplex konjugáltjával, $\sigma_{r_1+r_2+j}$-vel párosítjuk össze.
Így adódik, hogy $2r_2$ komplex beágyazás van, valamint $[K : \mathbb{Q}] = n = r_1 + 2r_2$.

Az egységcsoport struktúráját tehát ismerjük, meghatározhatjuk a rangját és előállíthatjuk csoportok direkt szorzataként is.
Ezek alapján egy valós kvadratikus test egységcsoportjának rangja 1, az imaginárius kvadratikus testeké pedig 0 lesz.

A Pell-egyenlet esetében a $\mathbb{Q}(\sqrt{d})$ kvadratikus testtel, illetve $\mathbb{Z}(\sqrt{d})$ egészekkel dolgozunk, melynek $U(O_K)$ egységcsoportja 1 rangú. Mivel a Dirichlet-egységtétel kimondja, hogy ez a csoport végesen generált, ezért elegendő megkeresni a generátorát.

A végesen generált Abel-csoportok alaptétele szerint minden végesen generált Abel-csoport egy véges rangú szabad Abel-csoport és egy véges Abel-csoport direkt összege, melyek izomorfizmus erejéig egyértelműen meghatározottak.

A vizsgált Pell-egyenlet esetén az U egységcsoport tehát

$$U \cong \mathbb{Z} \times \mathbb{Z}_2 \cong G \times H$$

adódik, ahol az egyenlet egy nemtriviális megoldása, $3+2\sqrt{2}$ választható a H csoport generátorának, ezen kívül $G = \{\pm 1\}$.

Mivel a vizsgált példában $x^2 - 2y^2 \not\equiv 3 \pmod 4$ miatt -1 normájú egység nem létezik, az egységek pontosan a Pell-egyenlet megoldásait adják. A $d \equiv 1 \pmod 4$ esetben $\frac{\sqrt{d}+1}{2}$ miatt összetettebb a megoldások szerkezete, $x^2 - dy^2 \equiv -1$ is előfordulhat, továbbá az egységcsoport elemeire x, y nem feltétlenül lesznek egész számok, így ott az egységek és a megoldások közötti kapcsolat bonyolultabb.

3. fejezet

Csoportok és Cayley-gráfok

Általában a csoportok és különösen a diszkrét csoportok struktúrájának vizsgálatakor fontos szerepe van a csoport generátorainak. A generátorelemek száma és rendje sokat elárul a csoport szerkezetéről és rendjéről is, ezen kívül csoportok közötti hasonlóságokra is következtethetünk. A csoportok generétorhalmazainak segítségével a felrajzolhatjuk Cayley-gráfjaikat, ami szintén egy hasznos eszköz a struktúra feltárásában.

A Cayley-gráfok tulajdonságait a véges vagy végesen generált csoportok esetén (ezek úgynevezett diszkrét csoportok) fogom vizsgálni.

Egy G csoporthoz általában többféleképpen választhatunk generátorhalmazt, ez a választás pedig tetszőleges, így a csoportelemek a generátorelemek más-más kombinációjaként fognak előállni. Amikor tehát egy csoporthoz felrajzoljuk a Cayley-gráfját, az természetesen különböző elemeknek megfeleltetett csúcsokat fog összeköti, attól függően, hogyan választottuk ki az S generátorhalmazt.

A Cayley-gráfokat sok helyen használják: alapvető eszköz a kombinatorikus és a geometriai csoportelméletben, a másodrendű logikában [5], a párhuzamos programozásban hálózati topológiaként használják irányítatlan, 3-reguláris változatait, a gyűrűs kockákat [17].

3.1. A Lovász-sejtés

További érdekesség, hogy egy máig nyitott probléma is kapcsolódik a Cayley-gráfokhoz: a Lovász-sejtés 1970-ből, mely a Hamilton-körök klasszikus problémájával foglalkozik [1, 7, 10].

38. Definíció. *[csúcs-tranzitivitás] Ha egy $G = (V, E)$ gráfnak minden $\forall u, v \in V$*

csúcspárra létezik olyan $\phi : V \to V$ gráfautomorfizmusa, amelyre $\phi(u) = v$, akkor a G gráf csúcs-tranzitív.

1. Sejtés. *[Lovász-sejtés] Minden véges, összefüggő csúcs-tranzitív gráf tartalmaz Hamilton-utat.*

Hamilton-kör esetében a sejtésre több ellenpéldát is ismerünk: a 2-csúcsú teljes gráf (K_2), a Petersen gráf, a Coxeter-gráf, valamint az utóbbi kettőből a csúcsok háromszöggel való helyettesítésével kapott gráfban sincs Hamilton-kör. Így a Lovász-sejtés erősített változata:

2. Sejtés. *[erős Lovász-sejtés] Az öt ismert kivételen kívül minden véges, összefüggő csúcs-tranzitív gráf tartalmaz Hamilton-kört.*

Mivel minden Cayley-gráf csúcs-tranzitív, a sejtés egy gyengített változatát is megfogalmazhatjuk:

3. Sejtés. *[Lovász-sejtés Cayley-gráfokra] Minden véges, összefüggő Cayley-gráf tartalmaz Hamilton-kört.*

A sejtés továbbá nem igaz irányított Cayley-gráfokra. A gyenge sejtés második változatát speciális esetekben csoportelméleti eszközökkel érdemes vizsgálni, Abel-csoportokra például könnyen igazolható az állítás.

3.2. Cayley-gráfok

Egy Γ Cayley-gráf egy G diszkrét csoport struktúráját kódolja a tetszőlegesen választott S generátorhalmaz szerint, így a csoport szerkezetét segít feltárni.

39. Definíció. *[színezett Cayley-gráf] Egy G diszkrét csoport tetszőleges S generátorhalmazához a $\Gamma = \Gamma_c(G, S)$ irányított színezett Cayley-gráf a következőképpen készíthető el:*

- *az S generátorhalmaz s elemeihez egy c_s színt rendelünk*
- *a G csoport minden g eleméhez egyértelműen hozzárendeljük Γ egy csúcsát: $V(\Gamma) \leftrightarrow G$*
- *minden $g \in G$ és $s \in S$ párhoz a Γ gráfban a g és $s \cdot g$ csúcsok között egy irányított, c_s színű él megy*

Ha az S-t úgy választjuk, hogy szimmetrikus generátorhalmaz legyen (vagyis minden $s \in S : s^{-1} \in S$), akkor egy olyan $\vec{\Gamma}(G, S)$ irányított Cayley-gráfot kapunk, amelynek minden éle kétszeres: $\forall uv \in \vec{E} : vu \in \vec{E}$).
Ha eltekintünk az élek színezésétől, akkor a $\vec{\Gamma}(G, S)$ irányított Cayley-gráfot kapjuk, ha az irányítást sem vesszük figyelembe, akkor a $\Gamma(U, V)$ Cayley-gráfot.

10. Példa. *[Cayley-gráf] (egy-két kisebb diszkrét csoport, a generátora és egy ábra a gráfról)*

Fontos megjegyezni, hogy az e egységelemet nem vesszük be az S generátorhalmazba, hiszen ezzel csak hurokéleket kapnánk minden egyes csúcshoz. Elmondható, hogy ha S valóban generátora G-nek, akkor a Cayley-gráf összefüggő lesz, többszörös élek 2-rendű elemeknél fordulhatnak elő, valamint pontosan akkor kapunk körmentes gráfot, vagyis Cayley-fát, ha G szabad csoport, hiszen ekkor áll elő minden $g \in G$ elem a generátorelemek egyértelmű kombinációjaként.

A Cayley-gráfról további alapvető tulajdonságokat is megállapíthatunk:

- minden irányított és irányítatlan Cayley-gráf is csúcs-tranzitív
- a $\vec{\Gamma}(G, S)$ Cayley-digráf reguláris, mégpedig $d = |S|$ esetében minden csúcsból pontosan d darab él megy ki és d darab él fut be, melyek száma természetesen függ a választott generátorhalmaztól
- az irányított Cayley-gráf erősen összefüggő
- a $\Gamma(G, S)$ Cayley-gráf reguláris, minden csúcs foka $|S \cup S^{-1} - \{1\}|$

Minden, a gráfban megtalálható kör egy összefüggést fog jelenteni az elemekre nézve a következőképpen:
A körön haladva folyamatosan jegyezzük fel az élek színéhez tartozó generátorelemeket (visszafelé mutató élen is haladhatunk előre, mivel ez az inverz elemmel való szorzást jelenti), majd mikor visszaértünk a kiinduló elemhez, megállunk. A feljegyzett elemeket összeszorozzuk a megfelelő sorrendben, s mivel a kör visszatér önmagába, az e egységelemet fogjuk kapni a szorzás végeredményeképp. Ezt egy *reláció*nak nevezzük. A gráfban minden kör egy ilyen relációt fog jelenteni, ami már a konkrét elemektől függetlenül, egészen absztrakt módon jellemzi a csoport szerkezetét. A *relátorok* olyan, a csoport elemeiből álló kifejezések, melyek a csoport egységelemével tekintendők egyenlőnek, ezáltal relációkat jelképeznek.

40. Definíció. *[csoport prezentációja] Egy G csoport prezentációja $\langle S \mid R \rangle$, ahol S a G csoport generátorhalmaza, R pedig a csoportot meghatározó relátorok S-ből képzett halmaza. Egy prezentáció véges, ha G végesen generált, vagyis S véges, valamint ha R is véges.*

7. Tétel. *[Dyck tétele] Tekintsünk egy S generátorhalmaz által generált $\langle S \rangle$ szabad csopotot. Tekintsük benne szavak egy R halmazát. N legyen R normális lezártja S-ben, vagyis az a minimális normális részcsoport, ami tartalmazza R-t. Ekkor a $\langle S, R \rangle$ prezentáció által meghatározott csoport:*

$$\langle S \mid R \rangle = \langle S \rangle / N$$

11. Példa. *[csoport prezentációja] A D_{2n} diédercsoport prezentációja:*
$\langle f, t \mid t^2, f^n, (ft)^2 \rangle$, ahol t tengelyes tükrözést, f pedig egy olyan forgatást jelent, melynek rendje relatív prím n-hez.

8. Tétel. *[csoportok prezentációja] Minden G csoportnak létezik prezentációja, valamint minden véges csopornak létezik véges prezentációja.*

Ahhoz, hogy a Cayley-gráfok definícióját még mélyebben megértsük, a Cayley-tétel nyújt alapot:

41. Definíció. *[szimmetrikus csoport] Egy S halmaz $Sym(S)$ szimmetrikus csoportja az a csoport, amely az S halmaz összes bijekcióját tartalmazza, a kompozícióra, mint csoportműveletre nézve. A szimmetrikus csoport elemei az S permutációi.*

12. Példa. *[szimmetrikus csoport] Egy n elemű halmaz szimmetrikus csoportja $n!$ rendű. Például a $\mathbb{Z}_4 = (\{0, 1, 2, 3\}, + \pmod 4)$ csoport szimmetrikus csoportjának rendje tehát 24, elemei:*
id, (12) ,(13*)*, (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (124), (134), (234), (132), (142), (143), (243), (1234), (1243), (1324), (1342), (1423), (1432).

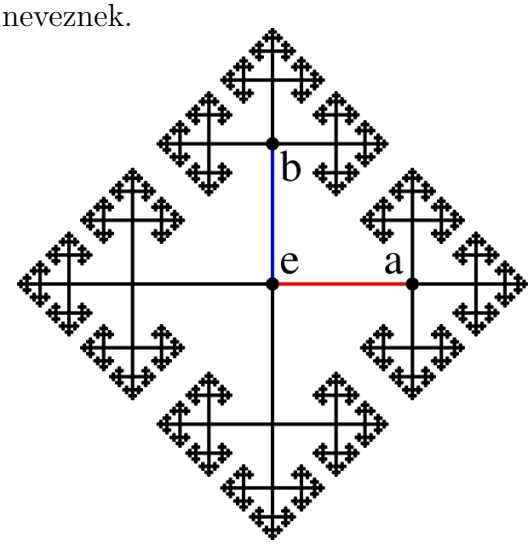
9. Tétel. *[Cayley-tétel] Minden G csoport izomorf a G alaphalmazot vett szimmetrikus csoportnak, $Sym(G)$-nek egy részcsoportjával.*

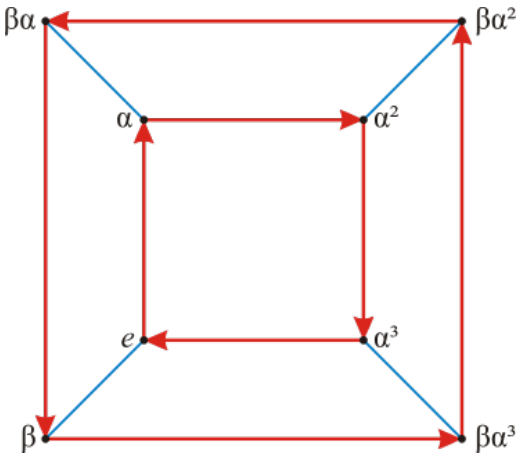
A Cayley-tételben szereplő $\tau : G \to K$ $(K < Sym(G))$ izomorfiát G reguláris reprezentációjának is szokás nevezni.

13. Példa. *[reguláris reprezentáció] A már bemutatott $\mathbb{Z}_4$ csoport elemei sorra az $\{id, (1234), (13)(24), (1432)\}$ elemeknek fognak megfelelni.*

Triviális, de a fenti példán is jól látszik, hogy a kiinduló csoport kommutativitásából egyáltalán nem következik a szimmetrikus csoporjának kommutativitása, hiszen az S_n szimmetrikus csoportok csak $n \leq 2$-re Abel-csoportok.

Gondoljuk meg, milyen gráfokat kapunk speciális G csoportokra!
Ha G Abel-csoport, akkor $\forall a, b \in G : ab = ba$, vagyis a kommutátorra $a^{-1}b^{-1}ab = 1$, így ez bármely két generátorelemre egy 4-hosszú kört eredményez a Cayley-gráfban. Ez a generátorelemek számától függően többdimenziós „rácsot" fog generálni, a csoport kommutativitása tehát magában egy sűrű rácsozatot jelent a gráfban.
Ha G szabad csoport, akkor a Cayley-gráf egy Cayley-fa lesz, amit Bethe-hálónak is neveznek.





Két olyan csoport Cayley-gráfját készítettük el, amelyek két generátorelemmel adottak. A különbség köztük prezentációban megadott R azonosságokban van:

Az első egy szabad csoport, melyet a és b generálnak, a csoport prezentációja $\langle a, b \mid \emptyset \rangle$. Látható, hogy minden csúcsban négy él találkozik: kettő indul ki és kettő érkezik be. Az így kapott Cayley-fa szimmetriája jól látható, a kiindulási egységelemnek más elemet választva (és természetesen az élek hosszát megfelelően átskálázva) a fa önmagába vihető át.

A második egy diédercsoport Cayley-gráfja, ahol a β elem egy tükrözést jelöl, ezáltal a rendje 2, a hozzá tartozó élek ezáltal kétszeres élek lesznek. A másik generátorelem, α rendje 4, ezért ez a négyzet izometriacsoportjának Cayley-gráfja. Prezentációja így $\langle \alpha, \beta \mid \alpha^4, \beta^2, (\alpha\beta)^2 \rangle$.

Látható, hogy egyik csoport sem kommutatív, hiszen egyik gráfban sincsenek

meg a megfelelően irányított, 4-hosszúságú körök. (A diédercsoport gráfjában ugyan vannak 4-körök, de az irányításuk nem megfelelő.) Mivel a kiválasztott elemek generálják az egyes csoportokat, a Cayley-gráfok összefüggőek.

Ha az S-t nem megfelelően választjuk meg, akkor előfordulhat, hogy nem generálja G-t és így a kapott Cayley-gráf ugyan reguláris lesz, de nem összefüggő.

3.3. Expander gráfok

Természetesen adódik, hogy egy csoport (irányítatlan) Cayley-gráfját szeretnénk szomszédsági mátrixként is felírni. Triviálisan ekkor $|S| = d$ generátor esetén a gráf d-reguláris, így a szomszédsági mátrix minden sorában és oszlopában is pontosan d darab 1-es van. Könnyű látni, hogy ilyenkor a mátrix egyik sajátvektora az 1-esekből álló vektor, a hozzá tartozó sajátérték pedig d. A generátorelemek rendjétől függően kapunk sűrűbb vagy ritkább gráfot (és ezzel mátrixot is).
Expander gráfok alatt tulajdonképpen olyan ritka gráfokat értünk, amelyek egyszersmind „jól összekötöttek" is, vagyis a csúcsokból induló élek struktúrája bizonyos értelemben sűrű. Azt, hogy egy ilyen irányítatlan gráf mennyire összefüggő, illetve mennyire „jól kötött", többféle mérőszámmal mérhetjük:

42. Definíció. *[Cheeger-konstans] A G gráf Cheeger-konstansa (izoperimetrikus száma vagy él-expanziója) a*

$$h(G) := \min_{1 \leq |S| \leq \frac{n}{2}} \frac{|\partial(S)|}{|S|}$$

szám, ahol $S \subset V$, és $\partial(S)$ azon élek halmaza, melyeknek pontosan egy végpontjuk S-beli.

Ha ez a h szám nem túl kicsi (a precíz megfogalmazástól most eltekintünk), akkor az S részhalmazoknak sok szomszédjuk lesz.

43. Definíció. *[konduktivitás] Egy $G = (V, E)$ gráfban egy $(S, \overline{S})$ vágás konduktivitása*

$$\varphi(S) = \frac{\sum_{i \in S, j \in \overline{S}} a_{ij}}{a(S)a(\overline{S})}$$

ahol $a(S) = \sum_{i \in S} \sum_{j \in V} a_{ij}$, vagyis azon élek száma, melyeknek van S-beli csúcsa. A G gráf konduktivitása:

$$\phi(G) = \min\{\varphi(S) \mid S \subseteq V\}.$$

44. Definíció. *[csúcs-expanzió] A G gráf α-csúcs-expanziója*

$$g_\alpha(G) = \min_{1 \le |S| \le \alpha n} \frac{|\Gamma(S)|}{|S|}$$

ahol $\Gamma(S)$ azon csúcsok halmaza, melyeknek van S-beli szomszédja.

45. Definíció. *[spektrális hézag] Ha egy G d-reguláris gráfra a gráf A szomszédsági mátrixának valós sajátértékei $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$, akkor G spektrális hézaga $\triangle(G) = \lambda_1 - \lambda_2 = d - \lambda_2$.*

A Cheeger-konstans azt méri, hogy az adott gráfnak van-e „szűkülete" és milyen mértékben: ha a gráf összefüggő, akkor szigorúan pozitív és minél kisebb, a gráf annál inkább „szűk". A konduktivitás megmutatja, mennyire gyorsan tart G-n egy véletlen séta az egyenletes eloszláshoz. A fenti mérőszámok között több összefüggés van:

- Egy d-reguláris gráf Cheeger-konstansa a konduktivitásának d-szerese.
- $h(G) \ge g_{\frac{1}{2}}(G) - 1$
- Egy d-reguláris gráfra $\frac{\triangle(G)}{2} \le h(G) \le \sqrt{2d \triangle(G)}$ [11, 14, 26].

46. Definíció. *[expander család] d-reguláris gráfok $\mathcal{G} = \{G_1, G_2, \dots\}$ családját él-expander családnak nevezzük, ha létezik olyan pozitív c konstans, hogy a család minden G gráfjára $h(G) \ge c$. $\mathcal{G}$ csúcs-expander család, ha létezik $1 < c$ konstans, hogy a család minden G gráfjára $g_{\frac{1}{2}}(G) \ge c$. $\mathcal{G}$ spektrál expander család, ha létezik olyan pozitív c konstans, ami alsó korlátja a családbeli gráfok spektrális hézagának.*

Igazolható, hogy expander családok léteznek, valamint Babai Lászlónak létezik egy sejtése is, mely szerint bizonyos jól megválasztott csoportok Cayley-gráfjainak családja is expander család. Ezek belátása nem egyszerű, nagy eredménynek számít ilyen expander családok konstruálása, ezért ezen állítások igazolásától most eltekintek.

Egy gráf Cheeger-konstansa és csúcs-expanziója közti $h(G) \ge g_{\frac{1}{2}}(G) - 1$ összefüggésből következik, hogy ha gráfok egy családja spektrál expander család egy $c > 1$ konstansra, akkor él-expander család is egy $c - 1 > 0$ konstansra.

Az expander gráfok széles körben elterjedt matematikai modellek: természetes vagy mesterséges struktúrák leírásánál, kapcsolatok modellezésénél, kommunikációs hálózatokban és hálózati topológiákban, hibajavító kódoknál [20, 27] használják őket.

3.4. Algebrai gráfelmélet

Egy G gráf $A(G)$ szomszédsági mátrixa valós értékű és szimmetrikus, ezért a sajátértékei mind valósak: $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. A következőket tudhatjuk meg egy gráf sajátértékeiből [7]: (bizonyítás kell vmelyikre?)

- ha G reguláris, akkor $\lambda_1 = d$
- G pontosan akkor összefüggő, ha $\lambda_1 > \lambda_2$
- G pontosan akkor páros gráf, ha $\lambda_1 = -\lambda_n$

Itt megjegyezzük, hogy elterjedt módszer a szomszédsági mátrix normálása a következőképpen:

47. Definíció. *[normált szomszédsági mátrix] Ha a G gráf szomszédsági mátrixa $A = a_{ij}$, akkor a normált szomszédsági mátrixa $A' = \frac{a_{ij}}{D}$, ahol D a gráf foka (a legnagyobb fokszámú csúcs foka).*

Látható, hogy d-reguláris gráfokra, amikkel most is foglalkozunk, $D = d$, valamint a mátrix soraiban és oszlopaiban is az elemek összege 1 lesz. A normált mátrix sajátértékei $1 \geq \frac{\lambda_2}{\lambda_1} \geq \cdots \geq \frac{\lambda_n}{\lambda_1}$ lesznek, páros gráfra pedig $\frac{\lambda_n}{\lambda_1} = -1$.

A spektrális gráfelméletben a gráf szomszédsági mátrixán kívül a Laplace-mátrixa is sok információval szolgál a struktúráról [3]:

48. Definíció. *[Laplace-mátrix] Ha a G egyszerű gráf szomszédsági mátrixa A, sajátértékei $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, akkor $D := diag(d(v_1), d(v_2), \ldots, d(v_n))$ a fokmátrix ($d(v_i)$ az i-edik csúcs foka) és a gráf Laplace-mátrixa $L = D - A$. A Laplace-mátrix elemei tehát:*

$$l_{ij} = \begin{cases} d(v_i) & \text{ha } i = j \\ -1 & \text{ha } i \neq j \text{ és } i, j \text{ szomszédosak} \\ 0 & \text{egyébként} \end{cases}$$

Az L' normalizált Laplace-mátrix:

$$l'_{ij} = \begin{cases} 1 & \text{ha } i{=}j \\ -\frac{1}{\sqrt{d(v_i)d(v_j)}} & \text{ha } i \neq j \text{ és } i, j \text{ szomszédosak} \\ 0 & \text{egyébként} \end{cases}$$

Az L Laplace-mátrix és $\mu_1 \leq \mu_2 \cdots \leq \mu_n$ sajátértékei a következő tulajdonságokkal rendelkeznek:

- L pozitív szemidefinit ($\mu_i \geq 0$)
- $\mu_1 = 0$
- a 0 sajátérték (algebrai) multiplicitása a gráf összefüggő komponenseinek száma
- μ_2 a G gráf algebrai összefüggősége, az előző állításból is következik, hogy $\mu_2 \neq 0$ pontosan akkor, ha G összefüggő
- a legkisebb nemnulla sajátérték a Fiedler-érték, a hozzá tartozó sajátvektor a Fiedler-vektor

1. Állítás. *[a 0 sajátérték] A Laplace-mátrix legkisebb sajátértéke: $\mu_1 = 0$.*

Bizonyítás. L-nek sajátvektora az $e = (1, 1, \ldots, 1)^T$ vektor, mert $d(v_i) = |\{j \in V \mid ij \in E\}|$, tehát $Ae = (0, 0, \ldots, 0)^T$. Mivel $Ae = 0 \cdot e$, a $\mu = 0$ sajátértéke L-nek. L minden sajátértéke nemnegatív, ezért $\mu_0 = 0$ mindenképpen. □

2. Állítás. *[alsó korlát] A G gráf $h(G)$ Cheeger-konstansa és μ_2 algebrai összefüggőségére $\frac{\mu_2}{2} \leq h(G)$.*

A G gráf Fiedler-vektora is sok információt nyújt a szerkezetről, segítségével particionálható egy gráf a következőképpen: a Fiedler-vektor pozitív és negatív elemeinek megfelelő csúcsok kerülnek az egyik, illetve másik osztályba. Ezen kívül a nagyon kicsi abszolútértékű elemekhez tartozó csúcsokat egy harmadik osztályba rakhatjuk, ha tovább szeretnénk bontani a gráfot. Az így kapott partícióban a részek megközelítőleg azonos méretűek lesznek, köztük pedig kevés él megy.

3.5. Egy numerikus példa

Vizsgáljuk meg egy „kis” Cayley-gráf expander-tulajdonságait!

14. Példa. *[kis kocka élgráfja] A $\mathcal{G} = \{\mathbb{Z}_2^n\}$ családból válasszunk egy kis elemszámú csoportot: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Ez az $\mathbb{F}_2$ fölötti 3-dimenziós vektortér, így rendje $2^3 = 8$ lesz, elemei a 3 hosszúságú $0-1$ vektorok.*

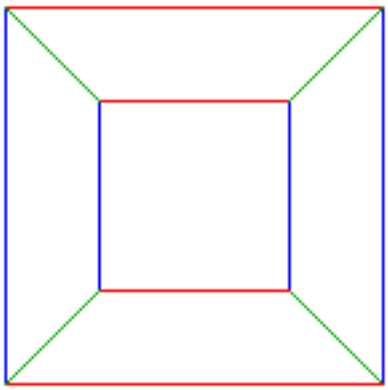
Mivel a vektortér dimenziója 3, ezért a csoport generátorhalmazához is 3 elemet választunk majd, legyen ez a szokásos bázis:

$$a := (1,0,0), \quad b := (0,1,0), \quad c := (0,0,1)$$

A csoport prezentációja az $S = \{a, b, c\}$ generátorral tehát:

$$\langle a, b, c \,|\, a^2, b^2, c^2, (ab)^2, (ac)^2, (bc)^2 \rangle$$

A csoport Cayley-gráfja irányítatlan lesz, mivel minden generátorelem rendje 2. Az egyes generátorelemekhez rendelt színek: a piros, b kék, c zöld színű él [24].



A csoport szomszédsági mátrixa így a következőképpen írható fel:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Mivel minden csúcs foka 3, a Laplace-mátrix a következő:

$$L = \begin{pmatrix} 3 & -1 & 0 & -1 & -1 & 0 & 0 & 0 \\ -1 & 3 & -1 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 3 & -1 & 0 & 0 & -1 & 0 \\ -1 & 0 & -1 & 3 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 3 & -1 & 0 & -1 \\ 0 & -1 & 0 & 0 & -1 & 3 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & 3 & -1 \\ 0 & 0 & 0 & -1 & -1 & 0 & -1 & 3 \end{pmatrix}$$

Minden csúcs foka 3, ezért a normalizálás során minden sort és oszlopot „végigosztunk” $\sqrt{3}$-mal. A normalizált Laplace-mátrix tehát:

$$L' = \begin{pmatrix} 1 & -\frac{1}{3} & 0 & -\frac{1}{3} & -\frac{1}{3} & 0 & 0 & 0 \\ -\frac{1}{3} & 1 & -\frac{1}{3} & 0 & 0 & -\frac{1}{3} & 0 & 0 \\ 0 & -\frac{1}{3} & 1 & -\frac{1}{3} & 0 & 0 & -\frac{1}{3} & 0 \\ -\frac{1}{3} & 0 & -\frac{1}{3} & 1 & 0 & 0 & 0 & -\frac{1}{3} \\ -\frac{1}{3} & 0 & 0 & 0 & 1 & -\frac{1}{3} & 0 & -\frac{1}{3} \\ 0 & -\frac{1}{3} & 0 & 0 & -\frac{1}{3} & 1 & -\frac{1}{3} & 0 \\ 0 & 0 & -\frac{1}{3} & 0 & 0 & -\frac{1}{3} & 1 & -\frac{1}{3} \\ 0 & 0 & 0 & -\frac{1}{3} & -\frac{1}{3} & 0 & -\frac{1}{3} & 1 \end{pmatrix}$$

Az A szomszédsági mátrix karakterisztikus polinomja:

$$x^8 - 12x^6 + 30x^4 - 28x^2 + 9.$$

A sajátértékek és algebrai multiplicitásuk egyszerűen kiszámítható:

$$x^8 - 12x^6 + 30x^4 - 28x^2 + 9 = (x-1)^3(x+1)^3(x-3)(x+3)$$

$$\begin{aligned} \lambda_1 &= 3 \\ \lambda_2 = \lambda_3 = \lambda_4 &= 1 \\ \lambda_5 = \lambda_6 = \lambda_7 &= -1 \\ \lambda_8 &= -3 \end{aligned}$$

A legnagyobb sajátérték $\lambda_1 = 3$, hiszen a gráf 3-reguláris. A $\lambda_1 = -\lambda_8$ megfigyelés

összhangban van azzal, hogy a gráf páros. A sajátvektoraira:

$$Av = \lambda v$$

A vizsgált 3-reguláris gráfra $L = D - A = 3I - A = 3v - \lambda v = (3 - \lambda)v$, ezért:

$$Lv = (D - A)v = Dv - Av = 3Iv - Av = 3v - Av.$$

Ezért pontosan az A mátrix sajátvektorai lesznek L sajátvektorai is, a megfelelő λ sajátértékekre pedig $\mu = 3 - \lambda$ sajátértékeket fogunk kapni, vagyis:

$$\begin{aligned} \mu_1 &= 0 \\ \mu_2 = \mu_3 = \mu_4 &= 2 \\ \mu_5 = \mu_6 = \mu_7 &= 4 \\ \mu_8 &= 6 \end{aligned}$$

A 0 sajátértékhez a $(1, 1, 1, 1, 1, 1, 1, 1)^T$ vektor tartozik, ez az összes csúcsot egy partícióba sorolja.
A gráf összefüggő, hiszen $\mu_2 > 0$ és a Laplace-mátrixának legkisebb nemnulla sajátértéke a $\mu_2 = 2$, ezért a Fiedler-értéke is 2. Mivel a 2 sajátérték multiplicitása 3, ezért az ehhez tartozó sajátvektorokhoz tartozó bázis 3-elemű:

$$\begin{aligned} v_1 &= (1, 1, 1, 1, -1, -1, -1, -1)^T \\ v_2 &= (1, 1, -1, -1, 1, 1, -1, -1)^T \\ v_3 &= (1, -1, -1, 1, 1, -1, -1, 1)^T \end{aligned}$$

Ezek a vektorok a kocka hálóját particionálva tulajdonképpen két, szemközti lapot eredményeznek partícóként.
A 4 sajátértékhez a következő sajátvektorok által generált sajátaltér tartozik:

$$\begin{aligned} u_1 &= (1, -1, 1, -1, 1, -1, 1, -1)^T \\ u_2 &= (1, 1, -1, -1, -1, -1, 1, 1)^T \\ u_3 &= (1, -1, -1, 1, -1, 1, 1, -1)^T \end{aligned}$$

Ekkor az osztályokba a kocka két, egymással szemközti élének csúcsa fog kerülni.
A legrosszabb partíciót a 6 sajátértékhez tartozó $(1, -1, 1, -1, -1, 1, -1, 1)^T$ sajátvektor adja, ez a kocka csúcsaiból alkotható két diszjunkt szabályos tetraédert eredményezi osztályokként.

A család minden egyes gráfja egy n-dimenziós hiperkocka hálózatát adja, ezekre is hasonló megfigyeléseket tehetünk a partíciókkal kapcsolatban.

A gráf spektrális hézaga $\triangle(G) = d - \lambda_2 = 3 - 1 = 2$ lesz.

A gráf izoperimetrikus számát egyszerűen ki tudjuk számolni.

$$h(G) := \min \frac{|\partial(S)|}{|S|}$$

Itt S-t egyeleműnek választva $|\partial(S)| = 3$ a regularitás miatt. A legkisebb értéket akkor veszi fel, ha $|S| = 4$, hiszen ekkor a csúcsok felét beválasztva $\partial S = \overline{S}$ lesz, így $h(G) = 1$ adódik.

4. fejezet

Elliptikus görbék

Számegyenesen, síkon, térben és többdimenziós terekben rengeteg csoportot találhatunk. A csoportok struktúrája függ a testtől, ami fölötti vektortérben dolgozunk, valamint a definiált csoportművelettől is. Többnyire a komplex számok és a kvaterniók multiplikatív csoportja által meghatározott szorzást használjuk, lehet a művelet a vektorok szokásos összeadása, de definiálhatunk egészen egyedi műveletet is, ami teljesen más struktúrát és ezáltal egészen eltérő részcsoportokat fog eredményezni. Ezen, számunkra valamiért érdekes részcsoportokból vizsgálunk meg néhány triviálisat, majd egy kevésbé közismert csoportstruktúrát az elliptikus görbék segítségével.

4.1. Részcsoportok síkban és terekben

A kvaterniók $(\mathbb{H}, \cdot)$ csoportjában sok érdekes részcsoportot találunk. Maguk a kvaterniók egy négydimenziós vektorteret alkotnak $\mathbb{R}$ fölött. Vektortérként tekintve szokásos bázis a $\{1, i, j, k\}$, a számolási szabályok pedig: $i^2 = j^2 = k^2 = ijk = -1$. Szoros kapcsolat áll fenn az úgynevezett Q kvaterniócsoporttal, mellyel a kvaterniók bővítésként az $\mathbb{R}(Q)$ formában írhatók fel. A kvaterniócsoport egy reguláris prezentációja $\langle i, j | i^4, i^2 j^2, iji^{-1}j^{-1} \rangle$, ez a D_4 diédercsoport mellett a másik nem-kommutatív 8 elemű csoport.
A kvaterniók legismertebb részcsoportjai $(\mathbb{R}, \cdot) < (\mathbb{C}, \cdot) < (\mathbb{H}, \cdot)$. A kvaterniók multiplikatív csoportja asszociatív, $\mathbb{C}$-vel és $\mathbb{R}$-rel ellentétben nem kommutatív és a báziselemek ismeretében a disztributivitási szabály segítségével számítható ki az

elemek szorzata:

$$\begin{gathered}(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) = \\ a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2 \\ +(a_1 b_2 + a_2 b_1 + c_1 d_2 - c_2 d_1) i \\ +(a_1 c_2 + a_2 c_1 - b_1 d_2 + b_2 d_1) j \\ +(a_1 d_2 + a_2 d_1 + b_1 c_2 - b_2 c_1) k.\end{gathered}$$

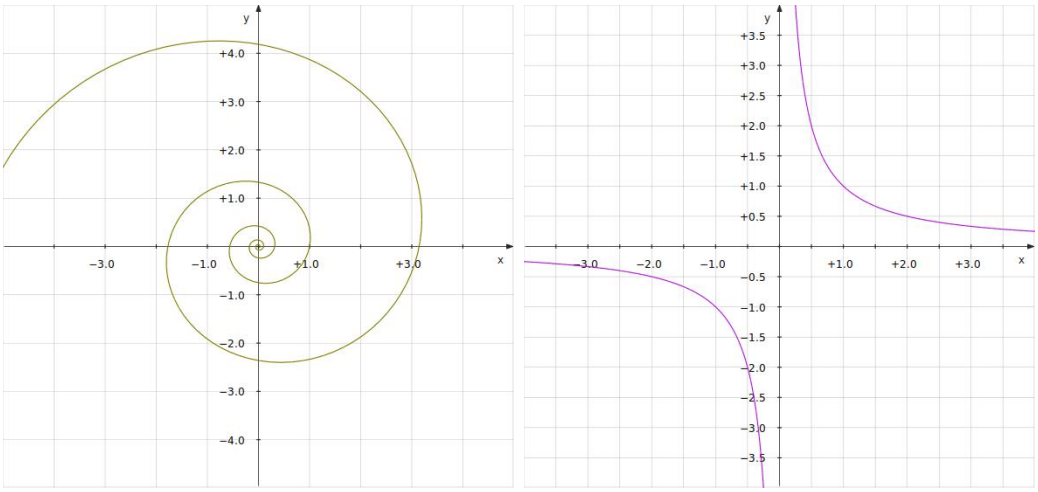
A kvaterniókon bevezetett normát a konjugálás segítségével értelmezhetjük. A konjugálás definíció szerint $\overline{a + bi + cj + dk} = a - bi - cj - dk$ és így $q\overline{q} = \overline{q}q$. Ebből is látszik, hogy egy $q \in \mathbb{H}$ elem centralizátora:

- ha $q \in \mathbb{R}$, akkor $C_{\mathbb{H}}(q) = \mathbb{H}$
- ha $q \in \mathbb{C}, q \notin \mathbb{R}$, akkor $C_{\mathbb{H}}(q) = \mathbb{C}$
- és általában ha $q = a_1 + bi + cj + dk$, akkor $C_{\mathbb{H}}(q) = \{a_2 + \lambda(bi + cj + dk) | \lambda \in \mathbb{R}\}$

Egy $q \in \mathbb{H}$ elem normája $N(q) = \sqrt{q\overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$, ez multiplikatív: $N(q_1 q_2) = N(q_1)N(q_2)$. Az inverz elem is a norma segítségével írható fel: $q^{-1} = \frac{\overline{q}}{N(q)}$.

Mivel a norma multiplikatív, ezért a kvaterniók multiplikatív csoportjának részcsoportjaiban az elemek normái is multiplikatív csoportok alkotnak. A norma képzése így egy homomorfizmus lesz: $N : \mathbb{H} \to \{\mathbb{R}^+ \cup 0\}$. Ezek alapján részcsoportot alkotnak az 1 normájú elemek, az egységgömb felszínét alkotó 4-dimenziós vektorok. Egy nagyobb részcsoportot kapunk, ha egy tetszőleges $a \in \mathbb{R}^+$ számra tekintjük az $S_a := \{q \in \mathbb{H} : \exists d \in \mathbb{Z} : N(q) = a^d\}$ számokat. Ezek pontosan azok a kvaterniók, amelyek normája az a egy egész kitevőjű hatványa, vagyis a 4-dimenziós térben azon egységgömbök, melyek sugara a-nak egy hatványa.

Egy másik érdekes részcsoport azon elemek halmaza, melyek egy adott q kvaternió egész kitevőjű hatványai, vagyis $S_q = \{\ldots, q^{-3}q^{-2}, q^{-1}, 1, q, q^2, q^3, \ldots\}$. Egy hasonló, de folytonos részcsoport azon kvaterniókból áll, melyek egy adott q kvaternióra: $P_q = \{q^d | d \in \mathbb{R}\}$. Nyilván $S_q < P_q$ és $S_q \cong (\mathbb{Z}, \cdot)$, valamint $P_q \cong (\mathbb{R}, \cdot)$. Ezek a csoportok a kvaterniók terében spirálokat rajzolnak ki, $q \in \mathbb{C}$ választással pontosan a sík logaritmikus spriáljait adják. (Itt megjegyezzük, hogy ez csak $N(q) \neq 1$ esetén van így, $N(q) = 1$-re egy kört kapunk.)



Ha másképpen definiáljuk pontok (illetve helyvektoraik) szorzatát, akkor más látványos részcsoportokat is kaphatunk. Ha az $S = \mathbb{R} \times \mathbb{R}$ síkban a pontok szorzatát $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$ definiálja, akkor részcsoportként tekinthetünk azon (x, y) pontokra, melyekre $xy = 1$. Ezek egy hiperbola pontjai, hiszen a definiált szorzásra a hiperbola zárt. Itt az egység az $(1, 1)$ pont, másodrendű a $(-1, -1)$ pont és a pontok így definiált szorzása Abel-csoportot határoz meg. Ha azon pontokat tekintjük, melyekre $xy = a \neq 0$, akkor azon hiperbolákból fog állni a csoport, amelyekre $xy = a^d$, ahol d egész.

4.2. Elliptikus görbék

Az elliptikus görbék olyan speciális görbék a síkon, amelyek pontjai (egy megfelelő művelettel) egy Abel-csoportnak felelnek meg. Nagyon jól alkalmazhatóak prímtesztelésre (ez elliptikus görbés prímtesztek a leggyorsabbaknak számítanak), valamint elterjedt használatuk az elliptikus kriptográfiai rendszerekben [21] is.

Tekintsünk egy K testet és fölötte egy $p(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ d-edfokú homogén polinomot. Azt vizsgáljuk, hogy a $p(x_0, x_1, x_2) = 0$ egyenletnek van-e megoldása a projektív síkon. (Az egyszerűség kedvéért a $K = \mathbb{R}$ test fölött fogunk foglalkozni a görbékkel.)
Ha egy L test tartalmazza K-t, akkor p nullhelyeit tekinthetjük $\mathbb{P}^2(K)$ helyett a $\mathbb{P}^2(L)$ projektív síkon. Ezt nevezzük a $\overline{H}_p(L)$ hiperfelületnek, amely jelen esetben projektív síkbeli görbe lesz.

49. Definíció. *[szingularitás] Nem-szinguláris pontoknak nevezzük azon*

$a \in \overline{H}_p(L)$ pontokat, melyek nem egyidejű megoldásai a következő egyenleteknek:

$$\partial_0 p = 0, \quad \partial_1 p = 0, \quad \partial_2 p = 0$$

Ekkor a p görbe a pontbeli érintőegyenesének egyenlete:

$$\partial_0 p(a)x_0 + \partial_1 p(a)x_1 + \partial_2 p(a)x_2 = 0$$

A $p(x_0, x_1, x_2) = 0$ egyenletű görbe nem-szinguláris, ha minden pontja nem-szinguláris. Egy nem-szinguláris harmadfokú homogén $p(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ polinom egy elliptikus görbét definiál, ha van legalább egy racionális pontja.

Ha L bővítése K-nak, akkor a $\overline{H}_p(L)$ görbét egyszerűen $E(L)$-lel jelöljük.

Ha a K test karakterisztikája nem 2 vagy 3, akkor igazolható, hogy minden K fölötti elliptikus görbe átalakítható a következő alakúvá:

$$x_0 x_2^2 = x_1^3 + a x_0^2 x_1 + b x_0^3, \quad a, b \in K$$

Ennek a görbének pontosan egy pontja van a végtelenben: $(0, 0, 1) \in \mathbb{P}^2(K)$. Ezt a pontot fogjuk ∞-nel jelölni.

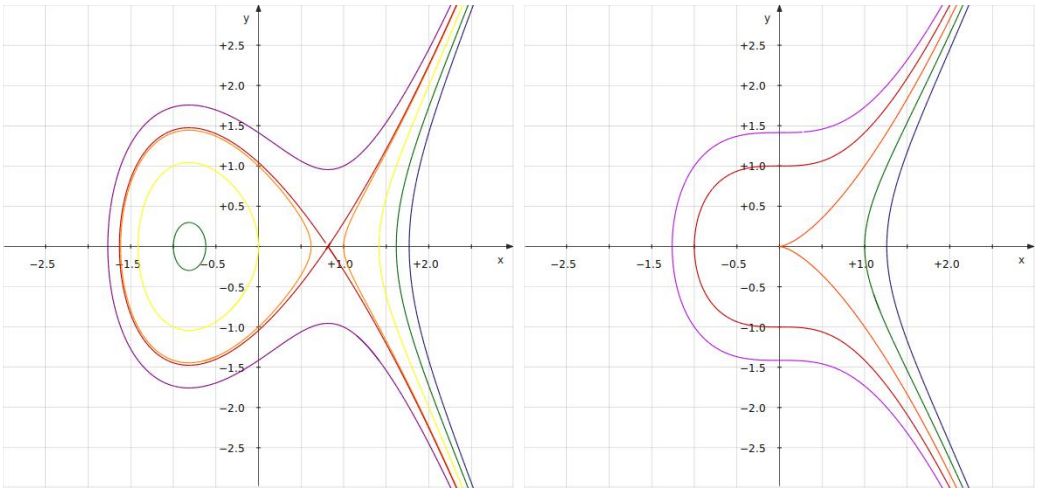
Áttérhetünk $x_0 \neq 0$ esetén affin koordinátákra ($x = x_1/x_0$ és $y = x_2/x_0$), így a görbe egyenletének $\mathbb{R}^2$-beli egyenletét kapjuk:

$$y^2 = x^3 + ax + b$$

Határozzuk meg, hogy mikor lesz a definiált görbe nem-szinguláris!
A $p(x_0, x_1, x_2) = x_0 x_2^2 - x_1^3 - a x_1^2 x_1 - b x_0^3$ görbe pontosan akkor szinguláris, ha a diszkriminánsa,

$$\triangle = -16(4a^3 + 27b^2) = 0,$$

vagyis p pontosan akkor lesz elliptikus görbe, ha $\triangle \neq 0$. A valós számsíkon $4a^3 + 27b^2 = 0$ paraméterválasztással $\triangle = 0$ lesz, így egy szinguláris görbét kapunk, egyébként elliptikus görbéket. A $\triangle$ diszkrimináns előjelétől függ a komponensek száma: ha $\triangle > 0$, akkor a görbe két komponensből áll, $\triangle < 0$ esetén pedig egy összefüggő komponenst kapunk.



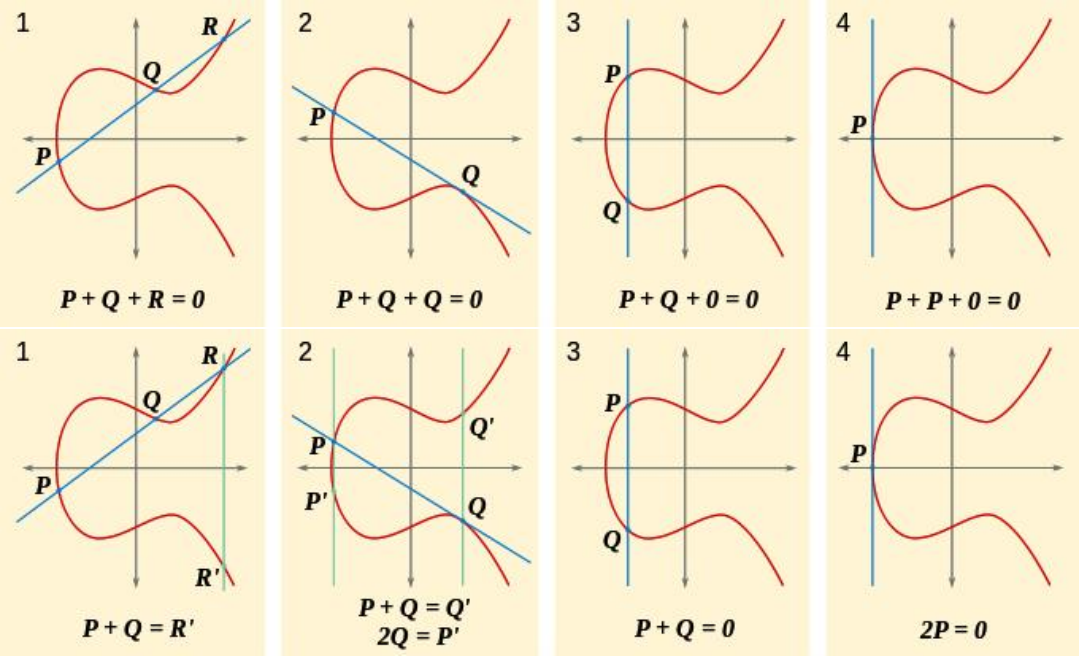
Az ábrákon látható néhány elliptikus görbe (és két, nem elliptikus görbe is) a következő paraméterválasztással:
Az első ábrán $a = -2 \quad b = -2, -1, 0, 1, \sqrt{\frac{2}{3}} \cdot \frac{4}{3}, 2$, így $b = \pm\sqrt{\frac{2}{3}} \cdot \frac{4}{3}$ esetén a görbe szinguláris lesz, itt a görbe átmetszi önmagát.
A második ábrán $a = 0 \quad b = -2, -1, 0, 1, 2.$ az $a = 0, b = 0$ paraméterválasztás jól láthatóan a $(0, 0)$ szinguláris pontot eredményezi.

4.3. Az elliptikus görbék csoporttulajdonsága

Egy kiválasztott elliptikus görbe pontjain bevezetjük az összeadás $(+)$ műveletet egy végtelenbeli pont hozzávételével a következőképpen:

50. Definíció. *[összeadás] A görbe P és Q pontjainak összege annak az R pontnak az R' inverze, amely a P-n és Q-n átmenő e egyenes és a görbe „harmadik" metszéspontja a következőképpen:*

- *ha az e egyenes három különböző pontban metszi a p görbét, akkor R a P-től és Q-tól különböző metszéspont ($P + Q + R = 0$)*
- *ha e érinti a görbét és $P \neq Q$, akkor R az érintési pont (és ezáltal vagy P-vel, vagy Q-val egybeesik) ($P + Q + Q = 0$)*
- *ha $P \neq Q$ és e párhuzamos az y tengellyel, akkor $R = 0$ a végtelenbeli pont ($P + Q + 0 = 0$)*
- *ha $P = Q$ és e párhuzamos az y tengellyel, akkor $R = 0$ ($P + P + 0 = 0$).*



3. Állítás. *[csoporttulajdonságok] A p elliptikus görbe pontjai az így definiált összeadásra nézve csoportot alkotnak.*

Bizonyítás.

- az összeadásra nézve triviálisan zárt
- az egységelem a végtelenbeli 0 pont
- P pont inverze a rajta átmenő, y tengellyel párhuzamos egyenes és a p görbe metszéspontja
- az asszociativitást nehéz feladat belátni, ezért most csak bizonyítás nélkül mondjuk ki

□

Az így definiált összeadásról könnyű látni, hogy kommutatív, hiszen sehol nem használtuk ki P és Q sorrendjét. A p elliptikus görbe pontjai tehát Abel-csoportot alkotnak az összeadásra nézve.

Az elliptikus görbe racionális pontjai részcsoportot alkotnak a definiált csoportban, ezt a tulajdonságot használják ki a kriptográfiai és prímfaktorizációs alkalmazásokban. A részcsoport máveleti zártságát az a meggondolás eredményezi, hogy ha egy valós együtthatós harmadfokú polinomnak létezik két racionális megoldása, akkor a harmadik megoldásnak is racionálisnak kell lennie.

Köszönetyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőmnek, Károlyi Gyulának, aki az ötletem alapján segített kiválasztani a dolgozatomban tárgyalt témákat. Külön hálás vagyok neki dolgozatom lektorálásáért és a tanácsokért, ötletekért.

Köszönöm Szabó Endre türelmes és alapos munkáját, amiért megismertetett a csoportelmélet alapjaival és szépségeivel.

Szeretném köszönetemet kifejezni családomnak és közeli barátaimnak a türelemért és támogatásért, amit tanulmányaim során nyújtottak, valamint amiért mellettem álltak és biztattak.

Irodalomjegyzék

[1] Babai László: Automorphism groups, isomorphism, reconstruction (Handbook of Combinatorics), 1994

[2] Bjorn Poonen: Elliptic curves, 2008

[3] Bojan Mohar: The Laplacian Spectrum of Graphs (Graph Theory, Combinatorics, and Applications), 1991

[4] C. Borgs, J. Chayes, L. Lovász, V.T. Sós and K. Vesztergombi: Counting Graph Homomorphisms, in: Topics in Discrete Mathematics, (ed. M. Klazar, J. Kratochvil, M. Loebl, J. Matousek, R. Thomas, P. Valtr), *Springer*, 2006

[5] Dietrich Kuske, Markus Lohrey: Logical Aspects of Cayley-Graphs: The Group Case (Annals of Pure and Applied Logic), 2005

[6] Dusan Djukić: Pell's Equation, *The IMO Compendium*, 2007

[7] Fan R. K. Chung: Spectral Graph Theory (CBMS Regional Conference Series in Mathematics), *Universtiy of Pennsylvania*, Philadelphia, 1997

[8] Hendrik W. Lenstra, JR.: Solving the Pell equation, 2008

[9] Harry Polard, Harold G. Diamond: The Theory of Algebraic Numbers, *The Mathematical Association of America*, 1975

[10] Igor Pak, Rados Radoičić: Hamiltonian Paths in Cayley Graphs, *Elsevier*, 2004

[11] J. Cheeger: A lower bound for the smallest eigenvalue of the Laplacian, *Princeton Univ. Press*, Princeton, 1970

[12] Kenneth Ireland, Michael Rosen: A Classical Introduction to Modern Number Theory (Graduate Texts in Mathematics Vol; 84) , *Springer-Verlag*, New York Heidelberg Berlin, 1982

[13] L. Lovász: Combinatorial structures and their applications, *Gordon and Breach*, New York, 1970

[14] P. Buser: A note on the isoperimetric constant (Annales Scientifiques de l'École Normale Supérieure), 1982

[15] Pelikán József, Gröller Ákos: Algebra jegyzet, http://www.cs.elte.hu/∼pelikan/algebra.html, 2000

[16] Robert B. Ash: Algebraic Number Theory, http://www.math.uiuc.edu/~r-ash/ANT.html

[17] Sheldon B. Akers, Balakrishnan Krishnamurthy: A Group-Theoretic Model for Symmetric Interconnection Networks, 1989

[18] http://en.wikipedia.org/wiki/Group_(mathematics)

[19] http://en.wikipedia.org/wiki/Rank_of_an_abelian_group

[20] http://dimax.rutgers.edu/~alexo/zemor.pdf

[21] http://hg8lhs.ham.hu/titkositas/ecc1.pdf

[22] http://homepage.mac.com/ehgoins/ma553/lecture_20.pdf

[23] http://math.mit.edu/~spielman/PAPERS/expandersIT.pdf

[24] http://mathworld.wolfram.com/CayleyGraph.html

[25] http://www.math.uwo.ca/~srankin/courses/403/2004/fund-theorem-abelian-groups.pdf

[26] http://www.math.ias.edu/~boaz/ExpanderCourse/lecture02.ps

[27] http://www.cs.huji.ac.il/~nati/PAPERS/expander_survey.pdf

Nyilatkozat

Név: Harkai Alexandra Dóra
ELTE TTK, Matematika B.Sc. szak, Matematikai elemző szakirány
ETR azonosító: HAANAAT.ELTE
Szakdolgozat címe: Csoportok a matematika különböző területein

A szakdolgozat szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló munkám eredménye, saját szellemi termékem, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2010. június 1.

Harkai Alexandra Dóra