Eötvös Loránd Tudományegyetem

Természettudományi Kar

Példák és ellenpéldák az algebrában

Szakdolgozat

Készítette:

Auffenberg András

Matematika BSc szakos hallgató

Témavezető:

Ágoston István

egyetemi docens

Budapest

2012

Tartalomjegyzék

1. fejezet

Bevezető

Az elmúlt néhány év alatt, miközben haladtam előre egyetemi tanulmányaimmal, egyre inkább azt vettem észre, hogy mind magamnak, mind azoknak, akikkel együtt tanultam szükségünk van arra, hogy a tanult tételeket kapcsolhassuk valamihez, és ne csak bemagolt mondatok halmazaként legyenek a fejünkben. Ennek egyik legjobb - és alighanem legegyszerűbb - módja a tételt igazoló illetve cáfoló példák megmutatása, természetesen a bizonyításon kívül. Az eddig tanultak alapján egyértelmű volt számomra, hogy szakdolgozatom alapvetően algebrai témájú lesz, hiszen a szerteágazó, sok nagy és már-már önálló területtel rendelkező matematika ezen ágának "gondolkodásmódja" áll hozzám legközelebb.

Szakdolgozatom célja, hogy néhány tétellel kapcsolatban rávilágítsak, hogy miért fontos minden benne szereplő feltétel vagy megmutassam, hogy a feltétel és a következmény szerepe felcserélhető.

Szerkezetileg a szakdolgozat úgy épül fel, hogy minden fejezet elején szerepel az ott tárgyalt állításokhoz kapcsolódó definíció, szükség esetén tétel is.

2. fejezet

Résznek része...

Amikor mélyebben foglalkozunk matematikával, különböző struktúrákkal kerülünk szembe, és hasznos, ha ismerjük ezek tulajdonságait. Egy adott struktúrát vizsgálva mindig felmerül a kérdés: vajon bővíthető-e vagy - a másik irányból szemlélve - van-e olyan rendszer, aminek ő része. Ebben a fejezetben adott struktúra részhalmazainak tulajdonságait vizsgáljuk.

Tudjuk, hogy egy adott vektortérben lévő altér altere altér a vektortérben, egy csoportban lévő részcsoport részcsoportja az eredeti csoportban is részcsoport és azt is tudjuk, hogy részgyűrű részgyűrűje a vizsgált gyűrűben is részgyűrűt alkot. Van azonban néhány speciális részhalmaz, amelyekre ez a tartalmazásnak nevezett reláció nem tranzitív, de meglepő vagy nem meglepő módon olyan is akad, hogy a feltételek további szigorításának következtében a reláció újra tranzitív lesz.

Elsőként egy speciális részcsoportot definiálunk, majd megmutatjuk, hogy ebben az esetben a tartalmazás nem tranzitív.

2.1. Definíció. *Egy $H \subseteq G$ nemüres részcsoport normális részcsoport (továbbiakban normálosztó) G-ben, ha zárt a konjugálás műveletére, amit úgy definiálunk, hogy minden $g \in G$ esetén $g^{-1}Hg \subseteq H$.*

2.2. Állítás. *Normálosztó normálosztója nem feltétlenül normálosztó.*

2.3. Példa. Tekintsük az A_4 alternáló csoportot. A csoport a következő elemekből áll: $A_4 = \{id, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$. Ebben normális részcsoportot, röviden normálosztót alkot az $N' = \{id, (12)(34), (13)(24), (14)(23)\}$ részcsoport, hiszen zárt a konjugálásra, ráadásul izomorf a Klein-csoporttal, melyről tudjuk, hogy benne bármely másodrendű elem részcsoportot, sőt, normálosztót alkot az identitással, azonban ez nem lesz normálosztó az A_4 csoportban. Vegyük ugyanis például az N' csoport $N = \{id, (12)(34)\}$ normálosztóját és az (123) harmadrendű elemet A_4-ből. Azt kell megvizsgálni, hogy a (321)(12)(34)(123) permutációszorzás eredménye benne van-e az N normálosztóban. Mivel $(321)(12)(34)(123) = (13)(24)$, ami nincs benne N-ben, így N nem normálosztó A_4-ben.

A normálosztó gyűrűelméleti "megfelelője" az ideál. Miután definiáltuk, az ideálról belátjuk, hogy ugyanaz igaz rá, mint a normálosztóra.

2.4. Definíció. *Egy $\mathcal{R}$ gyűrű $\mathcal{I}$ nemüres részhalmaza ideál, ha*

1. *$\mathcal{I}$ is gyűrű az $\mathcal{R}$-beli műveletek megszorításaira nézve,*
2. *zárt a külső elemmel való szorzásra, azaz $\forall r \in \mathcal{R}$ és $i \in \mathcal{I}$ esetén $ri \in \mathcal{I}$ és $ir \in \mathcal{I}$.*

2.5. Állítás. *Ideál ideálja nem feltétlenül ideál.*

2.6. Példa. Tekintsük azon 2×2-es felsőháromszög-mátrixok $\mathcal{R}$ gyűrűjét, melynek minden eleme racionális. Tehát az $\mathcal{R}$ gyűrű elemei az $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ alakú mátrixok, ahol $a, b, d, \in \mathbb{Q}$. Legyen $\mathcal{I} := \left\{ \begin{pmatrix} 0 & f \\ 0 & 0 \end{pmatrix} \;\middle|\; f \in \mathbb{Q} \right\}$. Ez az $\mathcal{I} \subseteq \mathcal{R}$ halmaz ideál $\mathcal{R}$-ben, ugyanis zárt az összeadásra, illetve a külső elemmel való szorzásra, vagyis $\begin{pmatrix} 0 & f \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & g \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & f+g \\ 0 & 0 \end{pmatrix} \in \mathcal{I}$, illetve $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} 0 & f \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & af \\ 0 & 0 \end{pmatrix}$. Az $\mathcal{I}$ ideálban pedig ideált alkot

a $\mathcal{J} := \left\{ \begin{pmatrix} 0 & f \\ 0 & 0 \end{pmatrix} \;\middle|\; f \in \mathbb{Z} \right\}$ részhalmaz, hiszen két egész szám összege is egész, és $\mathcal{I}$-beli elemmel való szorzás esetén pedig a nullmátrixot kapjuk. A $\mathcal{J} \lhd \mathcal{R}$ reláció nem igaz, ugyanis például $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{3}{2} \\ 0 & 0 \end{pmatrix}$, ami nem eleme $\mathcal{J}$-nek.

Fentebb megmutattuk, hogy normálosztó normálosztója nem feltétlenül normálosztó. Létezik egy - még a normálosztónál is speciálisabb - részcsoport, amelyre a tartalmazás tranzitív tulajdonsága újfent érvényes lesz, ez pedig a karakterisztikus részcsoport. Ehhez azonban még az automorfizmus definíciójára is szükségünk van.

2.7. Definíció. *Egy G csoporton értelmezett φ homomorfizmus automorfizmus, ha G-t önmagára képezi és bijektív. A G csoport automorfizmusait* $\mathrm{Aut}(G)$ *jelöli.*

2.8. Definíció. *Legyen G csoport. Egy $H \subseteq G$ halmaz akkor és csak akkor alkot karakterisztikus részcsoportot G-ben, ha bármely $\varphi \in \mathrm{Aut}(G)$ esetén $\varphi(H) \subseteq H$. Azt, hogy H karakterisztikus részcsoport G-ben, röviden úgy írjuk, hogy H char G.*

2.9. Állítás. *Karakterisztikus részcsoport karakterisztikus részcsoportja karakterisztikus részcsoport.*

Bizonyítás. Azt akarjuk tehát bizonyítani, hogy ha H *char* K *char* G, akkor H *char* G. Legyen $\varphi \in \mathrm{Aut}(G)$. A K karakterisztikus részcsoport G-ben, ezért $\varphi(K) \subseteq K$. Mivel φ bijektív, így φ^{-1} is automorfizmus és definíció szerint ekkor $\varphi^{-1}(K) \subseteq K$. Erre alkalmazva φ-t, kapjuk, hogy: $K \subseteq \varphi(K)$. Ebből az következik, hogy ha K *char* G, akkor $\varphi(K) = K$, vagyis G minden φ automorfizmusa K-nak is egy automorfizmusát adja. Emiatt leszűkíthetjük φ-t K-ra. Az így kapott $\varphi\big|_K$ automorfizmusa K-nak, tehát H-t H-ba viszi.

Végül még egy hasonló bizonyítás, ami a direkt tényezőre vonatkozik. Előbb - természetesen - ismét a definíció következik.

2.10. Definíció. *Egy H halmaz direkt tényező a G csoportban, ha:*

1. *H normálosztó G-ben*
2. *van olyan $\overline{H}$ normálosztó G-ben, hogy $H \cap \overline{H} = \{1\}$*
3. *$\langle H, \overline{H} \rangle = G$, ahol $\langle H, \overline{H} \rangle = \{h\overline{h} \mid h \in H, \overline{h} \in \overline{H}\}$.*

2.11. Állítás. *Direkt tényező direkt tényezője direkt tényező.*

Bizonyítás. A bizonyítás során azt, hogy a H halmaz direkt tényező a G csoportban, úgy jelöljük, hogy: $H \overset{\oplus}{\leq} G$. Azt kell tehát bizonyítani, hogy: $K \overset{\oplus}{\leq} H \overset{\oplus}{\leq} G \Rightarrow K \overset{\oplus}{\leq} G$. A 2.10 Definíció szerint a $K \overset{\oplus}{\leq} H$ azt jelenti, hogy van olyan $\overline{K}$, hogy $K, \overline{K} \lhd H,\ K \cap \overline{K} = \{1\}$ és $K \cdot \overline{K} = H$, az pedig, hogy $H \overset{\oplus}{\leq} G$, azt jelenti, hogy van olyan $\overline{H}$, hogy $H, \overline{H} \lhd G,\ H \cap \overline{H} = \{1\}$ és $H \cdot \overline{H} = G$. Azt szeretnénk bizonyítani, hogy van olyan $\overline{\overline{K}}$, hogy $K, \overline{\overline{K}} \lhd G,\ K \cap \overline{\overline{K}} = \{1\}$ és $K \cdot \overline{\overline{K}} = G$.
Válasszuk a $\overline{\overline{K}}$-t $\overline{K} \cdot \overline{H}$-nak. Először lássuk be, hogy $K \lhd G$. Mivel $G = H \cdot \overline{H}$, ezért tetszőleges $g \in G$ elemet felírhatunk $g = h \cdot \overline{h}$ alakban, ahol $h \in H$ és $\overline{h} \in \overline{H}$, így $g^{-1}kg = (h\overline{h})^{-1}kh\overline{h} = (\overline{h})^{-1}h^{-1}kh\overline{h}$. Itt $h^{-1}kh \in K \subseteq H$, hiszen tudjuk, hogy $K \lhd H$. Mivel diszjunkt normálosztók elemei felcserélhetők, ezért $(\overline{h})^{-1}h^{-1}kh\overline{h} = (\overline{h})^{-1}\overline{h}h^{-1}kh$. Ez $h^{-1}kh$, ami eleme K-nak. Így K valóban normálosztó G-ben.
Most mutassuk meg, hogy $\overline{K} \cdot \overline{H} \lhd G$. Az előzőekben bizonyítottakhoz hasonlóan $\overline{K} \lhd G$, s emiatt $\overline{K} \cdot \overline{H} \lhd G$, hiszen ha veszünk egy $\overline{k} \cdot \overline{h} \in \overline{K} \cdot \overline{H}$ elemet, akkor $g^{-1}(\overline{kh})g = g^{-1}\overline{k}gg^{-1}\overline{h}g \in \overline{K} \cdot \overline{H}$, ugyanis $g^{-1}\overline{k}g \in \overline{K}$, illetve $g^{-1}\overline{h}g \in \overline{H}$.
Lássuk most be, hogy $K \cap \overline{K} \cdot \overline{H} = \{1\}$. Tegyük fel, hogy $k = \overline{kh}$ valamely $k \in K$, illetve $\overline{k} \in \overline{K}$ és $\overline{h} \in \overline{H}$ elemekre. Szorozzuk meg az egyenlet mindkét oldalát balról $(\overline{k})^{-1}$-zel. Ekkor azt kapjuk, hogy $(\overline{k})^{-1}k = (\overline{k})^{-1}\overline{kh} = \overline{h}$. Itt $(\overline{k})^{-1}k \in H$, hiszen $K \cdot \overline{K} = H$, illetve $\overline{h} \in \overline{H}$. Ez azt jelenti, hogy találtunk egy elemet, mely eleme H-nak, és $\overline{H}$-nak is. Amiatt, hogy $H \cap \overline{H} = 1$, így $(\overline{k})^{-1}k = 1$, amiből $k = \overline{k}$ adódik. Mivel $k \in K$, illetve $\overline{k} \in \overline{K}$ és $K \cap \overline{K} = 1$, ezért $k = 1$.

Utolsó részállításunk, amit be kell látni: $K \cdot \overline{K} \cdot \overline{H} = G$. Ez könnyen belátható, hiszen $K \cdot \overline{K} = H$ és $H \cdot \overline{H} = G$, és máris a kívánt állítást kapjuk.

Sok hasonló jellegű állítás írható fel, mind pozitív, mind negatív eredmény szempontjából, ez csak egy kisebb válogatás azokból, amelyeket érdekesebbnek tartottam.

3. fejezet

Csoportelmélet

A csoportelmélet az algebra egyik legtöbb helyen használható ága, sok nevezetes - és nem is túl bonyolult - tétellel. Többek között a számelméleti Euler-Fermat-tétel az egyik legalapvetőbb csoportelméleti tételen alapszik, amely az olasz születésű francia matematikus Joseph-Louis Lagrange (eredeti nevén Giuseppe Luigi Lagrangia) nevéhez fűződik.

3.1. Tétel. *Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.*

Ennek a tételnek van egy rendkívül hasznos következménye.

3.2. Következmény. *Minden elem rendje osztója a csoport rendjének.*

Most megmutatjuk, hogy a tétel megfordítása nem igaz.

3.3. Állítás. *Ha egy G csoport rendje n és k osztója n-nek, abból nem következik, hogy van k-rendű részcsoport G-ben.*

3.4. Példa. Legyen $G = A_4$. Az A_4 csoport rendje 12, tehát a 3.1 Tétel miatt egy $H \subseteq A_4$ részcsoport lehetséges rendjei a triviálisaktól eltekintve: $2, 3, 4, 6$. Azt, hogy negyedrendű és másodrendű részcsoport létezik A_4-ben, már láttuk a 2.3 Példában. Egy harmadrendű részcsoportban az identitáson kívül két darab harmadrendű elem lehet, és mivel a részcsoportban benne kell lennie minden elem inverzének, így egy lehetséges harmadrendű részcsoport

a $H_3 = \{id, (123), (132)\}$. Hatodrendű részcsoport azonban nincs A_4-ben. Ha ugyanis lenne hatodrendű részcsoport, akkor az indexe 2 lenne, tehát normálosztót kapnánk, vagyis zártnak kellene lennie a konjugálásra. Két fajta szerkezete lehetne az elemrendek alapján:

1. egy másodrendű és négy harmadrendű elem
2. három másodrendű és két harmadrendű elem.

Az 1. esetben - az általánosság megszorítása nélkül - legyen az egyik harmadrendű elem (abc). Ezt konjugálva 3 olyan elemmel amelyek sem (abc)-nek sem egymásnak nem inverzei, az adódik, hogy:

- $(abd)(abc)(adb) = (dcb)$
- $(acd)(abc)(adc) = (dcb)$
- $(bcd)(abc)(bdc) = (dac)$,

vagyis bármely elemekkel konjugálva a kiválasztott (abc) elemet, nem az (acb), vagy a választott (abc) permutációt kapjuk, pedig ahhoz, hogy csoport legyen, ennek benne kell lennie, így több mint 4 harmadrendű elemet tartalmazna a csoport. Ez tehát ellentmondás. A 2. esetben szintén tekintsük az egyik harmadrendű elemet és legyen ez most is (abc). Ekkor a másik harmadrendű elem szükségképpen (bac), hiszen részcsoport zárt az inverzképzésre. Az (abc) elemmel jobbról megszorozva a 3 másodrendű elemet:

- $(ab)(cd)(abc) = (bdc)$
- $(ac)(bd)(abc) = (adb)$
- $(ad)(bc)(abc) = (acd)$,

elemek adódnak, melyek egyike sincs benne a részcsoportban, így ilyen szerkezetű hatodrendű részcsoport sem létezik A_4-ben.

Ha ismerjük egy csoport elemszámát, vagy egy adott csoport elemeinek rendjét, akkor gyakran következtethetünk a csoport bizonyos tulajdonságaira. Jöjjön most 3 ilyen jellegű tétel; először megnézzük mit állíthatunk egy csoportról, ha benne minden elem négyzete 1, majd megvizsgáljuk azt az esetet, ha a csoport rendje p^2, végül pedig rátérünk arra, hogy mit mondhatunk biztosan két olyan csoportról, melyek izomorfak egymással.

3.5. Tétel. *Legyen G egy csoport. Ha minden $g \in G$ esetén $g^2 = 1$, akkor a csoport kommutatív.*

Bizonyítás. Legyen $g, h \in G$. Ekkor $gh \in G$, így $ghgh = 1$. Ebből mindkét oldalt balról g-vel szorozva $gghgh = g$ adódik, majd jobbról h-val szorozva kapjuk, hogy $gghghh = gh$, azaz $hg = gh$, amit bizonyítani akartunk.

Mielőtt rátérnénk a p^2 rendű csoportokkal kapcsolatos tételre, szükségünk lesz néhány fogalomra és állításra.

3.6. Definíció. *Egy G csoportban az a és b elemeket akkor nevezzük konjugáltaknak, ha van olyan $g \in G$, melyre $gag^{-1} = b$, vagyis ha van olyan konjugálás, amely az a elemet a b-be viszi. Ennek az ekvivalenciarelációnak az osztályait a csoport konjugáltosztályainak nevezzük.*

3.7. Definíció. *Legyen G csoport. Egy $x \in G$ elem centralizátorának nevezzük és $C_G(x)$-szel jelöljük G-nek azt a részcsoportját, melynek elemei x-szel felcserélhetők, azaz*

$$C_G(x) = \{a \in G \mid ax = xa\}.$$

3.8. Következmény. *Egy $x \in G$ konjugáltosztályának elemszáma az x centralizátorának az indexe. Szimbólumokkal kifejezve:*

$$[x] = |G : C_G(x)|.$$

Bizonyítás. Az, hogy $a, b \in G$ az x elemnek ugyanazt a konjugáltját eredményezik, azzal ekvivalens, hogy:

$$a^{-1}xa = b^{-1}xb.$$

Balról b-vel, jobbról pedig b^{-1}-gyel szorozva

$$ba^{-1}xab^{-1} = x$$

adódik. Most balról ab^{-1}-gyel szorozva azt kapjuk, hogy:

$$xab^{-1} = ab^{-1}x.$$

Ez a 3.7 Definíció szerint éppen azt jelenti, hogy $ab^{-1} \in C_G(x)$.
Tehát $C_G(x)ab^{-1} = C_G(x)$, azaz $C_G(x)a = C_G(x)b$, vagyis a és b ugyanabba a $C_G(x)$ szerinti mellékosztályba esik. Mivel mindvégig ekvivalens átalakításokat végeztünk, azt mondhatjuk, hogy az $a, b \in G$ elemek pontosan akkor adják az x elemnek ugyanazt a konjugáltját, ha ugyanabba az x szerinti mellékosztályba esnek.

3.9. Definíció. *Egy G csoport $Z(G)$-vel jelölt centrumát azon elemek alkotják, melyek bármely más csoportbeli elemmel felcserélhetők. Jelölésekkel:*

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

3.10. Állítás. *Ha $|G| = p^\alpha$ és $\alpha \geq 1$, akkor $|Z(G)| > 1$.*

Bizonyítás. A G csoport elemszáma konjugáltosztályai elemszámának összege. Az egyelemű konjugáltosztályok épp a centrum elemeinek felelnek meg, tehát nyilván annyian vannak, mint a centrum elemszáma. A többi konjugáltosztály legyen $K_1, \ldots, K_m$. Ekkor

$$|G| = |Z(G)| + |K_1| + \cdots + |K_m|.$$

Tudjuk, hogy K_i elemszáma - ami tetszőleges eleme centralizátorának az indexe - osztója G rendjének, ami p-nek hatványa. Emiatt K_i elemszáma is p-hatvány. Mivel $|K_i| > 1$, - ugyanis csak a centrum elemei alkotnak egyelemű konjugáltosztályt - így $p \mid |K_i|$. Mivel G nem az egyelemű csoport, így $p \mid |G|$. A fenti egyenletből adódik, hogy $|Z(G)|$ is osztható p-vel, tehát nem lehet egyelemű.

Most már kimondhatjuk, hogy mi következik abból, ha egy csoport p^2 rendű.

3.11. Tétel. *Ha G olyan csoport, melynek rendje p^2, akkor G kommutatív.*

Bizonyítás. Az előző állítás miatt $|Z(G)| > 1$. Tehát $|Z(G)| = p$ vagy $|Z(G)| = p^2$. Utóbbi esetben kész vagyunk, hiszen $Z(G)$ definíció szerint kommutatív. Az első esetben vizsgáljuk a $G/Z(G)$ faktorcsoportot. Nyilvánvaló, hogy $|G/Z(G)| = p$. Így ciklikus, mivel prímrendű csoport mindig ciklikus. Tehát létezik olyan $a \in G$, hogy

$$G = Z(G) \cup Z(G)a \cup Z(G)a^2 \cup \cdots \cup Z(G)a^{p-1}.$$

Ebből következően G minden eleme felírható egy centrumbeli elem és a valamelyik hatványának szorzataként, azaz:

$$\forall g \in G : \exists z \in Z(G), k \in \{0, \ldots, p-1\},$$

hogy $g = z \cdot a^k$.
Most vizsgáljuk meg G kommutativitását. Legyen $g = z \cdot a^k$ és $h = w \cdot a^l$, ahol $g, h \in G$ és $z, w \in Z(G)$. A gh szorzatból kiindulva:

$$gh = z \cdot a^k \cdot w \cdot a^l = z \cdot w \cdot a^{k+l} = w \cdot z \cdot a^{k+l} = w \cdot a^l \cdot z \cdot a^k = hg$$

adódik. Eszerint G bármely két eleme felcserélhető egymással, vagyis azt kaptuk, hogy $G = Z(G)$. Azonban ez ellentmondás, hiszen abból indultunk ki, hogy $|G| = p^2$, illetve $|Z(G)| = p$.

Amikor két csoportról el akarjuk dönteni, hogy izomorfak-e egymással, több szempontból kell őket megnéznünk. Nyilvánvaló, hogy az elemszámuk egyenlő kell legyen. Kell az is, hogy mindkét csoportban ugyanolyan legyen az elemrendek rendszere. Ennek vizsgálatát azonban célszerű akkorra hagyni, ha semmi sem segített eldönteni az izomorfiát, hiszen ha mondjuk két 100 elemű csoport elemeinek rendszerét kell összevetni, az igen időigényes, és könnyen hibázhatunk közben. Második lépésként tehát érdemes a csoportok tulajdonságait ellenőrizni, mint például a kommutativitás, hiszen evidens,

hogy nem lehet izomorf két olyan csoport, melyek közül az egyikben kommutatív a csoportművelet, a másikban pedig nem.

3.12. Tétel. *Ha két csoport izomorf egymással, akkor elemszámuk egyenlő és bennük az elemek rendje megegyezik.*

Most kimondunk 3 állítást, melyek azt mutatják, hogy az előzőekben tárgyalt 3 tétel miért nem általánosítható, illetve miért nem fordítható meg.

3.13. Állítás. *Van olyan G csoport, hogy minden $g \in G$ esetén $g^3 = 1$, de G nem kommutatív.*

3.14. Állítás. *Van olyan G csoport, hogy $|G| = p^3$, de G nem kommutatív.*

3.15. Állítás. *Vannak olyan G és H csoportok, melyek elemszáma egyenlő, és ugyanolyan bennük az elemrendek rendszere, mégsem izomorfak egymással.*

Az előző 3 állításra egyetlen példát mutatunk.

3.16. Példa. Tekintsük azokat a 3×3-as felső háromszög mátrixokat, amelyek főátlójában csupa 1 áll, a többi helyen pedig $\mathbb{Z}_3$ elemei. Tehát egy tetszőleges $g \in G$ elem

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

alakú, ahol $a, b, c \in \mathbb{Z}_3$. A csoport egységeleme az:

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

mátrix. Az összes többi elem rendje 3, hiszen:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix},$$

valamint

$$\begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

a csoport elemszáma pedig 27, hiszen az a, b, c elemek mindegyikét háromféleképpen választhatjuk, s így $3^3 = 27$ elemet kapunk.
Ha a csoport egy tetszőleges elemét megszorozzuk egy tőle különbözővel jobbról, illetve balról akkor az

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix},$$

illetve az

$$\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$$

elemeket kapjuk. A kapott elemek akkor egyenlőek, ha $af = dc$. Ez nem teljesül például, ha a-t, f-et, d-t 1-nek, és c-t 0-nak választjuk.
Megmutattuk tehát, hogy bár a csoport elemeinek rendje 3, és a csoport rendje is egy prím harmadik hatványa, mégsem kommutatív. Most mutatunk egy olyan csoportot, ami szintén 27 elemű, elemeinek rendje 3, de az előző csoporttal ellentétben kommutatív. Ez a H csoport legyen a $(\mathbb{Z}_3^+)^3$, vagyis $H := \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Az elemszám ebben az esetben is $3^3 = 27$, az egységelem kivételével pedig szintén minden elem harmadrendű a csoportban, hiszen a 3.2 Következmény miatt az elemrendek csak 1, illetve 3 lehetnek, az pedig szintén ismeretes, hogy csak az egységelem rendje 1.
Hiába egyezik tehát meg a két csoportban az elemek rendje és ugyanolyan bennük az elemrendek rendszere, mégsem izomorfak egymással, hiszen mutattunk egy olyan csoporttulajdonságot - a kommutativitást -, amely az egyik csoportban teljesül, a másikban nem.

4. fejezet

Polinomok

Középiskolai tanulmányaink során azt tanuljuk a polinomokról, hogy éppen annyi gyökük van, mint amennyi a fokuk. Következzen most néhány olyan példa, ahol ez nem teljesül.

4.1. Állítás. *Ha az R gyűrűben vannak $\alpha \neq \beta$ nem nulla elemek, melyekre $\alpha\beta = 0$, akkor van olyan másodfokú polinom $R[x]$-ben, amelynek kettőnél több gyöke van.*

Bizonyítás. Tekintsük a $p(x) = \alpha(x - \beta)(x - \beta - 1)$ polinomot. Ennek a polinomnak egyaránt gyöke a 0, a β és a $\beta + 1$. (Itt $\beta + 1 \neq 0$, mert -1 nem lehet nullosztó.) Tehát $p(x)$-nek legalább három különböző gyöke van.

4.2. Példa. A $2x^2 + 2x$ polinomnak $\mathbb{Z}_4[x]$-ben minden $\mathbb{Z}_4$-beli elem gyöke. Ha pedig pl. $\mathbb{Z}_6[x]$-ben keresünk ilyen polinomot, ott $(x-2)(x-3)$-nak gyöke lesz a $0, 2, 3, 5$ elemek mindegyike.

A fenti példákban láthattuk, hogy ha a polinomot gyöktényezők szorzatára bontjuk, abból nem következik, hogy a polinomnak csak a gyöktényezőkben szereplő konstansok lehetnek a gyökei. A nullosztók jelenléte miatt most egy szorzat úgy is lehet nulla, ha egyik tényezője sem volt nulla.

Most megmutatjuk, hogy a gyökök számának meghatározása nemcsak nullosztót tartalmazó gyűrűben jelenthet gondot. Ugyanis ha az alapgyűrű nem kommutatív, akkor az okozhat problémát, hogy a polinom kanonikus

alakjába való behelyettesítés és a gyöktényezős alakba való behelyettesítés különböző értékeket eredményezhetnek, mivel az alapgyűrű nem kommutatív, és a behelyettesítés így nem (feltétlenül) szorzattartó.

4.3. Állítás. *A $\mathbb{H}$ kvaterniótestben az $f(x) = x^2 + 1$ polinomnak 2-nél több gyöke van.*

Bizonyítás. Behelyettesítéssel könnyen ellenőrizhető, hogy f-nek gyöke lesz az $i, -i, j, -j, k, -k$ elemek mindegyike, tehát máris van legalább 6 gyökünk. Azt sem túl nehéz azonban igazolni (lásd pl. [5] könyv 331-332. oldal), hogy az f-nek minden olyan $\alpha i + \beta j + \gamma k$ kvaternió gyöke lesz, melynél az $\alpha, \beta, \gamma \in \mathbb{R}$ együtthatókra teljesül, hogy $\alpha^2 + \beta^2 + \gamma^2 = 1$. (Sőt, az is igaz, hogy csak az ilyen alakú kvaterniók lesznek gyökei az f polinomnak.) Ez azt mutatja, hogy ennek a másodfokú polinomnak végtelen sok gyöke van $\mathbb{H}$-ban.

Tehát egy polinom gyökeinek száma és a polinom foka között az alábbi összefüggés áll fenn biztosan:

4.4. Tétel. *Kommutatív, nullosztómentes gyűrű feletti polinomnak legfeljebb annyi gyöke van, mint a foka.*

Szintén középiskolában tanultunk a prímszámokról. Itt prímszám alatt olyan egész számot értettünk, melyet csak az 1 illetőleg önmaga oszt. A polinomok körében is létezik ez a fogalom, ami azt mondja el egy polinomról, hogy van-e olyan polinom, - az 1 polinomon és önmagán kívül - amivel maradék nélkül osztható, vagyis, amely segítségével szorzattá bontható. Ha egy racionális együtthatós polinom csak triviálisan bomlik fel, akkor irreducibilisnek mondjuk. Az irreducibilitás vizsgálata fontos szerepet játszik a polinomok elméletében. Az egyetemi tanulmányok során több szempontból is vizsgáltuk ezt a kérdést. Az irreducubilitás általában függ attól, hogy milyen együtthatótartomány felett vizsgáljuk egy polinom irreducibilitását. Bizonyos esetekben a kérdés egyszerűen eldönthető (pl. $\mathbb{C}[x]$-ben), néha kicsit nehezebben (pl. a valós együtthatójú polinomok között). A legnehezebbnek azonban a $\mathbb{Q}[x]$, illetve, ami ezzel egyenértékű, a $\mathbb{Z}[x]$ feletti vizsgálat

bizonyult. A fejezet további részében különböző módszereket, kritériumokat mutatunk, amelyek valamelyike szinte biztosan segít eldönteni egy adott polinomról, hogy irreducibilis-e vagy sem.

Egyik legismertebb eszközünk a Schönemann-Eisenstein-kritérium volt. Idézzük föl tehát a kritériumot.

4.5. Definíció. *Egy $f(x)$ egész együtthatós polinomról azt mondjuk, hogy Eisenstein-alakú egy p prímre nézve, ha*

$$f(x) = \sum_{j=0}^{n} a_j x^j = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_n x + a_0,$$

és $p \nmid a_n$, $p \mid a_j$, ha $j < n$ és $p^2 \nmid a_0$.

Ekkor a közismert Schönemann–Eisenstein-kritérium a következőt mondja ki.

4.6. Állítás. *Ha egy egész együtthatós polinom Eisenstein alakú valamilyen p-re, akkor irreducibilis $\mathbb{Q}$ felett.*

A következő példa mutatja, hogy a prím kiválasztása figyelmet igényel.

4.7. Példa. Tekintsük az $f(x) = 3x^6 - 84x^4 + 168x^3 - 210x - 112$ polinomot. Mivel - a főegyüttható kivételével - minden együttható páros, ezért célszerű elsőként a $p = 2$ lehetőséggel próbálkozni. Ekkor $p \nmid a_n$ és $p \mid a_j$, ha $j < n$ teljesül, azonban $p^2 \mid a_0$ és így a $p = 2$ nem jó választás. Nézzük a $p = 3$ esetet. Ekkor $p \mid a_n$ és így a másik két feltétel hiába teljesül ez sem jó prím. A $p = 5$ esetnél azzal a feltétellel van probléma, hogy $p \mid a_j$, ha $j < n$. A megoldást a $p = 7$ eset adja, hiszen 7 a főegyüttható kivételével minden együtthatónak osztója és $7^2 = 49$ nem osztója 112-nek.

Nyilván nem minden egész együtthatós polinom lesz Eisenstein alakú, ami $\mathbb{Q}[x]$-ben irreducbilis. Ilyenkor – ha tehát a fenti kritérium nem működik – gyakran alkalmazzuk a modulo p vizsgálatot.

4.8. Tétel. *Legyen $f(x)$ egész együtthatós polinom, és legyen p prím olyan, amely nem osztja az f főegyütthatóját. Jelölje $\bar{f}(x)$ azt a $\mathbb{Z}[x]$-beli polinomot, melyet úgy kapunk, hogy az f együtthatóit modulo p vesszük. Ha $\bar{f}(x)$ irreducibilis $\mathbb{Z}_p$ fölött, akkor $f(x)$ irreducibilis $\mathbb{Z}[x]$ fölött.*

4.9. Példa. Legyen $f(x) = 25x^4 + 8x^3 + 13x^2 + 7$. Ekkor a polinom nem Eisenstein alakú, és mivel negyedfokú, nem is elég csak egyszerűen azt megmutatni, hogy nincsenek racionális gyökei (amit könnyen megtehetnénk a racionális gyöktesztttel). Ugyanakkor vizsgálhatjuk a polinomot modulo p. Nézzük először a $p = 2$ esetet. Ekkor $\bar{f}(x) = x^4 + x^2 + 1$, ami nem irreducibilis, hiszen jól ismert az a tétel, hogy $\mathbb{Z}_p$ fölött tagonként lehet p-edik hatványra emelni, ezért $\bar{f}(x) = (x^2+x+1)^2$ mint $\mathbb{Z}_2[x]$-beli polinom. A $p = 3$ esetben, azaz ha $\bar{f}(x) \in \mathbb{Z}_3[x]$, az $\bar{f}(x) = x^4 + 2x^3 + x^2 + 1$ polinomot kapjuk. Ez a polinom irreducibilis: ehhez először meg kell mutatni, hogy nincs gyöke $\mathbb{Z}_3$-ban, ami egyszerű behelyettesítéssel elvégezhető, majd maradékos osztással ellenőrizhetjük azt is, hogy $\bar{f}(x)$-nek nem osztója $\mathbb{Z}_3[x]$ normált, másodfokú irreducibilis polinomjainak - $x^2 + 1$, $x^2 + x + 2$ és $x^2 + 2x + 2$ - egyike sem. Mivel $\bar{f}(x)$ irreducibilis $\mathbb{Z}_3[x]$-ben, ezért $f(x)$ is irreducibilis $\mathbb{Z}[x]$-ben is.

Sajnos, még ez sem tökéletes módszer az irreducibilitás ellenőrzésére. Mutatunk ugyanis olyan $f \in \mathbb{Z}[x]$ polinomot, amely irreducibilis ugyan $\mathbb{Z}[x]$-ben, de $\bar{f}(x)$ egyetlen p prímre sem lesz irreducibilis $\mathbb{Z}[x]$-ben.

Ehhez először idézzük föl a kvadratikus maradék fogalmát.

4.10. Definíció. *Legyen $p > 2$ prím és $(a, p) = 1$. Az a számot aszerint nevezzük kvadratikus maradéknak, illetve kvadratikus nemmaradéknak modulo p, hogy az $x^2 \equiv a \pmod{p}$ kongruencia megoldható-e, vagy sem.*

Készen állunk a jelzett példa bemutatásához.

4.11. Állítás. *Az $x^4 - x^2 + 1$ polinom irreducibilis $\mathbb{Z}$ felett, de minden p-re reducibilis modulo p.*

Bizonyítás. Legyen $q(x) = x^4 - x^2 + 1$. Először azt mutatjuk meg, hogy $q(x)$ irreducibilis $\mathbb{Z}[x]$ fölött. Polinomok szorzásakor a fokszámok összeadódnak, ezért egy negyedfokú polinom vagy egy első- és egy harmadfokú, vagy két másodfokú polinom szorzatára bomlik, vagy pedig irreducibilis. A $q(x)$ polinomnak nincs elsőfokú faktora, hiszen a racionális gyökteszt miatt minden gyök osztja a konstans tagot, ami azt jelenti, hogy az adott polinom lehetséges gyökei az 1 és a -1. Ezekről azonban behelyettesítéssel könnyen láthatjuk, hogy nem gyökei $q(x)$-nek. Most nézzük meg, hogy felbomlik-e két másodfokú egész együtthatós polinom szorzatára, azaz léteznek-e olyan ax^2+bx+c és dx^2+ex+f polinomok, hogy $(ax^2+bx+c)(dx^2+ex+f) = x^4-x^2+1$. Ebből $ad = 1$, $cf = 1$, $ae + bd = 0$ és $af + cd + be = -1$ adódik. Az $ad = 1$ miatt $a = d = \pm 1$. Mindkét esetben $e = -b$. Mivel $cf = 1$ miatt $c = f = \pm 1$, így $af = cd = \pm 1$. Az eddig nem használt egyenlőség tehát kétféleképp írható fel: $2 - b^2 = -1$, vagy $-2 - b^2 = -1$. Előbbiből $b^2 = 3$, míg utóbbiból $b^2 = -1$ adódik. Egyik sem lehetséges, hiszen $b \in \mathbb{Z}$, tehát $q(x)$ irreducibilis $\mathbb{Z}[x]$ felett. Most megmutatjuk, hogy $q(x)$ minden p-re reducibilis modulo p. Először is a $p = 2$ esetben $q(x) = (x^2+x+1)^2$, így a továbbiakban feltehetjük, hogy $p > 2$. (Ez azért kell, mert 2-vel, illetve 4-gyel szeretnénk majd osztani.) Alakítsuk át kétféleképpen a $q(x)$ polinomot, hogy két jól ismert azonosságot láthassunk benne. Tekintsük először azt, hogy $q(x) = x^4 - 2x^2 + 1 + x^2$. Innen $(x^2-1)^2 + x^2 = (x^2-1)^2 - (-x^2)$. Ha $-1 \equiv a^2 \pmod{p}$, akkor kapjuk, hogy $(x^2-1)^2 - (a^2x^2) = (x^2 - 1 - ax)(x^2 - 1 + ax)$. A másik átalakítási lehetőség: $x^4 + 2x^2 + 1 - 3x^2$, amiből $(x^2+1)^2 - 3x^2$ adódik. Ha $3 \equiv b^2 \pmod{p}$, akkor ebből $(x^2+1)^2 - b^2x^2 = (x^2 + 1 - bx)(x^2 + 1 + bx)$. Ha sem a -1 sem a 3 nem kvadratikus maradék modulo p, akkor viszont a szorzatuk az kell legyen. Ekkor pedig $q(x)$-et bontsuk fel $x^4 - x^2 + 4^{-1} + 3 \cdot 4^{-1}$ alakra. Legyen $a = 4^{-1}$ és $b = 2^{-1}$, így $b^2 = a$. Ezt beírva $q(x)$-be és néhány átalakítást végezve és felhasználva, hogy $-3 \equiv c^2 \pmod{p}$ kapjuk, hogy $x^4-x^2+b^2+3b^2 = (x^2-b)^2+3b^2 = (x^2-b)^2-(c^2b^2) = (x^2-b-cb)(x^2-b+cb)$.

A fenti példa jól demonstrálja, hogy egy egész együtthatós polinomnál lehet, hogy nem elég azt vizsgálni, vajon irreducibilis-e modulo p. A követ-

kező példa azt mutatja, hogy előfordulhat, hogy még ilyenkor is eldönthető az irreducibilitás. Azt kell megnézni, hogy ha $\bar{f}$ nem irreducibilis modulo p, akkor milyen irreducibilis faktorok szorzatára bomlik. Ha különböző prímekre különbözők a lehetséges tenyezők fokai, akkor ezek nem származhatnak $\mathbb{Z}[x]$-beli fölbontásból, így az eredeti polinomunk irreducibilis.

4.12. Példa. Konstruáljunk meg egy $f(x) \in \mathbb{Z}[x]$ polinomot úgy, hogy $p = 2$ és $q = 3$ esetén különbözőképpen bomoljon föl $\bar{f}(x)$ irreducibilisek szorzatára. Ehhez vegyünk $\mathbb{Z}_2$-ben egy első- és egy negyedfokú irreducibilis polinomot. Legyenek ezek $g_1(x) = x + 1$ és $g_4(x) = x^4 + x^3 + 1$. Az irreducibilitásuk gyorsan ellenőrizhető: behelyettesítve a 0-t és az 1-et látjuk, hogy egyik sem gyök. A $g_4(x)$ még felbomolhatna két irreducibilis másodfokú polinom szorzatára, ez csak az $x^2 + x + 1$ polinom önmagával vett szorzata lehetne, azonban $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, ami nem egyenlő $g_4(x)$-szel.
Ezután vegyünk $\mathbb{Z}_3$-ban egy másod- és egy harmadfokú irreducibilis polinomot. Jelölje ezeket $h_2(x)$ és $h_3(x)$. Legyen $h_2(x) = x^2 + 1$. Ez irreducibilis, hiszen ha nem lenne az, akkor a fentebb leírtak miatt lenne gyöke $\mathbb{Z}_3[x]$-ben. A harmadfokú $h_3(x) = x^3 + x^2 + 2$ polinomra ugyanez igaz. Behelyettesítéssel mindkét polinomnál látható, hogy egyiknek sincs gyöke $\mathbb{Z}_3$-ban.
A $\mathbb{Z}_2[x]$-beli polinomok szorzata $g(x) = x^5 + x^3 + x + 1$, a $\mathbb{Z}_3[x]$-beliek szorzata pedig $h(x) = x^5 + x^4 + x^3 + 2$. Keressünk most egy olyan $f(x) \in \mathbb{Z}[x]$ polinomot, amely $\mathbb{Z}_2$ felett a $g(x)$ és $\mathbb{Z}_3$ felett a $h(x)$ polinomot adja. Az $f(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f$ együtthatóinak kiszámításához a következő kongruenciarendszereket kell megoldani:

$$\begin{aligned}
a &\equiv 1 \pmod 2 \quad \text{és} \quad a \equiv 1 \pmod 3 \\
b &\equiv 0 \pmod 2 \quad \text{és} \quad b \equiv 1 \pmod 3 \\
c &\equiv 1 \pmod 2 \quad \text{és} \quad c \equiv 1 \pmod 3 \\
d &\equiv 0 \pmod 2 \quad \text{és} \quad d \equiv 0 \pmod 3 \\
e &\equiv 1 \pmod 2 \quad \text{és} \quad e \equiv 0 \pmod 3 \\
f &\equiv 1 \pmod 2 \quad \text{és} \quad f \equiv 2 \pmod 3.
\end{aligned}$$

Ennek a rendszernek az egyik megoldása adja a következő $f(x)$ polinomot:

$f(x) = x^5+4x^4+x^3+6x^2+3x+5$. Az $f(x)$ polinom irreducibilitása tehát abból adódik, hogy a $\mathbb{Z}_2$ feletti faktorok fokai különböznek a $\mathbb{Z}_3$ feletti faktorok fokaitól, így nem származhatnak ugyanabból a $\mathbb{Z}[x]$-beli felbontásból.

Térjünk most vissza a Schönemann–Eisenstein-kritériumhoz. A kritériumot általánosabban is megfogalmazhatjuk.

4.13. Definíció. *Egy $g(x)$ polinomot Eisenstein-polinomnak nevezünk, ha létezik olyan a egész szám, hogy $g(x+a)$ Eisenstein alakú valamilyen p prímre nézve.*

Megfogalmazható az ún. eltolt Schönemann–Eisenstein-kritérium is.

4.14. Tétel. *Ha $f(x)$ Eisenstein-polinom, akkor irreducibilis $\mathbb{Q}$ felett.*

Bizonyítás. Az könnyen látható, hogy amennyiben $f(x) = f_1(x)f_2(x)$, akkor $f(x+a) = f_1(x+a)f_2(x+a)$, így f reducibilitásából következik az eltoltjának a reducibilitása is. Mivel $f(x)$-et $f(x+a)$-ból a $-a$-val való eltolással visszakaphatjuk, az utóbbi következtetés visszafelé is igaz. Így ha f Eisenstein-polinom (azaz valamelyik eltoltja Eisenstein alakú valamilyen p-re), akkor az eredeti Schönemann–Eisenstein-kritérium szerint f irreducibilis.

4.15. Példa. Legyen $f(x) = x^2 + x + 1$. Helyettesítsünk x helyébe $x + 1$-et. Ekkor $f(x+1) = (x+1)^2 + (x+1) + 1 = x^2 + 2x + 1 + x + 2 = x^2 + 3x + 3$. Az így kapott polinom már Eisenstein alakú és $p = 3$ egy jó prím, tehát irreducibilis $\mathbb{Q}$ fölött.

A fenti példa annak speciális esete, ahogy tetszőleges p prímre bebizonyítottuk, hogy a p-edik körosztási polinom, $\Phi_p(x)$, irreducibilis $\mathbb{Z}[x]$-ben: $f(x)$ ugyanis épp a harmadik körosztási polinom.

Attól, hogy egy $f(x) \in \mathbb{Z}[x]$ polinom nem Eisenstein-polinom - azaz sem maga $f(x)$, sem bármelyik eltoltja nem Eisenstein alakú - még lehet, hogy irreducibilis. Lássunk most erre egy példát. A példa megkonstruálásánál a nehézséget az okozza, hogy annak igazolására, miszerint egy polinom nem Eisenstein-polinom, elvben végtelen sok eltoltat kellene megvizsgálnunk.

Mutatunk egy algoritmust, - a [3] kéziratot követve - amellyel a kérdést véges kérdésre redukáljuk, majd megkonstruáljuk a megígért példát.

Először is szükségünk van két polinom rezultánsának a fogalmára.

4.16. Definíció. *Legyenek* $f = \sum_{j=0}^{n} a_j x^j$ *és* $g = \sum_{j=0}^{r} b_j x^j$ *tetszőleges komplex együtthatós polinomok, melyek fokaira teljesül, hogy* $\deg f = n$, $\deg g = r$ *és* $a_n \cdot b_r \neq 0$. *Ekkor az* f *és* g *rezultánsának nevezzük és* $R(f,g)$*-vel jelöljük azt az* $(n+r) \times (n+r)$ *méretű determinánst, ami az* f *és* g *polinomok együtthatóiból áll a következőképpen:*

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}$$

A rezultáns fő tulajdonságát mondja ki az alábbi tétel, melynek bizonyítását megtalálhatjuk [5] könyv 3.7.3 Tételében.

4.17. Tétel. *A fentiekben definiált* $R(f,g)$ *rezultáns pontosan akkor nulla, ha a két polinomnak van közös gyöke.*

A fenti állításnak egy egyszerű következménye az alábbi:

4.18. Állítás. *Legyen* $f \in \mathbb{Q}[x]$ *nem konstans polinom. Ha az*

1. $R(f,f') = 0$,
2. f*-nek és* f'*-nek van közös gyöke,*
3. f*-nek létezik többszörös gyöke*

ekvivalens állítások valamelyike teljesül, akkor f *nem irreducibilis* $\mathbb{Q}[x]$*-ben.*

Bizonyítás. Az, hogy $R(f, f') = 0$, éppen azt jelenti, hogy f-nek és f'-nek van közös gyöke $\mathbb{C}[x]$-ben. Ebből következik, hogy $\mathbb{Q}[x]$-ben f és f' legnagyobb közös osztója nem a konstans 1 polinom, tehát $\mathbb{Q}[x]$-ben f-nek van alacsonyabb fokú nem konstans osztója, vagyis f nem irreducibilis.

Most következzen az algoritmus annak eldöntésére, hogy egy $f(x)$ polinom Eisenstein-e.
Legyen

$$f(x) = \sum_{j=0}^{n} a_j x^j = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

ahol $n \geq 2$. Számítsuk ki az $R(f, f')$ értékét. Ha $R(f, f') = 0$, akkor $f(x)$ nem Eisenstein semmilyen p prímre, hiszen a 4.18 Állítás miatt nem is irreducibilis. Ha $R(f, f') \neq 0$, akkor faktorizáljuk. Minden olyan p prímre, amelyek osztják az $R(f, f')$ értéket, ellenőrizzük, hogy $f(x + a)$ Eisenstein alakú-e a p prímre nézve, ahol $a \in \{0, 1, \ldots, p - 1\}$, vagyis a egy modulo p maradékosztály. Ha a p prím és az a egész olyanok, hogy $f(x + a)$ Eisenstein alakú p-re nézve, akkor $f(x)$ Eisenstein-polinom. Ha viszont a most leírt p-k és a-k egyikével sem kapunk Eisenstein alakú polinomot, akkor be lehet bizonyítani, hogy más prímek és eltoltak sem működnek, azaz f nem Eisenstein-polinom. Némi meggondolást igényel két dolog a bizonyításban:

1. miért elég azokat a prímeket vizsgálni, amelyek osztják az $R(f, f')$ rezultánst,

2. miért lesz egyszerre Eisenstein alakú $f(x)$ és $f(x+p)$ a p prímre nézve.

Nézzük először az 1. kérdést:
Ha $f(x+a)$ Eisenstein alakú, akkor az $f_p(x+a)$ polinomnak, ami az $f(x+a)$ polinom modulo p véve, létezik többszörös gyöke $\mathbb{Z}_p$-ben. Ugyanis a főegyüttható kivételével p minden tagot oszt, így $f_p(x+a) = \overline{b}x^n$. Ennek a 0 nyilván többszörös gyöke. Az is könnyen látszik, hogy $f_p(x)$-nek az a többszörös gyöke modulo p. Ha $f(x)$, vagy valamelyik eltoltja Eisenstein alakú valamilyen p-re nézve, akkor f_p-nek van többszörös gyöke $\mathbb{Z}_p$-ben. A 4.17 tétel miatt ez éppen azt jelenti, hogy $\mathbb{Z}_p$-ben $R(f_p, f_p') = 0$. Ebből $p \mid R(f, f')$ adódik.

Jöjjön a 2. kérdés:
Tekintsünk egy $f(x) = a_n x^n + \ldots + a_1 x + a_0$ polinomot, és tegyük fel, hogy Eisenstein alakú. Ennek a p-vel való eltoltja:

$$f(x+p) = a_n(x+p)^n + \ldots + a_1(x+p) + a_0 = \sum_{i=0}^{n} a_i(x+p)^i.$$

Azt kell, belátnunk, hogy ez is Eisenstein alakú p-re nézve. Bontsuk tehát fel ezt az összeget 4 részösszegre a következőképpen: a főegyütthatóra, és azon tagokra, melyek tagjainak tényezői közt nincs p, vagy nincs x - azaz a konstansok -, vagy mindkettő van, ezt a tagot jelölje $P(x)$. Így az $f(x+p)$ polinom az alábbi alakú lesz:

$$f(x+p) = a_n x^n + \sum_{i=0}^{n-1} a_i x^i + \sum_{i=0}^{n} a_i p^i + P(x).$$

Az nyilvánvaló, hogy $p \nmid a_n$, hiszen $f(x)$-nek is a_n a főegyütthatója, és $f(x)$ Eisenstein alakú. A 2. tag az $f(x)$ polinom x-et tartalmazó tagjait tartalmazza, ezeket p osztja. A $P(x)$ minden tagjában van p, azaz ezt a tagot is osztja p. Azt kell még megvizsgálni, hogy teljesül-e, hogy $p^2 \nmid \sum_{i=0}^{n} a_i p^i$. Tudjuk, hogy $p \mid a_i$, ha $i \neq 0$, azaz $p^2 \mid \sum_{i=1}^{n} a_i p^i$. Mivel azonban $f(x)$ Eisenstein alakú, így $p^2 \nmid a_0$, vagyis $p^2 \nmid \sum_{i=0}^{n} a_i p^i$ valóban teljesül. Tehát ha az $f(x)$ polinom Eisenstein alakú valamilyen p prímre nézve, akkor $f(x+p)$ is Eisenstein alakú lesz a p prímre nézve, így elég csak egy modulo p maradékosztályt vizsgálnunk.

4.19. Példa. A következőkben példát mutatunk olyan egész együtthatós polinomra, amely irreducibilis $\mathbb{Q}[x]$-ben, de nem Eisenstein-polinom, azaz egyetlen eltoltjára sem teljesülnek a Schönemann–Eisensetin-kritérium feltételei.

Legyen $f(x) = x^3 + x^2 + x + 5$. Ez nem Eisenstein alakú, és megmutatjuk, hogy nem is Eisenstein-polinom. A fent ismertetett algoritmus alkalmazásához szükségünk van az $f(x)$ deriváltjára, ami $f'(x) = 3x^2 + 2x + 1$. Most ki

kell számítanunk az $R(f, f')$ értékét:

$$R(f, f') = \begin{vmatrix} 1 & 1 & 1 & 5 & 0 \\ 0 & 1 & 1 & 1 & 5 \\ 3 & 2 & 1 & 0 & 0 \\ 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 3 & 2 & 1 \end{vmatrix}$$

Fejtsük ki az első oszlop szerint:

$$R(f, f') = 1 \cdot \begin{vmatrix} 1 & 1 & 1 & 5 \\ 2 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 0 & 3 & 2 & 1 \end{vmatrix} + 3 \cdot \begin{vmatrix} 1 & 1 & 5 & 0 \\ 1 & 1 & 1 & 5 \\ 3 & 2 & 1 & 0 \\ 0 & 3 & 2 & 1 \end{vmatrix}$$

Ezeket az utolsó oszlopuk szerint kifejtve és a beszorzásokat elvégezve kapjuk, hogy

$$R(f, f') = (-5) \cdot \begin{vmatrix} 2 & 1 & 0 \\ 3 & 2 & 1 \\ 0 & 3 & 2 \end{vmatrix} + 1 \cdot \begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{vmatrix} + 15 \cdot \begin{vmatrix} 1 & 1 & 5 \\ 3 & 2 & 1 \\ 0 & 3 & 2 \end{vmatrix} + 3 \cdot \begin{vmatrix} 1 & 1 & 5 \\ 1 & 1 & 1 \\ 3 & 2 & 1 \end{vmatrix}$$

Az így kapott 3×3-as determinánsokat tovább kifejtve, vagy akár Sarrus-szabállyal kiszámolva:

$$R(f, f') = -5 \cdot (-4) + 1 \cdot 0 + 15 \cdot 40 + 3 \cdot (-4) = 20 + 0 + 600 - 12 = 608.$$

A 608 prímtényezős felbontása: $608 = 2^5 \cdot 19$. A két prím tehát, amelyeket meg kell vizsgálni a $p_1 = 2$ és a $p_2 = 19$.
Nézzük először a $p = 2$ esetet. Ekkor az egyetlen szóba jövő a érték az 1. Így az $f(x+1) = (x+1)^3 + (x+1)^2 + (x+1) + 5 = x^3 + 4x^2 + 6x + 4$ polinomot kell vizsgálni. Ez nem Eisenstein-polinom, hiszen p^2 osztja a konstans tagot. A $p = 19$ esetben, ha nincs szerencsénk, akkor 18 eltoltról kellene eldönteni, hogy Eisenstein-polinom-e. Ez hosszadalmas, fárasztó és könnyen elszámolhatjuk. Nem kell azonban soká gondolkodnunk, hogy rájöjjünk: "sokat" kizárhatunk a vizsgálandó a-k közül. Ugyanis ahhoz, hogy

$f(x)$ egy eltoltja Eisenstein alakú legyen egy p prímre nézve, p-nek osztania kell az $n-1$-edfokú tag együtthatóját. Ebből következik, hogy csak olyan a lehet megfelelő, amelyre $na + a_{n-1} \equiv 0 \pmod{p}$ teljesül. Példánk esetében $n = 3$, így $a_{n-1} = a_2 = 1$, valamint $p = 19$, tehát a megoldandó kongruencia: $3a+1 \equiv 0 \pmod{19}$. Az eredmény: $a = 6$. A "sokat" tehát azt jelenti, hogy a $p-1$ darab vizsgálandó számot egyetlen darabra redukáltuk.
Azt kell tehát még ellenőrizni, hogy $f(x+6)$ Eisenstein alakú-e a 19-re nézve. Az x helyébe $x+6$ -ot helyettesítve az $(x+6)^3+(x+6)^2+(x+6)+5$ polinom adódik, aminek konstans tagja: $6^3 + 6^2 + 6 + 5 = 216 + 36 + 6 + 5 = 263$. Mivel 19 nem osztja 263 -at, így az $f(x) = x^3 + x^2 + x + 5$ polinom nem Eisenstein-polinom. Ugyanakkor a polinom mégis irreducibilis $\mathbb{Q}[x]$-ben, hiszen a racionális gyökteszt alapján ellenőrizhetjük, hogy nincs neki gyöke (a szóba jövő "gyökjelölt" értékek a ± 1 és a ± 5, ezek azonban nem gyökök).

Lássunk még egy módszert az irreducibilitás vizsgálatára:

4.20. Állítás. *Az $f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)-1$ polinom irreducibilis, ha az $\alpha_1, \alpha_2, \dots, \alpha_n$ különböző egész számok.*

Bizonyítás. Legyen $f(x) = g(x)h(x)$, ahol $g(x)$ és $h(x)$ egész együtthatósak. Az könnyen látszik, hogy $f(\alpha_i) = -1$. Mivel $f(\alpha_i) = g(\alpha_i)h(\alpha_i)$, ebből adódóan $-1 = g(\alpha_i)h(\alpha_i)$, ezért $g(\alpha_i) = 1$ és $h(\alpha_i) = -1$ vagy $g(\alpha_i) = -1$ és $h(\alpha_i) = 1$. Így $g(\alpha_i) + h(\alpha_i) = 0$ minden $1 \le i \le n$ esetén. Ha a $g(x)$ és $h(x)$ polinomok közül egyik sem állandó, akkor $\deg(g(x) + h(x)) < n$, ez pedig az n darab gyök miatt csak úgy lehetséges, ha $g(x)+h(x) = 0$, azaz ez az összefüggés azonosság. Ebből az $f(x) = -[g(x)]^2$ következne, ez azonban lehetetlen, mivel $f(x)$ főegyütthatója pozitív.

Most mutatunk egy példát egy olyan polinomra, amely nem Eisenstein alakú, de ez előző tétel miatt mégis irreducibilis.

4.21. Példa. Megkonstruáljuk a polinomot. Egy olyan negyedfokú $f(x)$ polinomot szeretnénk, melynek főegyütthatója 1, van olyan p prím, amely a főegyüttható kivételével minden együtthatóját osztja, p^2 osztja a konstans

tagját, valamint $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)-1$, ahol $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ különböző egész számok.

Legyen $p = 2$. Ekkor kell, hogy $4 \mid \alpha_1\alpha_2\alpha_3\alpha_4 - 1$ teljesüljön. Ehhez mind a négy gyöknek páratlannak kell lennie. A néggyel való oszthatóság szempontjából a páratlan számok vagy $4k+1$ vagy $4k-1$ alakúak. Mivel nekünk úgy kell néggyel osztható számot kapnunk, hogy le kell vonnunk 1-et, így a négy szám szorzata $4k+1$ alakú kell legyen. Ez azt jelenti, hogy páros sok $4k-1$ alakú gyöke lehet, tehát $0, 2$ vagy 4. Talán az a példa a legegyszerűbb, amikor 2 ilyen alakú gyök van, hiszen ez éppen azt jelenti, hogy bármely négy egymást követő páratlan számot választhatjuk gyöknek. Már csak azt kell megvizsgálni, hogy ekkor a $p = 2$ prím valóban oszt-e minden együtthatót. Mivel tetszőleges sok páratlan szám szorzata páratlan és páros sok páratlan szám összege páros, így igen, hiszen az x^i, - ahol $i \in \{1, 2, 3\}$ - tag együtthatója egy $\binom{4}{i}$ tagú összeg, melynek minden tagja $4 - i$ darab páratlan szám szorzata.

Egy jó példa tehát az

$$(x-1)(x-3)(x-5)(x-7) - 1 = x^4 - 16x^3 + 86x^2 - 176x + 104$$

polinom. Korábban a rezultáns segítségével is vizsgáltuk az irreducibilitást. Alkalmazzuk most erre a polinomra is. Itt

$$f(x) = x^4 - 16x^3 + 86x^2 - 176x + 104,$$

a derivált pedig

$$f'(x) = 4x^3 - 48x^2 + 172x - 176.$$

Az együtthatókból felírható 7×7 determináns értéke: 591872, aminek prímtényezős felbontása: $2^{11} \cdot 17^2$. A $p_1 = 2$ esetben az $f(x+1)$ polinom konstans tagja $4 + 104 = 108$, ami osztható 4-gyel, tehát nem Eisenstein-polinom. A $p_2 = 17$ esetben az $na + a_{n-1} \equiv 0 \pmod{p}$ kongruenciába az ismert adatokat beírva: $4a - 16 \equiv 0 \pmod{17}$ kongruencia adódik. Ezt megoldva azt kapjuk, hogy $a \equiv 4 \pmod{17}$, tehát $a = 4$. Az $f(x+4)$ polinom konstans tagja 8,

ami nem osztható 17-tel, így ez az eltolt nem Eisenstein alakú. Ebből következően a polinom irreducibilitásáról nem mondhatunk semmit ez a módszer alapján, míg az első módszer egyértelművé teszi azt.

Befejezésül álljon itt még néhány példa arra, hogy milyen további állításokkal lehet igazolni egy egész együtthatós polinom irreducibilitását.

4.22. Állítás. *Az*

$$f(x) = (x-\alpha_1)^2(x-\alpha_2)^2 \dots (x-\alpha_n)^2 + 1$$

polinom irreducibilis $\mathbb{Q}[x]$-ben, ha az $\alpha_1, \alpha_2, \dots, \alpha_n$ különböző egész számok.

4.23. Állítás. *Az*

$$(x-a)(x-a-1)(x-a-2)(x-a-3)+1 = [(x-a-1)(x-a-2)-1]^2$$

és az

$$(x-a)(x-a-2)+1 = (x-a-1)^2$$

esetek kivételével az

$$f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)+1$$

polinom irreducibilis, ha az $\alpha_1, \alpha_2, \dots, \alpha_n$ különböző egész számok.

Mindkét állítás és bizonyításuk megtalálható a [2] könyvben.

5. fejezet

Példa egy nem euklideszi főideálgyűrűre

Egyetemi tanulmányaink során megtanultuk, hogy azon gyűrűk között, melyekre igaz a számelmélet alaptétele, fontos szerepet játszanak a főideálgyűrűk, s azok között is az euklideszi gyűrűk. Így pl. euklideszi gyűrű lesz minden test fölötti egyváltozós polinomgyűrű, de euklideszi gyűrűt alkotnak a Gauss-egészek is. Azt könnyű megmutatni, hogy minden euklideszi gyűrű főideálgyűrű, de azt már sokkal nehezebb, hogy a következtetés fordított iránya nem igaz: nem minden főideálgyűrűn tudunk euklideszi struktúrát értelmezni. Ahhoz, hogy ezt megmutassuk, szükségünk lesz néhány tétel kimondására. A példa igazolásához segítséget nyújt az [1] könyv.

Először definiáljuk az euklideszi gyűrű, illetve a főideálgyűrű fogalmát. Az [5] könyv terminológiáját használjuk, és a kommutatív egységelemes nullosztómentes gyűrűket az egyszerűség kedvéért szokásos gyűrűnek fogjuk nevezni.

5.1. Definíció. *Legyen R szokásos gyűrű. Az R euklideszi gyűrű, ha nemnulla elemein értelmezve van egy $\varphi : R\setminus\{0\} \to \mathbb{N}_0$ euklideszi normának nevezett függvény a következő tulajdonsággal: $\forall a, b \in R,\ b \neq 0$ esetén $\exists q, r \in R$, hogy $a = bq + r$ és $r = 0$ vagy $\varphi(r) < \varphi(b)$ teljesül.*

5.2. Definíció. *Az R szokásos gyűrűt főideálgyűrűnek nevezzük, ha minden ideálja főideál, vagyis egy elemmel generálható.*

Most kimondjuk a főideálgyűrűk egy hasznos tulajdonságát:

5.3. Tétel. *Ha R főideálgyűrű, akkor R-ben igaz a számelmélet alaptétele.*

Következzen a fejezet fő tételének szempontjából a két legfontosabb tétel bizonyítással együtt.

5.4. Tétel. *Egy D egységelemes integritási tartomány pontosan akkor főideálgyűrű, ha van olyan $\nu : D \to \mathbb{N}_0$ leképezés, mely csak a $0 \in D$ elemet viszi a 0-ba, és amelyre tetszőleges $a, b \in D,\ b \nmid a,\ b \neq 0$ esetén léteznek olyan $u, v \in D$ elemek, hogy $0 < \nu(au + bv) < \nu(b)$.*

Bizonyítás. Tegyük először föl, hogy a D integritási tartomány főideálgyűrű. Ekkor az 5.3 Állítás miatt igaz benne a számelmélet alaptétele. Így értelmezhetjük a következő függvényt: legyen ν az a függvény, mely minden $d \in D$ nem nulla és nem egység elemhez a d prímosztóinak számánál eggyel nagyobb számot rendeli úgy, hogy a prímtényezőket multiplicitásukkal számoljuk; legyen továbbá $\nu(0) = 0$, és tetszőleges D-beli e egységre legyen $\nu(e) = 1$. Legyenek most $a, b \in D$ tetszőleges elemek, melyekre teljesülnek az állítás feltételei. Mivel D főideálgyűrű, ezért van olyan d elem, melyre $(d) = (a, b)$; ez a d nyilván kitüntetett közös osztója a-nak és b-nek, és $d \in (a, b)$ miatt $d = au + bv$ alakú. Mivel $b \nmid a$, ezért d és b nem asszociáltak, azaz d valódi osztója b-nek, így $\nu(d) < \nu(b)$.
Most azt látjuk be, hogy ha létezik ilyen ν függvény, akkor D főideálgyűrű. Ehhez megmutatjuk, hogy ha $\{0\} \neq I \lhd D$ és $b \in I$ olyan, hogy $\nu(b) = \min\Big\{\nu(a) : a \in I \setminus \{0\}\Big\}$, akkor $I = (b)$. Mivel $b \in I$, így $(b) \subseteq I$. Másrészt legyen $a \in I$ tetszőleges eleme az ideálnak. Ha $b \nmid a$, akkor léteznek olyan $u, v \in D$ elemek, hogy $0 < \nu(au + bv) < \nu(b)$. Ekkor azonban $au + bv \in I$ teljesülne, mivel $a, b \in I$, és ez ellentmondana annak, hogy $\nu(b)$ értéke minimális az ideálbeli nem nulla elemek ν értékei között. Ebből következik, hogy feltevésünk hamis volt, azaz $b \mid a$ minden $a \in I$ esetén. Tehát $I \subseteq (b)$, vagyis azt kaptuk, hogy $I = (b)$.

A másik fontos tétel, amire szükségünk van:

5.5. Tétel. *Legyen D olyan euklideszi gyűrű, amely nem test. Ekkor D tartalmaz olyan u elemet, amely nem egység, de bármely $d \in D$ elemhez van olyan $r \in D$ egység vagy 0, hogy $u \mid d - r$.*

Bizonyítás. Legyen $\varphi(u) = \min\{\varphi(v) \mid v \in D,\ v \neq 0,\ v \text{ nem egység}\}$. Ekkor tetszőleges $d \in D$ esetén léteznek $q, r \in D$ elemek, hogy $d = qu + r$, ahol $r = 0$ vagy $\varphi(r) < \varphi(u)$. A $\varphi(r) < \varphi(u)$ feltétel a $\varphi(u)$ minimalitása miatt azt jelenti, hogy r egység. Ha rendezzük a d-re kapott összefüggést, akkor $d - r = qu$ adódik, amiből következik, hogy $u \mid d - r$.

5.6. Állítás. *A $\mathbb{Z}[(1 + i\sqrt{19})/2]$ főideálgyűrű, de nem euklideszi.*

Bizonyítás. Vezessük be a $\zeta = (1 + i\sqrt{19})/2$ jelölést, az állításban szereplő gyűrű legyen R. A gyűrűben értelmezett komplex normát jelöljük N-nel. Definiáljuk ezt a normát a következőképpen: minden $u \in \mathbb{Z}[\zeta]$ elemhez rendelje hozzá az abszolút értékének a négyzetét, azaz legyen $N(u) = |u|^2$. Most belátjuk, hogy ez valóban minden u esetén egész számot ad. A $\mathbb{Z}[\zeta]$ egy tetszőleges u eleme

$$u = a + b\left(\frac{1}{2} + \frac{\sqrt{19}i}{2}\right),$$

alakú, ahol a és b egész számok. A zárójel felbontása után

$$u = a + \frac{b}{2} + \frac{b\sqrt{19}i}{2}$$

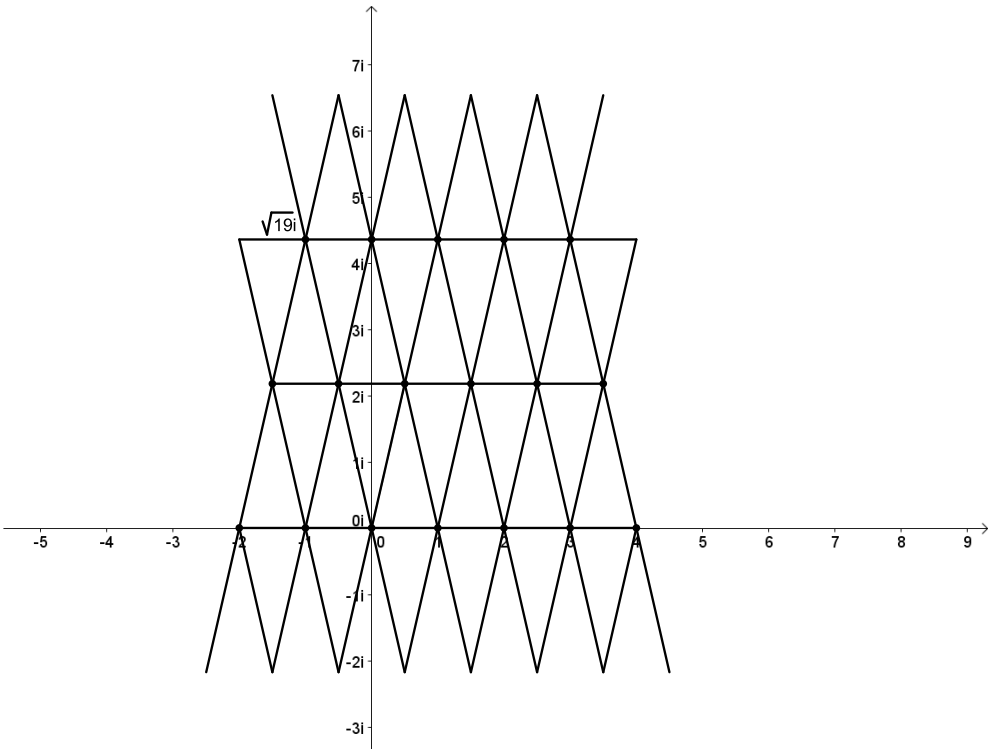
adódik, amely alakból már könnyen ki tudjuk számítani a normát. Tehát u normája:

$$N(u) = |u|^2 = \left(a + \frac{b}{2}\right)^2 + \left(\frac{b\sqrt{19}}{2}\right)^2.$$

A négyzetre emeléseket és az egynemű tagok összevonását elvégezve adódik, hogy:

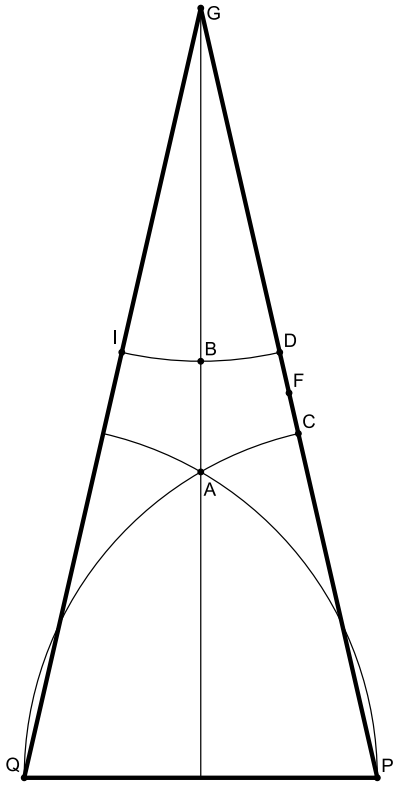
$$a^2 + ab + \frac{b^2}{4} + \frac{19b^2}{4} = a^2 + ab + \frac{20b^2}{4} = a^2 + ab + 5b^2,$$

ami nyilván egész szám.
Mielőtt tovább mennénk, nézzük meg, hogyan helyezkednek el a gyűrű elemei a komplex számsíkon:



5.1. ábra. A $\mathbb{Z}[(1+i\sqrt{19})/2]$ gyűrű elemeinek ábrázolása

A gyűrű elemei éppen a háromszögrács pontjai.
Azt szeretnénk megmutatni, hogy a $\nu = N$ választással teljesülnek az 5.4 Tétel feltételei, s így $\mathbb{Z}[(1+i\sqrt{19})/2]$ főideálgyűrű.
Ahhoz, hogy ezt jól lássuk, emeljünk ki egy háromszöget az előbbi háromszögrácsból:



5.2. ábra. A háromszögrács egy háromszöge

Vegyünk az 5.4 Tétel feltételeinek megfelelő a, b számokat a gyűrűből, és tekintsük az $\frac{a}{b} \in \mathbb{C}$ számot a síkon, ahol a rácspontok $\mathbb{Z}[\zeta]$ elemei. Az $\frac{a}{b}$ benne van valamelyik rácsháromszögben, és a $b \nmid a$ feltétel miatt nem rácspont. Belátjuk, hogy az esetek majd mindegyikében vagy $0 < \left| \frac{a}{b} - q \right| < 1$ a háromszög valamely q csúcsára, és így $|a - qb| < |b|$ miatt az $u = 1$ és a $v = -q$ jó választás, vagy $0 < \left| \frac{a}{b} - \frac{q_1 + q_2}{2} \right| < \frac{1}{2}$ a háromszög két - alkalmasan választott - q_1, q_2 csúcsára, és így $|2a - (q_1 + q_2)b| < |b|$ miatt $u = 2$ és $v = -(q_1 + q_2)$ jó, s a kimaradó esetben is teljesülnek a 5.4 Tétel feltételei. Szimmetriaokok miatt feltehetjük, hogy a rácsháromszög, amiben $\frac{a}{b}$ benne van, épp olyan alakú, mint a fenti ábrán látható háromszög. A most következő érvelésünk nyilván elmondható a tükrözött háromszögre is.

Írjuk föl a kiemelt rácsháromszög számunkra fontos adatait: a háromszög ma-

gassága $\frac{\sqrt{19}}{2}$, alapja 1, szára pedig $\sqrt{\left(\frac{1}{2}\right)^2+\left(\frac{\sqrt{19}}{2}\right)^2}=\sqrt{5}$. A csúcsok körüli egység sugarú körök lefedik a háromszög egy részét; ha $\frac{a}{b}$ a lefedett részbe esik (magát a körvonalat nem számítva), akkor a megfelelő körközéppontot (azaz rácspontot) kiválasztva az első esetet kapjuk: $\left|\frac{a}{b}-q\right|<1$. Jelölje most F a PG szár felezőpontját, és vizsgáljuk azt az esetet, amikor $\frac{a}{b}$ nem a lefedett részbe esik. Szimmetriaokok miatt ismét feltehető, hogy $\frac{a}{b}$ az F felőli oldalon van, és tegyük még fel, hogy $\frac{a}{b}$ nem F. Elég azt belátni, hogy A, B, C, D benne vannak az F körüli $\frac{1}{2}$ sugarú körben, ugyanis a konvex burkuk lefedi a hiányzó félterületet.

Számítsuk most ki az F pont távolságát az A, B, C, D pontoktól. A C és D pontok egyenlő távolságra vannak F-től, és ez a távolság nem más, mint

$$|FC| = |FD| = \frac{\sqrt{5}-2}{2},$$

ami kisebb $\frac{1}{2}$-nél, ugyanis $\sqrt{5}<3$. Most azt kell megvizsgálni, hogy az A pont $\frac{1}{2}$-nél közelebb van-e F-hez, azaz teljesül-e a

$$\sqrt{\left(\frac{1}{4}\right)^2+\left(\frac{\sqrt{19}}{4}-\frac{\sqrt{3}}{2}\right)^2}<\frac{1}{2}$$

egyenlőtlenség. Mivel itt pozitív számokról van szó, az egyenlőtlenség mindkét oldalát négyzetre emelhetjük, majd a további számolásokat elvégezve azt kapjuk, hogy a kiinduló egyenlőtlenségünk ekvivalens azzal, hogy

$$\frac{1}{16}+\frac{31}{16}-\frac{\sqrt{57}}{4}<\frac{1}{4},$$

amiből még némi átalakítással a $8-\sqrt{57}<1$ igaz egyenlőtlenség adódik, hiszen $\sqrt{57}>7$. Így tehát az A pont $\frac{1}{2}$-nél közelebb van F-hez, azaz $|FA|<\frac{1}{2}$. Az F pont B-től való távolsága:

$$|FB| = \sqrt{\left(\frac{1}{4}\right)^2+\left(\frac{\sqrt{19}}{4}-1\right)^2}.$$

Mivel $1 > \frac{\sqrt{3}}{2}$, így $|FB| < |FA| < \frac{1}{2}$.
Hátra van még az az eset, amikor az $\frac{a}{b}$ szám éppen az F pont. Válasszuk most q-nak a háromszög P csúcsát, és legyen $r = \frac{a}{b} - q$. Ekkor $2r \in R$, mivel r épp a háromszög oldalának fele, így $2r$ rácsvektor. Mivel R zárt a konjugálásra, ezért $2\overline{r} \in R$ is teljesül, és így $2\overline{r}r = 2|r|^2 = 2\left(\frac{\sqrt{5}}{2}\right)^2 = \frac{5}{2}$.
Innen

$$2\overline{r} \cdot \frac{a}{b} - 2\overline{r}q - 2 = \frac{1}{2}$$

adódik, ahonnan azt kapjuk, hogy

$$|(2\overline{r})a - (2\overline{r}q + 2)b| = \frac{|b|}{2} < |b|.$$

Ezzel az 5.4 Tétel alapján beláttuk, hogy $\mathbb{Z}[\zeta]$ főideálgyűrű.
Most megmutatjuk, hogy nem euklideszi.
A $\mathbb{Z}[\zeta]$ főideálgyűrűben csak az 1 és a -1 egység, hiszen csak e két szám normája 1. A norma ugyanis multiplikatív, és azt már korábban beláttuk, hogy R elemein mindig egész szám, így egységeknek a normája osztja az 1 normáját, azaz 1-et. Ha $\mathbb{Z}[\zeta]$ euklideszi lenne, akkor az 5.5 Tétel szerint van olyan $u \in \mathbb{Z}[\zeta]$ elem, ami nem egység, vagyis $u \neq \pm 1$ és bárhogy is válasszunk egy $z \in \mathbb{Z}[\zeta]$ elemet, az u-nak lesz többszöröse a $Z_z = \{z-1, z, z+1\}$ halmazban.
Legyen először $z = 2$. Ekkor $Z_2 = \{1, 2, 3\}$. A Z-beli elemek normája rendre $1, 4, 9$. Most legyen $z = \zeta$, ekkor pedig $Z_\zeta = \{\zeta - 1, \zeta, \zeta + 1\}$. Ezek normája pedig rendre: 5,5,7. Tudjuk, hogy ha $\alpha \mid \beta$, akkor $N(\alpha) \mid N(\beta)$, tehát, ha u-nak van többszöröse a Z_2 halmazban, akkor normája osztja valamelyik Z_2-beli elem normáját. Mivel nem egység, így nem lehet 1 a normája. Ha viszont osztja 4-et vagy 9-et, akkor nem oszthatja az 5 és a 7 egyikét sem, tehát $\mathbb{Z}[\zeta]$ nem euklideszi.

A fenti tétel tehát azt mutatja, hogy a főideálgyűrűk osztálya szigorúan bővebb, mint az euklideszi gyűrűké.

Köszönetnyilvánítás

A szakdolgozat elkészítésében nyújtott rendkívül nagy segítségért és támogatásért köszönet illeti témavezetőmet, Ágoston István egyetemi docenst. Konzultációink alkalmával mindig lelkiismeretesen magyarázott, ha nem értettem valamit, akár többször is, ha szükség volt rá. Irányítása és útmutatásai következtében algebrai ismereteim nagy mértékben mélyülhettek, hiszen sok érdekességet mutatott konzultációinkon a szakdolgozatban érintett témákon túlmenően is.

Irodalomjegyzék

[1] B. Szendrei - Czédli - Szendrei: *Absztrakt algebrai feladatok*, Polygon (2005)

[2] D. K. Fagyejev - I. Sz. Szominszkij: *Felsőfokú algebrai feladatok*, Műszaki Könyvkiadó (1973)

[3] Filaseta: The theory of irreducible polyonomials (kézirat)

[4] Freud - Gyarmati: *Számelmélet*, Nemzeti Tankönyvkiadó (2006)

[5] Kiss Emil: *Bevezetés az algebrába*, Typotex (2007)