Eötvös Loránd Tudományegyetem

Természettudományi Kar

Algebra és Számelmélet Tanszék

Irreducibilis polinomok szakkörre

Szakdolgozat

Készítette

Birtha Nikoletta

Matematika Tanári BSc.

Konzulens

Dr. Zábrádi Gergely

adjunktus

Budapest, 2014

Tartalomjegyzék

Bevezetés **2**

1. Irreducibilitás **3**

1.1. Gyökök és irreducibilitás 5

1.2. Komplex számok feletti irreducibilitás 6

1.3. Valós számok feletti irreducibilitás 7

2. A maradékos osztás **9**

3. Irreducibilitás racionális számtest fölött **12**

3.1. Schönemann-Eisentesin kritérium 13

3.1.1. Schönemann-Eisenstein-kritérium alkalmazása 14

3.2. mod p vizsgálata 16

3.3. A polinom általános együtthatókkal való szorzatra bontása 16

3.4. A módszerek alkalmazása 17

3.5. Racionális együtthatós polinomok Newton-poligonja 18

4. Egész együtthatós polinomok **22**

5. A körosztási polinomok **26**

6. Köszönetnyilvánítás **30**

7. Irodalomjegyzék **31**

Bevezetés

A szakdolgozatom az "irreducibilis polinomok szakkörre" címet kapta, mert az algebrai tanulmányaim során ez a témakör keltette fel legjobban az érdeklődésemet. A szakdolgozat egységes képet alkot a különböző témakörökről, amelyekkel kapcsolatban áll az irreducibilitás. A fejezetek nem úgy követik egymást, ahogy tanultam őket, hanem elsősorban azzal foglalkoztam, amikor a polinom irreducibilis a megadott test felett, majd azzal, hogy hogyan kapcsolódik az irreducibilitás a különböző témákhoz.

A szakdolgozatom első része az alapfogalmakat mutatja be, és a felmerülő alapvető tételeket, illetve azok bizonyítását. A gyökök és irreducibilitás alfejezet tartalmazza a polinomok gyökeire vonatkozó tételeket, állításokat és azok bizonyítását, majd a komplex számok, illetve a valós számok feletti irreducibilitásról olvashatunk, ahol szintén olyan tételekkel ismerkedhetünk meg, amelyek megkönnyítik a komplex, illetve valós polinomok felbonthatóságának igazolását.

A második fejezet a maradékos osztás és az irreducibilitás összefüggésére világít rá.

A harmadik rész a racionális számtest fölötti irreducibilitást mutatja be. Különböző módszereket tartalmaz, hogy megtudjuk, mikor felbonthatatlan az adott polinom racionális test felett. Mindegyik módszert - az érthetőség kedvéért - példákkal támasztom alá. Az egyik alfejezet kevert feladatokat tartalmaz, amelyeket a felsorolt módszerek egyikével, vagy azok egymásutánjával kell megoldani. Az utolsó alfejezet a racionális együtthatós polinomok Newton-poligonja témakört tartalmazza. Tanulmányaim során ez nem szerepelt, teljesen új és érdekes volt számomra, hogy ez is összefügg az irreducibilitással, ezért is tartottam fontosnak, hogy ezt is tartalmazza a szakdolgozatom.

A negyedik rész az egész együtthatós polinomok irreducibilitását mutatja be. A fejezet tartalmazza a Gauss lemmákat, illetve azok következményeit és bizonyítását.

Az utolsó fejezet a körosztási polinomokat és azok tulajdonságait mutatja be. A fejezet először az alapfogalmakkal kezd, majd példákkal támasztja alá őket és összefüggést mutat be az irreducibilitással kapcsolatban.

1. fejezet

Irreducibilitás

Ebben a fejezetben az alapfogalmakat fogom bemutatni. Az első és legfontosabb definíció, hogy mit jelent az irreducibilitás, és mikor irreducibilis azaz felbonthatatlan a polinomunk.

1.0.1. Definíció. *Legyen R szokásos gyűrű. A $p \in R$ elemet felbonthatatlannak vagy irreducibilisnek nevezezzük, ha nem nulla, nem egység, és p-nek nincs nemtriviális felbontása.*

A következő definícióban az előzőben felmerülő alapfogalmakat fogom definiálni, hogy az irreducibilitás definíciója teljesen érthetővé váljon.

1.0.2. Definíció. *Legyen R szokásos gyűrű, és $0 \neq r = bc$, ahol $r, b, c \in R$. Azt mondjuk, hogy az r elemnek ez a felbontása triviális, ha b és c egyike r-nek asszociáltja. Ami ezzel ekvivalens: b és c közül a másik egység.*

Azonban, az irreducibilitás definíciójában kizártuk az egységeket (u egység, ha $u|1$ itt a $\pm 1 - et$), mivel ezekre nem építhetünk, ha egy általános számot szeretnénk felbontani.

1.0.1. Állítás:. *Legyen R szokásos gyűrű. A $p \in R$ elem akkor és csak akkor felbonthatatlan, ha nem nulla, nem egység, és p minden osztója vagy egység vagy p-nek asszociáltja.*

Bizonyítás: Ha p felbonthatatlan és $r|p$, akkor van olya $t \in R$, hogy $p = rt$. Ennek a felbontásnak tiriviálisnak kell lennie, tehát r vagy egység, vagy pedig t egység, de ez utóbbi esetben p és r asszociáltak. Megfordítva, ha p-ről azt tudjuk, hogy minden osztója vagy egység, vagy p-nek asszociáltja, akkor tegyük fel, hogy $p = bc$ egy felbontás. Ekkor $b|p$, ezért feltevésünk szerint b vagy egység , vagy p-nek asszociáltja. Az első esetben $p = bc$ felbontás tiriviális, de a másodikban is az: ekkor c lesz az egység. Valóban, $p = be$ alkalmas e egységre, és így $bc = be$. Mivel $p \neq 0$, a b sem nulla, és így $c = e$ tényleg egység.

1.1. Feladat. *Az 21 számot bontsuk fel felbonthatatlanok szorzatára $\mathbb{Z}-$ben*

Megoldás: Négyféleképpen fogom felbontani.

$$21 = 7 \cdot 3 = 3 \cdot 7 = (-7) \cdot (-3) = (-3) \cdot (-7)$$

Az első felbontásból az utolsót úgy kaptuk meg, hogy felcseréljük a tényezőket és mindkét esetben kapnak egy – előjelet azaz vesszük az asszociáltjukat. Tehát a felbontás egyértelműsége azt jelenti, hogy bárhogy vesszük az r elemnek két felbontását irreducibilis elemek szorzatára, a tényezők száma megegyezik, és a két felbontás tényezői egymással párba állíthatók úgy, hogy a párok tagjai egymás asszociáltjai legyenek. Általánosan leírva:

$$r = p_1 \dots p_k = q_1 \dots q_l$$
$$k = l$$

Amikor összevonjuk a megegyező felbonthatatlanokat akkor a szám kanonikus alakját kapjuk. A kanonikus alak definíciója a következő:

1.0.3. Definíció. *Az $r \neq 0$ elem kanonikus alakja*

$$r = ep_1^{\alpha_1} \dots p_m^{\alpha_m} \quad ,$$

ahol e egység és p_i páronként nem asszociált felbonthatatlanak elemek, az α_i pedig nemnegatív egész számok.

1.2. Feladat. *Mi a -9 kanonikus alakja?*

Megoldás:

$$-9 = 3 \cdot (-3) = (-3) \cdot 3 = -3^2 = -(-3)^2$$

Láthatjuk, hogy ezen feladat során csak úgy tudjuk összevonni, ha a -1-es tényezőt meghagyjuk, ezért a definícióban is megengedjük az egység tényezőt.

1.0.2. Állítás:. *Legyen T test. Egy $f \in T[x]$ polinom akkor és csak akkor irreducibilis T fölött, ha nem konstans, és nem bontható föl két alacsonyabb fokú T-beli együtthatós polinom szorzatára.*

Ennek bizonyítása a következő:

Bizonyítás: Test fölötti polinomgyűrűben, az egységek a nem nulla konstans polinomok. Tehát egy polinom triviális felbontásai azok, amikor az egyik tényező konstans, és így nemtriviális felbontásaok azok, amikor egyik tényező sem konstans. Ez ugyanazt jelenti, mintha azt mondanánk, hogy mindkét tényező az eredeti polinomnál alacsonyabb fokú kell, hogy legyen, hiszen a tényezők fokainak összege az eredeti polinom foka.

1.1. Gyökök és irreducibilitás

Ebben a fejezetben azt fejtem ki, hogy hogyan függ össze, hogy egy polinom irreducibilis-e, egy adott test felett azzal, hogy van-e gyöke az adott esetben.
A következő állítás a legegyszerűbb esetről, amikor elsőfokú a polinom, akkor biztosan irreducibilis lesz.

1.1.1. Állítás:. *Test fölött egy elsőfokú polinom mindig irreducibilis.*

Bizonyítás: Elsőfokú polinomot nem lehet alacsonyabb fokúak szorzatára bontani, hiszen két nulladfokú polinom szorzata is nulladfokú.

Az alábbi állítás a másodfokú polinomokat vizsgálja, azonban az előzővel ellentétben itt nem mindig teljesül az irreducibilitás.

1.1.2. Állítás:. *Legyen T test. Ha egy legalább másodfokú $T[x]$-beli polinomnak van gyöke T-ben, akkor nem irreducibilis T fölött.*

Bizonyítás: Legyen $b \in T$ gyöke egy $f \in T[x]$-beli polinomnak. Ekkor a hozzá tartozó $x - b$ gyöktényező kiemelhető f-ből. Ha f legalább másodfokú, akkor ezzel f-et két alacsonyabb fokú polinom szorzatára bontottuk.

Megjegyzés: Egy polinom esetén nem elég megkeresni a gyököket ahhoz, hogy eldöntsük irreducibilis-e. Ha nincs gyöke a polinomnak akkor abból nem következik, hogy irreducbilis.

1.3. Feladat. *Erre a következő racionális test fölötti polinom mutat példát:* $(x^2 + 1)$. *Ennek valós gyöke sincs, és nem irreducibilis, mert szorzat alakban van megadva. Tehát nem elég csak a gyököket megkeresni az irreducibilitás eldöntéséhez.*

A következő állítás pedig segít megtalálni a polinom gyökeit.

1.1.3. Állítás:. *Legyen T test. Ekkor egy $f \in T[x]$ polinomnak akkor és csak akkor van gyöke T-ben, ha van elsőfokú tényezője.*

Bizonyítás: Azt már láttuk, hogy ha van gyök, akkor a megfelelő gyöktényező kiemelhető. Megfordítva, tegyük fel, hogy $f = gh$, ahol $g(x) = ax + b$ egy elsőfokú polinom. ekkor $-b/a$

gyöke f-nek.

Azonban a következő állítás kimondja, hogy milyen esetben lehet egy másod illetve egy harmadfokú polinom irreducibilis.

1.1.4. Állítás:. *Legyen T test. Ha egy másod vagy harmadfokú $T[x]$-beli polinomnak nincs gyöke T-ben, akkor irreducibilis T fölött.*

Bizonyítás: Egy másodfokú polinomot alacsonyabb fokú tényezők szorzatára csak úgy lehet felbontani, hogy mindkét tényező elsőfokú lesz. Hasonlóképpen egy harmadfokú polinomot alacsonyabb fokúak szorzatára csak úgy bonthatunk, hogy az egyik tényező elsőfokú lesz, és így az előző állítás szerint gyök is.

1.2. Komplex számok feletti irreducibilitás

1.2.1. Tétel:. *A komplex számok teste fölött (és általában egy algebrailag zárt T test fölött) az irreducibilis polinomok pontosan az elsőfokúak.*

Bizonyítás: Ez nyilvánvaló az eddigiekből, hiszen algebrailag zárt test fölött minden nemkonstans polinomnak van gyöke.

1.2.1. Lemma. *Legyen z komplex gyöke a valós együtthatós f polinomnak. Ekkor z konjulgáltja is gyöke f-nek, sőt z és $\overline{z}$ ugyanannyiszoros gyökök.*

Bizonyítás: Legyen $f(x) = a_0+a_1x+\cdots+a_nx^n$. Ennek gyöke a z, tehát $0 = a_0+a_1z+\cdots+a_nz^n$. Vegyük mindkét oldal konjugáltját. Tudjuk, hogy összeg konjugáltja a konjugáltak összege, ezért a bal oldalán álló összeget tagonként konjugálhatjuk. De a konjugálás szorzattartó is, ezért az eredmény a következő:

$$\overline{a_0} + \overline{a_1 \cdot z} + \cdots + \overline{a_n \cdot z^n} = \overline{0} \quad .$$

Valós szám konjugáltja önmaga, tehát $\overline{0} = 0$ és $\overline{a_j} = a_j$. Így a bal oldalon $f(\overline{z})$ áll, a jobb oldalon 0, tehát $\overline{z}$ tényleg gyöke f-nek.

Most f foka szerinti teljes indukcióval belátjuk, hogy z és $\overline{z}$ minden valós együtthatós f polinomnak ugyanannyiszoros gyökei. Ha z valós, azaz $z = \overline{z}$, akkor az állítás nyilvánvaló, ezért feltehető, hogy $z \neq \overline{z}$. Az indukciós feltevésünk az, hogy f-nél alacsonyabb fokú polinomokra igaz az állítás, be kell látnunk f-re is. Ha z és $\overline{z}$ közül egyik sem gyöke f-nek, akkor az imént

bizonyított állítás miatt a konjugáltja, vagyis a másikuk is gyök. Mivel $z \neq \overline{z}$, a z és $\overline{z}$ gyökökhöz tartozó gyöktényezők egyszerre kiemelhetők:

$$f(x) = (x - z)(x - \overline{z})q(x)$$

ahol $q \in \mathbb{C}[x]$ polinomra. Azonban

$$g(x) = (x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z}$$

valós együtthatós polinom, hiszen $z\overline{z}{=}|z|^2$ és $z + \overline{z} = 2 \operatorname{Re} z$ valós számok. A maradékos osztás egyértelműsége miatt tehát q is valós együtthatós polinom. Az indukciós feltevés miatt tehát q-nak z és $\overline{z}$ ugyanannyiszoros gyöke, és így ugyanez igaz f-re is.

1.4. Feladat. *Bontsuk fel a* $6(x^2 - 2)(x^2 + 1)$ *polinomot irreducibilisek szorzatára* $\mathbb{C}$ *fölött.*

Megoldás: Jelen esetben a 6 egység, így külön tényezőként nem szerepelhet.

$$(6x + 6\sqrt{2})(x - \sqrt{2})(x + i)(x - i)$$

1.5. Feladat. *Irreducibilis-e* $x^7 + x + 1$ *polinom* $\mathbb{C}$ *fölött?*

Megoldás: Az 1.2.1. tételre hivatkozva ez a polinom nem irreducibilis $\mathbb{C}$ fölött.

1.6. Feladat. *Irreducibilis-e* $x^2 - 2$ *polinom* $\mathbb{C}$ *fölött?*

Megoldás: Ahogy az előző esetben is hivatkozunk az 1.2.1. tételre. Ez a polinom nem irreducibilis $\mathbb{C}$ fölött.

1.3. Valós számok feletti irreducibilitás

1.3.1. Tétel:. *A valós számok teste fölött az irreducibilis polinomok pontosan az elsőfokúak, és azok a másodfokúak, melyeknek nincs valós gyöke.*

Bizonyítás: A felsorolt polinomokról a korábbi állításokon már beláttuk, hogy irreducibilisek. Tegyük fel, hogy f irreducibilis polinom $\mathbb{R}$ fölött. Ekkor nem konstans, és így van egy z komplex gyöke. Ha ez valós, akkor f csak elsőfokú lehet. Ha z nem valós, akkor az előző bizonyításban láttuk, hogy a valós együtthatós $g(x) = (x - z)(x - \overline{z})$ kiemelhető f-ből, és a megmaradó q polinom is valós együtthatós. Mivel f irreducibilis, $q(x)$ csak konstans lehet, és így f tényleg másodfokú, melynek gyökei nem valósak.

Következmény: Páratlan fokú valós együtthatós polinomnak van valós gyöke.

Bizonyítás: Bontsuk a polinomot irreducilisek szorzatára $\mathbb{R}$ fölött. Ezek első vagy másodfokúak. Mindegyik tényező nem lehet másodfokú, mert a polinom foka páratlan. Tehát van elsőfokú tényező, és így valós gyök is.

Megjegyzés: Az előző bizonyítás felhasználja az algebra alaptételét.

1.7. Feladat. *Bontsuk fel irreducibilis polinomok szorzatára a* $x^4 - 1$ *polinomot* $\mathbb{R}$ *fölött.*

Megoldás:A polinomot gyöktényezők szorzatára bontjuk, majd a nemvalós gyökökhöz tartozó gyöktényezőket párosítjuk a konjugáltjukkal.

$$x^4 - 1 = (x-1)(x+1)(x^2+1)$$

1.8. Feladat. *Bontsuk fel irreducibilis polinomok szorzatára a* $x^4 + 9$ *polinomot* $\mathbb{R}$ *fölött.*

Megoldás: Az előző eljárás alapján a megoldás:

$$x^4 + 9 = (x^2 + \sqrt{6}x + 3)(x^2 - \sqrt{6}x + 3) \quad .$$

1.9. Feladat. *Bontsuk fel irreducibilis polinomok szorzatára a* $x^6 - 4x^3 + 3$ *polinomot* $\mathbb{R}$ *fölött.*

Megoldás: Az $x^6 - 4x^3 + 3 = 0$ egyenletbe $y = x^3$ helyettesítéssel kapunk egy másodokú egyenletet kapunk, melynek gyöke 1 és 3. Így

$$x^6 - 4x^3 + 3 = (x^3 - 1)(x^3 - 3) \quad .$$

A két tényezőnek egy-egy valós gyöke van, így a végeredmény a következő:

$$x^6 - 4x^3 + 3 = (x-1)(x^2 + x + 1)(x - \sqrt[3]{3})(x^2 + \sqrt[3]{3}x + \sqrt[3]{9})$$

2. fejezet

A maradékos osztás

Ezen fejezet során rámutatok, hogy milyen összefüggés van az irreducibilitás és a maradékos osztás között.
Először az alábbi tétellel vezetem be a fejezetet.

2.0.2. Tétel:. *Legyen R szokásos gyűrű. Ekkor $R[x]$ polinomgyűrűben minden olyan $g \in R[x]$ polinommal lehet maradékosan osztani, amelynek főegyütthatója invertálható. Ez azt jelenti, hogy tetszőleges $f \in R[x]$ polinomhoz lézetnek olyan $q, r \in R[x]$ polinomok, amelyekre $f = gq + r$, és vagy $r = 0$, vagy r foka kisebb g fokánál. A q és r polinomok egyértelműen meghatározottak.*

A tételben szereplő $f = gq + r$ maradékos osztásban az f az osztandó és a g az osztó, a q polinomot hányadosnak, az r-et pedig a maradéknak nevezzük.

Bizonyítás: Ha $f = 0$, akkor $0 = g \cdot 0 + 0$ előállítás megfelelő lesz. Ha f foka kisebb g fokánál, akkor is készen vagyunk, mert $f = g \cdot 0 + f$ maradékos osztás is eleget tesz a feltételeknek. Tegyük fel indirekten, hogy az állítás nem igaz, azaz van olyan ellenpolinom, amely nem osztható el maradékosan g-vel. Láttuk, hogy a nullapolinom eloszthatóó maradékosan g-vel, és így az ellenpéldák között nincs ott a nulla, vagyis mindegyik ellenpélda-polinomnak van foka. Válasszunk ki közülük egy lehető legkisebb fokú f polinomot. Az ennél kisebb fokúak már nem ellenpéldák, vagyis maradékosan oszthatók g-vel.
Jelőle f főtagját ax^n és g főtagját bx^m, ahol b invertálható eleme R-nek. Az állítást beláttuk abban az esetben, amikor f foka kisebb g fokánál, vagyis az m-nél kisebb fokú polinomok nem ellenpéldák. Mivel f ennelpélda, ezért $deg(f) = n \geq m$.
Ha elvégezzük az osztást, azaz f tagját osszuk el g főtagjával, szorozzuk ezzel vissza a g osztót, és a kapott szorzatot vonjuk ki f-ből. Az eredmény $f_0 = f - (a/b)x^{n-m}g$. Ez értelmes, hiszen

feltettük, hogy b-vel lehet R-ben osztani.

A kivonásnál f főtagja kiesik, és így f_0 foka kisebb, mint $deg(f) = n$. Ezért f_0 már nem ellenpélda az állításra, vagyis maradékosan eloszthető g-vel: $f_0 = gq_0 + r$, ahol $r = 0$, vagy r foka kisebb g fokánál. De innen:

$$f = f + (a/b)x^{n-m}g = g(q_0 + (a/b)x^{n-m}) + r,$$

tehát f is eloszthető maradékosan g-vel. Ez az ellentmondás bizonyítja a tétel első állítását, azt, hogy a maradékos osztás elvégezhető.

Az egyértelműség bizonyításához tegyük fel, hogy f-et kétféleképpen is elosztottuk maradékosan g-vel:

$$f = gq_1 + r_1 = gq_2 + r_2,$$

ahol r_1 és r_2 is nulla, vagy g-nél kisebb fokú polinom. Átrendezéssel:

$$g(q_1 - q_2) = r_2 - r_1 \quad .$$

A jobb oldalon álló $r_2 - r_1$ polinom vagy nulla, vagy g-nél kisebb fokú. Ha $q_1 - q_2 \neq 0$, akkor viszont a bal oldalon álló polinom foka legalább annyi, mint g foka, hiszen szorzásnál a fokok összeadódnak, ami ellentmondás. Ezért $q_1 - q_2 = 0$, de akkor nyilván $r_2 - r_1 = 0$, és így a két maradékos osztásban a hányados is ugyanaz.

2.1. Feladat. *Osszuk el a* $2x^3 + 2x^2 + 3x + 2$ *polinomot a* $x^2 + 1$ *polinommal.*

Megoldás: Az első lépésben az osztandó főtagját elosztjuk az osztó főtagjával: $2x^3/x^2 = 2x$. Ezt leírjuk, majd visszaszorozzuk vele az osztót: $(2x)(x^2 + 1) = 2x^3 + 2x$. Ezt az osztandó alá írjuk, és kivonjuk: $(2x^3 + 2x^2 + 3x + 2) - (2x^3 + 2x) = 2x^2 + x + 2$. Ezzel az új polinommal ismételjük az eljárást addig, amíg a kapott különbség foka még nagyobb vagy egyenlő, mint az osztó foka. Láthatjuk, hogy a hányados $2x + 2$, a maradék pedig x.

$$\begin{array}{l} (2x^3 + 2x^2 + 3x + 2) : (x^2 + 1) = 2x + 2 \\ \underline{-(2x^3 + 0 + 2x)} \\ \quad + 2x^2 + x + 2 \\ \quad \underline{-(2x^2 + 0 + 2)} \\ \quad\quad x \end{array}$$

2.2. Feladat. *Osszuk el a* $x^3 - 2$ *polinomot a* $2x^2 + 2x - 3$ *polinommal.*

Megoldás: Az előző feladat megoldásának módszerével oldjuk meg ezt a feladatot is. Azonban én átírom az osztandó polinomot, hogy még szemléltetesebb legyen a megoldás.

$$
\begin{array}{l}
(x^3 \quad + \quad 0x^2 + 0x - 2) : (2x^2 + 2x - 3) = \frac{x}{2} - \frac{1}{2} \\
\underline{-(x^3 \quad + \quad x^2 - \frac{3x}{2} - 0 \quad)} \\
0 \quad - \quad x^2 + \frac{3x}{2} - 2 \\
\quad \underline{-(-x^2 - x + \frac{3}{2})} \\
\qquad\qquad \frac{5x}{2} - \frac{7}{2}
\end{array}
$$

2.3. Feladat. *Osszuk el a $x^4 + x^2 + 1$-et a $x^2 + x + 1$-gyel. Milyen maradékot kapunk?*

Megoldás: Az osztás elvégzése után 0 maradékot kapunk.

$$
\begin{array}{l}
(x^4 \quad + \quad x^2 \quad + \quad 1) \quad : (x^2 + x + 1) = x^2 - x + 1 \\
\underline{-(-x^4 + \quad x^3 \quad + x^2)} \\
\qquad -x^3 \quad + \quad 1 \\
\qquad \underline{-(-x^3 - \quad x^2 \quad - x)} \\
\qquad\qquad\qquad x^2 \quad + x + \quad 1 \\
\qquad\qquad\qquad \underline{-(x^2 + \quad x \quad + \quad 1)} \\
\qquad\qquad\qquad\qquad\qquad 0
\end{array}
$$

2.4. Feladat. *Mi a maradék $x^{64} + x^{54} + x^{14} + 1$et osztjuk $x^2 - 1$-egyel illetve $x^2 + 1$-gyel.*

Megoldás: Ezen feladat során egy új technikát fogunk alkalmazni, az f-et $x - b$-vel osztjuk ekkor a maradék $f(b)$ lesz:

1. $x^2 - 1$-egyel osztva:

   $$x^{64} + x^{54} + x^{14} + 1 = (x^2 - 1)q(x) + (ax + b)$$

   Az x helyére ± 1-et helyettesítve kapjuk 1 esetén: $a + b = 4$ és -1 esetén: $-a + b = 4$ adódik így a maradékunk a 4.

2. $x^2 + 1$-egyel osztva:

   $$x^{64} + x^{54} + x^{14} + 1 = (x^2 + 1)q(x) + (ax + b)$$

   Ebben az esetben az x helyére $\pm i$-t helyettesítünk, ekkor i esetén $ai + b = 0$ így a maradékunk 0.

3. fejezet

Irreducibilitás racionális számtest fölött

Eddig a $\mathbb{C}$ illetve $\mathbb{R}$ testek fölött vizsgáltuk a polinomokat, most viszont a racionális testek felett fogjuk vizsgálni őket, amely fölött már nem tudjuk olyan könnyen vizsgálni, mint eddig. A $\mathbb{Q}$ fölötti polinomok akárhányadfokúak lehetnek. Az eddig bizonyított állítások segítenek ebben, mert ha találunk egy racionális gyököt, akkor tudjuk, hogy a polinom nem lehet irreducibilis, hacsak nem elsőfokú. Az alábbiakban egy eljárást ismertetünk a racionális gyökök megkeresésére.

Ha adott egy racionális együtthatós polinom, akkor szorozzuk be az együtthatók nevezőivel. Így, egy egész együtthatós polinomot kapunk, amelynek gyökei ugyanazok, mint a kiinduló polinomé. Így elegendő az egész együtthatós polinomok racionális gyökeit megkeresni. Erre szolgál a következő tétel.

3.0.3. Tétel:. *Tegyük fel, hogy a p/q már nem egyszerűsíthető tört gyöke az f egész együtthatós polinomnak. Ekkor a számláló osztja f konstans tagját, a nevező pedig osztja f főegyütthatóját.*

Az előző tételt racionális gyöktesztnek szokás nevezni.

Bizonyítás: Az, hogy a tört miért nem egyszerűsíthető, azt jelenti, hogy p és q relatív prím egész számok. Legyen $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$. Ekkor p/q-t behelyettesítve, majd q^n-nel beszorozva

$$a_0q^n + a_1pq^{n-1} + ... + a_np^n = 0$$

adódik. Ebben az összegben mindegyik tag oszható p-vel, kivéve esetleg a legelsőt. Mivel a 0 is osztható p-vel, ezért a legelső tag is, tehát $p|a_0q^n$. De p és q relatív prímek, és így $p|a_0$. Ugyanezzel a módszerrel kapjuk a $q|a_n$ oszthatóságot is.

A következő feladat mutatja ennek a tételnek az alkalmazását és segíthet, ha a polinomnak

a komplex gyökeit ismerjük.

3.1. Feladat. *Mutassuk meg, hogy $x^4 + 36$ irreducibilis $\mathbb{Q}$ felett.*

Először a komplex gyököket kell meghatározni. Ezt egyenlet rendezés és gyökvonás segítségével érjük el.

$$x = \sqrt{3}(\pm 1 \pm i)$$

Ennek a következő a gyöktényezős alakja:

$$x^4 + 36 = (x - \sqrt{3} - \sqrt{3}i)(x - \sqrt{3} + \sqrt{3}i)(x + \sqrt{3} - \sqrt{3}i)(x + \sqrt{3} + \sqrt{3}i) \quad .$$

Az előbbi felbontásból láthatjuk, hogy egyik gyök sem valós így, ha a $x^4 + 36$ felbomlik $\mathbb{Q}$ felett, akkor csak az alábbi $f(x)$ és $g(x)$ polinom szorzata lehet. Az f és g gyökei összesen kiadják a fenti négy komplex gyököt, mert az f és g valósegyütthatósak, gyökeik konjugáltak kell, hogy legyenek.

$$f(x) = r(x - \sqrt{3} - \sqrt{3}i(x - \sqrt{3} + \sqrt{3}i) = r(x^2 - 2\sqrt{3}x + 6),$$

$$g(x) = s(x + \sqrt{3} - \sqrt{3}i(x + \sqrt{3} + \sqrt{3}i) = s(x^2 + 2\sqrt{3}x + 6),$$

ahol r és s eleme a valós számoknak és a szorzatuk 1. Az f és g polinomok racionális együtthatósok, az r is racionális szám és az x együtthatója is: $-2r\sqrt{3}$ és ezzel ellentmondásba ütköztünk, mert akkor az $r = 0$ miatt $\sqrt{3}$ is raconális lenne. Így az eredeti polinomunk $x^4 + 36$ irreducibilis $\mathbb{Q}$ felett.

3.1. Schönemann-Eisentesin kritérium

Az első ilyen módszer a Schönemann-Eisenstein kritérium, amelynek alkalmazásával bizonyos speciális polinomokról könnyen be tudjuk látni, hogy irreducibilis $\mathbb{Q}$ fölött. Abban az esetben ha a Schönemann-Eisentesin kritérium nem teljesül, még lehet a polinomunk irreducibilis. A következő tételeket a Newton-poligon speciális eseteként bizonyítom a 3.5. fejezetben.

3.1.1. Tétel:. *A Schönemann-Eisenstein irreducibilitási kritérium: Legyen f egész együtthatós, nem konstans polinom. Ha van olyan p prímszám, amelyre teljesül, hogy*

1. *p nem osztja f főegyütthatóját;*

2. *p osztja f összes többi együtthatóját;*

3. *p^2 nem osztja f konstans tagját*

akkor f irreducibilis $\mathbb{Q}$ fölött.

3.1.1. Állítás:. *Fordított Schönemann-Eisenstein-kritérium: f egy egész együtthatós, nem konstans polinom. Ha létezik olyan p prímszám, amelyre*

1. *p nem osztja f konstans tagját;*

2. *p osztja f összes többi együtthatóját;*

3. *p^2 nem osztja f főegyütthatóját*

akkor f irreducibilis $\mathbb{Q}$ fölött.

3.1.1. Schönemann-Eisenstein-kritérium alkalmazása

A következő polinomokról döntsük el, hogy melyekre alkalmazható közvetlenül a Schönemann-Eisentesin-kritérium.

3.2. Feladat. $x^{11} + 2x + 18$

Megoldás: A feladat során érdemes olyan prímet választani, amely a főegyütthatót nem osztja. Jelen esetben a keresett prímünk $p = 2$, mert ez osztja a többi együtthatót azaz a 2-t és a 18-at is viszont a négyzete azaz $p^2 = 4$ nem osztja a konstans tagot a 18-at.

3.3. Feladat. $x^{11} + 2x + 12$

Megoldás: Az előző megoldásra alapozva a $p = 2$ itt megfelelő lehet, azonban a $p^2 = 4$ már osztja a konstans így a polinomunkról ezzel a módszerrel nem tudjuk eldönteni, hogy irreducibilis-e vagy sem.

3.4. Feladat. $x^{11} + 12x + 5$

Megoldás: A feladatunk megoldása során az előző tétel feltételein megyünk végig és ezek alapján keressük meg a prímünket.

1. Ebben az esetben a második kritérium nem teljesül így ezzel a módszerrel nem tudjuk megállapítani a polinomunkról, hogy irreducibilis vagy sem.

3.5. Feladat. $x^{11} + 24$

Megoldás:A feladatunk megoldása során az előző tétel feltételein megyünk végig és ezek alapján keressük meg a prímünket.

1. $2 \nmid 1$ és $3 \nmid 1$ $\surd$
2. $24 = 2^3 \cdot 3$ $\surd$
3. A két prímünk a $p = 2$ és a $p = 3$. Négyzetük a $p^2 = 4$ és $p^2 = 9$.

A konstans tagunkat osztja a 4, de nem osztja a 9, így a megfelelő prímünk a 3. Teljesül a kritérium, a polinomunk irreducibilis.

3.6. Feladat. $x^{11} + 72$

Megoldás: Ismét az előző módszert alkalmazzuk a feladat megoldása során.

1. $2 \nmid 1$ és $3 \nmid 1$ $\surd$
2. $72 = 3^2 \cdot 2^3$ $\surd$
3. Ekkor kiderült melyik az a két prím, ami megfelelő lehet a 2 és a 3. Az előző prímek négyzete: $2^2 = 4$ és $3^2 = 9$.

Mindkét prímünk osztja a konstans tagot így a kritérium nem teljesül.

3.7. Feladat. $x^{13} - 35$

Megoldás: Először megnézzük, hogy melyek azok a prímek, amelyek szóba jöhetnek. Megnézzük az első feltételt: a keresett prím nem osztja az egyenlet főegyüttható ját így jelen esetben 1 a főegyüttható tehát eddig bármelyik prím megfelel. A következő feltétel alapján a prímünk osztja a többi együthatót, azaz $35 = 5 \cdot 7$. Az utolsó feltétel alapján, a prím négyzete nem osztja a konstans tagot, azaz 5^2 és a 7^2 nem oszthatja, jelen esetünkben egyik sem, tehát a keresett prímeink az 5 és a 7.

Megjegyzés: A feladatok során előfordul, hogy közvetlenül nem tudjuk alkalmazni a Schönemann-Eisenstein kritériumot, azonban átalakítás után már igen. A következő feladat erre mutat példát:

3.8. Feladat. *Irreducibilis-e a következő polinom* $f(x) = x^4 + 1$ $\mathbb{Q}$ *fölött?*

Megoldás: A feladat során vegyük az $f(x+1)$ polinomot, ekkor a következőt kapjuk:

$$(x+1)^4+1 = x^4+4x^3+6x^2+4x+2$$

Ekkor már alkalmazhatjuk a kritériumot $p=2$ tehát:

1. $2 \nmid 1$ $\surd$
2. $2|4$ $2|6$ $\surd$
3. $2^2 \nmid 2$ $\surd$

3.2. mod p vizsgálata

3.9. Feladat. *Mutassuk meg, modulo 3 szerint, hogy* $6x^4+3x+1$ *irreducibilis* $\mathbb{Q}$ *felett.*

Megoldás: Ebben az esetben nem tudjuk alkalmazni a Schönemann-Eisenstein-kritériumot, de ha f főegyütthatóit fordított sorrendben írjuk fel, akkor már igen. Tehát a polinom irreducibilis.

3.3. A polinom általános együtthatókkal való szorzatra bontása

3.10. Feladat. *Mutassuk meg, hogy* $f(x)=x^4+x^2+x+1$ *irreducibilis* $\mathbb{Q}$ *felett.*

Megoldás: Ennek a polinomnak nincs racionális gyöke így csak a következő két másodfokú polinom szorzata lehet:

$$x^4+x^2+x+1 = (ax^2+bx+c)(ux^2+vx+w) \quad ,$$

ahol a,b,c,u,v,w egész számok a második Gauss-lemma miatt. Beszorozva, majd összehasonlítva az együtthatókat, a következő egyenletrendszert kapjuk.

$$au=1,\ av+bu=0,\ aw+bv+cu=1,\ bw+cv=1,\ cw=1$$

Láthatjuk $au=1$ ebből adódik, hogy $a=u=1$ vagy $a=u=-1$ lehet. A második egyenletből $v+b=0$. Az előző elv alapján az utolsó két egyenletből $c=w=b+v=1$ vagy $c=w=b+v=-1$ adódik, ez nem lehetséges, mert $b+v=0$.

3.11. Feladat. *Mutassuk meg, hogy* $f(x)=x^4+x+1$ *irreducibilis* $\mathbb{Q}$ *felett.*

Megoldás: Hasonlóan az előző példához, csak akkor nem használtuk ki az x^2-es együtthatójából kapott egyenletet. Azonban most láthatjuk, hogy $\mathbb{Z}_2$ felett irreducibilis és a főegyütthatója páratlan ezért $\mathbb{Q}$ fölött is irreducibilis.

3.4. A módszerek alkalmazása

Ebben a fejezetben az előző módszerek alkalmazásával oldom meg a feladatokat.

3.12. Feladat. *Irreducibilis-e a* $3x^7 - 6x^6 + 6x^2 + 3x - 2$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás: Alkalmazzuk a fordított Schönemann-Eisentein-kritérumot $p = 3$-ra és így igazoltuk, hogy irreducibilis a polinom.

3.13. Feladat. *Irreducibilis-e a* $3x^7 + x^6 + 6x^2 + 2x - 2$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás: Ez a polinom nem irreducibilis a gyöke:-1. Ezt a racionális gyökteszt segítségével állapítottuk meg.

3.14. Feladat. *Irreducibilis-e az* $x^{16} + 2$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás:A Schönemann-Eisenstein-kritérium alapján $p = 2$-re irreducibilis.

1. $2 \nmid 1$ $\surd$
2. $2|2$ $\surd$
3. $2^2 \nmid 2$ $\surd$

3.15. Feladat. *Irreducibilis-e az* $x^4 - 14x^2 + 9$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás: Irreducibilis, gyökei:$\pm\sqrt{2} \pm \sqrt{5}$

3.16. Feladat. *Irreducibilis-e a* $3x^7 + 6x - 18$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás: Irreducibilis, Schönemann-Eisenstein-kritérium miatt $p = 2$-re.

1. $2 \nmid 3$ $\surd$
2. $2|18$ $2|6$ $\surd$
3. $2^2 \nmid 18$ $\surd$

3.17. Feladat. *Irreducibilis-e az* $x^5 + 729$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás: Ebben az esetben helyettesítéssel tudjuk megállapítani. $y = \frac{x}{3}$ ekkor:

$$\frac{x^5+729}{243} = y^5 + 3$$

Ebben az esetben tudjuk alkalmazni a Schönemann-Eisenstein-kritérium $p = 3$-ra.

3.18. Feladat. *Irreducibilis-e az* $x^4 + 4x + 1$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás: Az $x \to x + 1$ helyettesítéssel:

$$(x+1)^4 + 4(x+1) + 1 = x^4 + 4x^3 + 6x^2 + 8x + 6$$

Ekkor tudjuk alkalmazni a Schönemann-Eisenstein-kritérium $p = 2$-re.

1. $2 \nmid 1$ $\surd$
2. $2|4$ $2|6$ $2|8$ $\surd$
3. $2^2 \nmid 6$ $\surd$

3.19. Feladat. *Irreducibilis-e az* $x^{20} + 20$ *polinom* $\mathbb{Q}$ *felett?*

Megoldás: Schönemann-Eisenstein-kritérium $p = 5$-ra

1. $5 \nmid 1$ $\surd$
2. $5|20$ $\surd$
3. $5^2 \nmid 20$ $\surd$

3.20. Feladat. *Igazoljuk, hogy* $x^n + x + 3$ *polinom irreducibilis.*

Megoldás: Ha ez a polinom felbomlana, akkor az egyik szorzótényező konstans tagja ± 1 kellene, hogy legyen. Ekkor viszont, a Viete-formulák miatt, annál a tényezőnél a gyökök szorzata is ± 1. Tehát lenne egy olyan komplex gyök, aminek az abszolútértéke legfeljebb 1. Azonban az eredeti polinomnak nincs ilyen gyöke! Ugyanis ha $|\alpha|$ legfeljebb 1, akkor $|\alpha^n|$ legfeljebb 1. Tehát a háromszögegyenlőtlenség miatt $|\alpha^n + \alpha|$ legfeljebb $1 + 1 = 2$. Viszont ha $\alpha^n + \alpha + 3 = 0$, akkor $\alpha^n + \alpha = -3$, aminek 3 az abszolútértéke, ami nagyobb, mint 2. Tehát a feltevés hamis, a polinomunk irreducibilis.

3.5. Racionális együtthatós polinomok Newton-poligonja

A következő témakör az algebra tanulmányaim során nem szerepelt, számomra teljesen új és érdekes volt. Először egy bevezető definícióval szeretném a későbbiek definiált newton poligont bevezetni.

3.5.1. Definíció. *Legyen* $p \in \mathbb{Z}$ *egy rögzített prímszám. Egy* $0 \neq a \in \mathbb{Q}$ *racionális szám p-adikus értékelése alatt az a prímtényezős felbontásban p kitevőjét értjük. Azaz, ha* $a = p^\alpha u/v$*, ahol* $(p, u) = (p, v) = 1$ *és* $\alpha \in \mathbb{Z}$*, akkor p-adikus értékelése* $v_p(a) = \alpha$ *Továbbá legyen* $v_p = \infty$*.*

Megjegyzés: Vegyük észre, hogy minden $0 \neq a \in \mathbb{Q}$ ilyen alakba írható.

3.5.1. Lemma. *$v_p(ab) = v_p(a) + v_p(b)$,*
$v_p(a+b) \geq min(v_p(a), v_p(b))$ és egyenlő, ha $v_p(a) \neq v_p(b)$

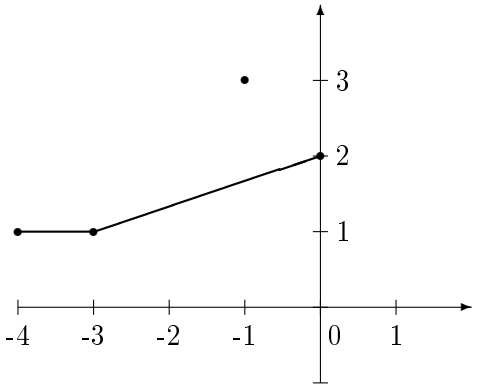
Bizonyítás: Ha $a = p^\alpha u_1/v_1$ és $b = p^\beta u_2/v_2$, akkor $ab = p^{\alpha+\beta}u_1u_2/v_1v_2$. Továbbá, ha $\alpha \leq \beta$, akkor $a + b = p^\alpha \frac{u_1v_2+p^{\beta-\alpha}u_2v_1}{v_1v_2}$, ahol p nem osztja v_1v_2 és $\beta > \alpha$ esetén $p \nmid u_1v_2 + p^{\beta-\alpha}u_2v_1$.

3.5.2. Definíció. *Legyen $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ egy egész együtthatós n-edfokú polinom és tegyük fel, hogy $a_n \neq 0 \neq a_0$. Az f-polinom (p-hez tartozó) Newton-poligonja a síkon a $\{(-i, v_p(a_i))|i = 0, ..., n\} \subset \mathbb{Z}^2 \subset \mathbb{R}^2$ rácspontok alsó konvex burka, mint a $(-n, v_p(a_n))$ és a $(0, v_p(a_0))$ pontokat összekötő töröttvonal. (Azaz a konvex burok alsó határvonala.) Ha valamely $i - re$ $a_i = 0$ és így a $v_p(a_i) = \infty$, akkor ezt a pontot figyelmen kívül hagyjuk. A Newton-poligon meredeksége az $S(f) := \{s_n, ..., s_1\}$ multihalmaz (egy szám többször is szerepelhet), ahol s_i a töröttvonal meredeksége a függőleges $x = -i$ és $x = -i + 1$ egyenesek között.*

Megjegyzés: A Newton-poligont olyan polinomokra is értelmezhetjük, melyeknek konstans tagja 0. Ekkor ha j a legkisebb indexe, melyre $a_j \neq 0$, akkor a Newton-poligon töröttvonala csak $(-j, v_p(a_j))$-ig, és a meredekségeinek multihalmazát kiegészíthetjük j db ∞-nel. Így az $S(f)$ multihalmaz minden esetben $deg(f)$ elemű.

3.21. Feladat. *Mi $2x^4 + 2x^3 + 8x + 4$ egyenlet Newton-poligon töröttvonala $p = 2$ esetén?*

Megoldás: A következő módszerrel tudjuk ezt meghatározni:
Először megnézzük a kitevőket. Ezek lesznek a helyek a koordinátarendszerben, majd a hozzájuk tartozó együtthatókat 2-vel osztva megnézzük, hogy milyen eredményeket adnak. Ezek lesznek az y értékek. Ezek alapján a Newton-poligon törött vonala:



3.5.1. Állítás:. *A Newton-poligon csúcsai rácspontok, meredekségeire teljesül $s_n \leq s_{n-1} \leq \ldots \leq s_1 \in \mathbb{Q}$*

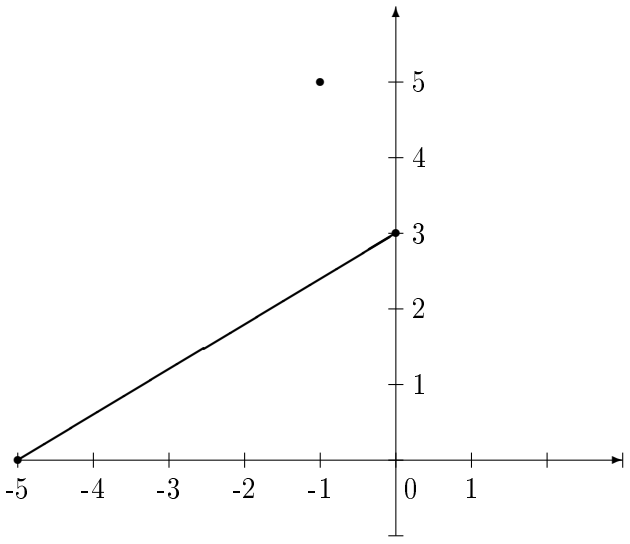
Bizonyítás: Véges sok konvex burkának csúcsai a véges sok pont közül kerülnek ki, a Newton-poligon esetében ezek a rácspontok. A meredekségekre vonatkozó egyenlőség a konvexitás következménye.

3.5.1. Tétel:. *Legyenek* $f(x)$, $g(x) \in \mathbb{Q}[x]$ *polinomok, melyekre* $f(0) \neq 0 \neq g(0)$. *Ekkor a Newton-poligon meredekségeire teljesül:* $S(fg) = S(f) \cup S(g)$ *(mint multihalmazok).*

Bizonyítás: Legyen $f(x) = \sum_{i=0}^{n} a_i x^i$ $g(x) = \sum_{j=0}^{k} b_j x^j$. Elég belátni, hogy fix $s \in \mathbb{Q}$ s multiplicitása $S(fg)$-ben megegyezik $S(f)$-beli és $S(g)$-beli multiplicitások összegével. Ehhez kiszámoljuk $f(x)$ és s ismeretében s multiplicitását $S(f)$-ben. Vegyük az $y = sx + c$ egyenletű egyenest. Ennek meredeksége pedig s. Legyen $c = c_f \in \mathbb{Q}$ az a konstans, melyre az $y = sx + c_f$ egyenes érinti s Newton-poligonját. Másszóval $c_f := \min_{0 \leq i \leq n}(v_p(a_i) - s(-i))$. Legyen továbbá $M = M_f$ (illetve $m = m_f$) a maxiális (illetve minimális) i index, melyre a c_f-et definiáló minimum felvétetik. Másszóval $M_f := \max(i | v_p(a_i) + si = c_f)$, illetve $m_f := \min(i | v_p(a_i) + si = c_f)$. Vegyük észre, hogy ekkor s multiplicitása az $S(f)$ multihalmazban nem mást mint, $M_f - m_f$.

3.22. Feladat. $x^5 + 32x + 8$ *polinomnak rajzoljuk fel a Newton-poligon töröttvonalát.*

Megoldás:



Megjegyzés: Látthatjuk, hogy nincs rajta rácspont ebből pedig az következik, hogy irreducibilis a feladatban megadott polinom.

3.5.2. Lemma. $c_{fg} = c_f + c_g$, $M_{fg} = M_f + M_g$, $m_{fg} = m_f + m_g$

Bizonyítás: A polinom szorzásának definíciójából $fg(x) = \sum_{r=0}^{n+k}(\sum_{i=0}^{r} a_i b_{i-r})x^r$. A fejezet első lemmája miatt:

$$v_p(\sum_{i=0}^{r} a_i b_{i-r}) \geq min_{0\leq i\leq r}(v_p(a_i)+v_p(b_{r-i})+rs =$$
$$= min_{0\leq i\leq r}(v_p(a_i)+si+v_p(b_{r-i}+s(r-i)) \geq$$
$$\geq min_{0\leq i\leq r}(v_p(a_i)+si+min_{0\leq j\leq k}(v_p(b_j)+sj) = c_f+c_g.$$

A fenti egyenlet bal oldalán minimumot véve (r fut 0-tól $n+k$-ig) azt kapjuk, hogy $c_{fg} \geq c_f + c_g$. Továbbá vegyük észre, hogy $i > M_f$ vagy $i < m_f$ esetén $v_p(a_i) + si > c_f$. Hasonlóképp, ha $r - i > M_g$ vagy ha $r - i < m_g$, akkor $v_p(b_{r-i}) + s(r - i) > c_g$. Tehát ha $r > M_f + M_g$ vagy ha $r < m_f + m_g$, akkor a fenti egyenletben szigorú egyenlőtlenség van. Ha pedig $r = M_f + M_g$ vagy $r = m_f + m_g$, akkor egyenlőség áll fenn. Ezzel mindhárom állítást beláttuk.

3.5.1. Következmény. *Ha $f(x) \in \mathbb{Q}[x]$, p prím, és f p-hez tartozó Newton-poligonja egy darab szakasz, melyen a két végén kívül nincs más rácspont, akkor f irreducibilis.*

Bizonyítás: Ez esetben f Newton-poligonját nem lehet két rácstöröttvonal valódi uniójára bontani.

3.5.2. Következmény. *(Schönemann-Eisenstein kritérium) Ha $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ polinomra $p \nmid a_n$, $p|a_i (0 \leq i < n)$ és $p^2 \nmid a_0$, akkor f irreducibilis $\mathbb{Q}$ fölött.*

Bizonyítás: Ez esetben a Newton-poligon a $(-n, 0)$ és a $(0, 1)$ pontokat összekötő szakasz, melynek belsejében nincs rácspont.

3.5.3. Következmény. *(fordított Schönemann-Eisenstein kritérium) Ha $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ polinomra $p|a_0$, $p|a_i (0 < i \leq n)$ és $p^2|a_n$, akkor f irreducibilis $\mathbb{Q}$ fölött.*

Bizonyítás: Hasonlóan a Schönemann-Eisenstein kritériumhoz, a Newton-poligon a $(-n, 1)$ és a $(0, 0)$ pontokat összekötő szakasz, melynek belsejében szintén nincs rácspont.

4. fejezet

Egész együtthatós polinomok

Ezen fejezet során $\mathbb{Z}[x]$ gyűrű esetén, vizsgáljuk az irreducibilis polinomokat.
Egy példán keresztül vezetem be ezt a fejezetet.

4.1. Feladat. *Irreducibilis-e a $2x$ polinom $\mathbb{Z}$ fölött?*

Megoldás: Nem irreducibilis, mert a $2x = 2 \cdot x$ nemtiriviális felbontás, mert $\mathbb{Z}[x]$ egységei ± 1 és a 2 illetve az x sem az.
Ahhoz, hogy meg tudjuk állapítani $\mathbb{Z}$ fölött, hogy irreducibilis-e a polinomunk, fel kell bontani úgy, hogy kiemeljük belőle az együtthatóinak a legnagyobb közös osztóját.

4.2. Feladat. *Emeljünk ki a következő polinomból az együtthatóinak legnagyobb közös osztóját* $143x^3 + 55x + 99 = 11(13x^3 + 5x + 9)$

Megoldás: $143x^3 + 55x + 99 = 11(13x^3 + 5x + 9)$. Az így kapott polinomot $(13x^3 + 5x + 9)$ primitívnek fogjuk nevezni, aminek a pontos definíciója a következőképpen szól.

4.0.3. Definíció. *Egy egész együtthatós nem nulla polinomot primitívnek nevezünk, ha együtthatóinak legnagyobb közös osztója 1.*

A következő lemmákat és a belőlük származó következményeket Gauss-lemmának hívjuk összefoglalásként.

4.0.3. Lemma. *Első Gauss-lemma: Ha $p \in \mathbb{Z}$ prímszám, akkor p a $\mathbb{Z}[x]$-ben mint konstans polinom is prímtulajdonságú.*

Az előző lemmára kétféle bizonyítás van, az egyik elemi számolásokból áll, a másik pedig felhasználja a p modulo számolásról tanultakat, viszont közülük csak a mod p számolást mutatom be.

Bizonyítás: Tudjuk, hogy p nem nulla és ± 1 így $\mathbb{Z}[x]$-ben nem egység. Tegyük fel, hogy $p|fg$, ahol fg $\mathbb{Z}[x]$-ben. Meg kell mutatni, hogy $p|f$ vagy $p|g$.
Vegyük az f, g és fg polinomokat mod p, az eredményt jelölje $\overline{f}, \overline{g}, \overline{fg} \in \mathbb{Z}_p[x]$. Ekkor $\overline{fg} = \overline{f}\overline{g}$. Mivel $p|fg$, az $\overline{fg}$ a nullapolinom. De $\mathbb{Z}_p$ test, és így a $\mathbb{Z}_p[x]$ nullosztómentes. Tehát $\overline{f}$ és $\overline{g}$ egyike nulla, vagyis f és g egyike osztható p-vel.

4.0.4. Következmény. *Első Gauss-lemma, első következmény: Primitív polinomok szorzata is primitív.*

Bizonyítás: Tegyük fel, hogy f és $g \in \mathbb{Z}$ primitív polinomok. Azt kell megmutatni, hogy fg nem osztható egységtől különböző egész számmal. Ha osztható lenne, akkor lenne egy p prímosztója is. Az előző lemma miatt ekkor $p|f$ vagy $p|g$, ami nem lehet, hiszen f és g primitívek.

4.0.5. Következmény. *Első Gauss-lemma, második következmény: Legyen f egész együtthatós primitív polinom. Ha g olyan racionális együtthatós polinom, melyre $h = fg$ egész együtthatós, akkor g is egész együtthatós. Speciálisan, ha f osztója egy h egész együtthatós polinomnak $\mathbb{Q}[x]$-ben, akkor f osztója h-nak $\mathbb{Z}[x]$-ben is.*

Bizonyítás: Hozzuk g együtthatóit közös nevezőre, és emeljük ki a számlálókból a legnagyobb közös osztójukat. Így a $g = (s/t)g_0$ felbontást kapjuk, ahol g_0 már primitív, egész együtthatós polinom, és az s,t egész számokról az s/t törtet egyszerűsítve feltehetjük, hogy relatív prímek. A $h = fg$ egyenlőséget t-vel megszorozva kapjuk, hogy $th = sfg_0$. Ha p prímosztója t-nek, akkor $p|sfg_0$, az első Gauss lemma miatt tehát $p|s$ vagy $p|f$ vagy $p|g_0$. Mindhárom lehetetlen. Az első azért mert t és s relatív prímek, a másik kettő pedig f és g_0 primitívek. A t számnak tehát nincs prímosztója, vagyis t egység, és így $g = (s/t)g_0$ tényleg egész együtthatós polinom.

4.0.4. Lemma. *Második Gauss-lemma: Tegyük fel, hogy az $f \neq 0$ egész együtthatós polinomot felbontottuk racionális együtthatós g és h polinomok szorzatára. Ekkor g és h megszorozható alkalmas racionális számokkal úgy, hogy a kapott g_0 és h_0 polinomok egész együtthatósak legyenek, és $f = g_0h_0$ teljesüljön.*

Bizonyítás: Írjuk fel a g és h polinomokat rg_1 és sh_1 alakban, ahol r,s racionális számok, g_1 és h_1 pedig egész együtthatós primitív polinomok. Ekkor $f = (rs)(g_1h_1)$. Az első Gauss-lemma első következménye miatt pedig g_1h_1 primitív polinom, a második következménye miatt tehát $n = rs$ egy egész együtthatós polinom, azaz egész szám. Így a $g_0 = ng_1$ és $h_0 = h_1$ választás megfelel a követelményeknek.

4.0.2. Tétel:. *Egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ fölött, ha*

1. *vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),*
2. *vagy egy (nem konstans) primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.*

Bizonyítás: A $\mathbb{Z}$-beli felbonthatatlan számokról láttuk, hogy mint konstans polinomok szintén felbonthatatlanok. Tegyük föl, hogy f nem konstans primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis. Ha $f = gh$ egy felbontás, ahol $g, h \in \mathbb{Z}[x]$, akkor a $\mathbb{Q}$ fölötti irreducibilitás miatt g és h egyike egység $\mathbb{Q}$-ban, vagyis konstans, és így egész szám, hiszen g és h egész együtthatós. Mivel f primitív, ez az egész szám csak egység lehet, és így az $f = gh$ felbontás $\mathbb{Z}$-ben is triviális. Tehát f irreducibilis $\mathbb{Z}$ fölött.
Megfordítva, tegyük föl, hogy f irreducibilis $\mathbb{Z}[x]$-ben. Ekkor f fölírható nk alakban, ahol n egész szám, és k primitív polinom. Mivel f irreducibilis, ez a felbontás tiriviális. Így van n egység és akkor f primitív, vagy k egység és akkor f konstans.
Ha f konstans, akkor nyilván felbonthatatlannak kell lennie $\mathbb{Z}$-ben, hiszen a $\mathbb{Z}$-beli nemtriviális felbontások egyben $\mathbb{Z}[x]$-beli nemtriviális felbontások is. Ha f nem konstans primitív polinom, akkor meg kell mutatnunk, hogy nemcsak $\mathbb{Z}$, hanem $\mathbb{Q}$ fölött is irreducibilis.
Tegyük föl, hogy f előáll a nála alacsonyabb fokú (és ezért nem konstans) racionális együtthatós g és h polinomok szorzataként. A második Gauss-lemma miatt ekkor f fölírható $g_0 h_0$ alakban is, ahol ezek már egész együtthatós polinomok, és g_0 foka megegyezik g fokával, h_0 foka pedig h fokával. Tehát g_0 és h_0 egyike sem konstans, és így ez nemtriviális felbontás $\mathbb{Z}$ fölött.

4.0.2. Állítás:. *A $\mathbb{Z}[x]$ gyűrű minden irreducibilis eleme prímtulajdonságú.*

Bizonyítás: Az előző tétel miatt ez az irreducibilis elem vagy egy $\mathbb{Z}$-beli prím (mint konstans polinom), vagy egy primitív f polinom, amely $\mathbb{Q}$ fölött irreducibilis. Az első esetben az első Gauss-lemma pont az állítást mondja ki. A második esetben tegyük föl, hogy f osztója $\mathbb{Z}[x]$-ben a gh szorzatnak, ahol g és h egész együtthatós polinomok. Mivel $\mathbb{Q}[x]$-ben igaz az alaptétel, f prímtulajdonságú $\mathbb{Q}[x]$-ben. Az első Gauss lemma második következménye miatt ez az oszthatóság $\mathbb{Z}[x]$-ben is fönnáll. Így f tényleg prímtulajdonságú.

4.3. Feladat. *Bontsuk fel $\mathbb{Z}$ fölött irreducibilis szorzatára a $30x^3 - 30$ polinomot.*

Megoldás:
$30x^3 - 30 = 2 \cdot 3 \cdot 5 \cdot (x-1) \cdot (x^2 + x + 1)$. A felbontásban irreducibilis $2, 3, 5$ tényezők irreducibilisek $\mathbb{Z}$ fölött, mert $\mathbb{Z}$-beli prímek. Az $x - 1$ és$(x^2 + x + 1)$is, mert primitív és $\mathbb{Q}$ fölött irreducibilis.

4.4. Feladat. *Irreducibilis-e az* $x^5 + 5x + 26$ *polinom* $\mathbb{Z}$ *fölött?*

Megoldás: A megoldás során x helyére $x - 1$ helyettesítünk $(x-1)^5 + 5(x-1) + 26 = (x-1)^5 + 5x + 21$ és ezután felhasználjuk a Schönneman-Eisenstein kritériumot $p = 5$ esetén.

1. $5 \nmid 1$-et $\surd$
2. $5|5$ $\surd$
3. $5^2 \nmid 21$ $\surd$

4.5. Feladat. *Irreducibilis-e a* $3x^7 + 6x - 18$ *polinom* $\mathbb{Z}$ *fölött?*

Megoldás: Kiemelek 3-at$\rightarrow 3(x^7 + 2x - 6)$

4.6. Feladat. *Irreducibilis-e a* $x^6 + 1$ *polinom* $\mathbb{Z}$ *fölött?*

Megoldás: Ha felbontjuk a polinomot $(x^2 + 1)(x^4 - x^2 + 1)$-re akkor láthatjuk, hogy nem irreducibilis az eredeti polinomom.

4.7. Feladat. *Irreducibilis-e a* $x^3 + 7x - 3$ *polinom* $\mathbb{Z}$ *fölött?*

Megoldás:A racionális gyökteszt alkalmazva nincs racionális gyöke, ezenkívül harmadfokú tehát irreducibilis.

4.8. Feladat. *Irreducibilis-e a* $x^4 + 3x^3 + x^2 + 1$ *polinom* $\mathbb{Z}$ *fölött?*

Megoldás: Ennek a polinomnak -1 a gyöke így nem irreducibilis.

5. fejezet

A körosztási polinomok

Ebben a fejezetben a körosztási polinomokról és az irreducibilitás közti összefüggésről lesz szó. A polinomok gyökei az n-edik primitív egységgyökök, amelyek akkor adódnak, amikor az $x^n - 1$ polinomot irreducibilisek szorzatára bontjuk $\mathbb{Z}$ fölött.
Először deifináljuk, hogy mit is jelent a körosztási polinom.

5.0.4. Definíció. *Ha $n \geq 1$ egész, akkor Φ_n jelöli az n-edik körosztási polinomot, vagyis azt a normált polinomot, melynek gyökei pontosan primitív n-edik egységgyökök (mindegyik egyszeres). Képletben:*

$$\Phi_n(x) = (x - \xi_1) \dots (x - \xi_{\varphi(n)}) \quad ,$$

ahol $\xi_1 \dots \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes olyan komplex szám, melynek rendje n.

A deifníciót alkalmazva kis n számok esetén:

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x - (-1) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1$$

Ezeket a későbbi feladatok során felhasználjuk.

5.1. Feladat. *Számítsuk ki a hatodik körosztási polinomot.*

Megoldás: Először a hatodik egységgyököket kell megállapítanunk. Ez esetben:

$$\eta = \cos\tfrac{2\pi}{n} + i \sin\tfrac{2\pi}{n} \to \eta = \cos 60^\circ + i \sin 60^\circ$$

Ez a primitív hatodik egységgyök így ennek hatványai a hatodik egységgyökök, amiket a rend definíciójából állapítunk meg:

$$o(\eta) = o(\eta^5) = 6$$

A két primitív harmadik egységgyök:

$$o(\eta^2) = o(\eta^4) = 3$$

A második egységgyök:

$$o(\eta^3) = 2 \text{ és } \eta^3 = -1$$

Végül az első egységgyök:

$$o(\eta^6) = 1 \text{ és } \eta^6 = 1$$

A $x^6 - 1$ polinom gyökei a hat darab hatodik egységgyök, ekkor azt kapjuk, hogy:

$$x^6 - 1 = (x - \eta)(x - \eta^2)(x - \eta^3)(x - \eta^4)(x - \eta^5)(x - \eta^6)$$

Most pedig a rendek szerint csoportosítjuk ezeket:

$$x^6 - 1 = [(x - \eta)(x - \eta^5)][(x - \eta^2)(x - \eta^4)][(x - \eta^3)(x - \eta^6)] = \Phi_6(x) \cdot \Phi_3(x) \cdot \Phi_2(x) \cdot \Phi_1(x)$$

Most pedig felhasználjuk az előzőekben említett körosztási polinomok megoldását. Ezen kívül felhasználjuk a $\Phi_1(x)\Phi_3(x) = x^3 - 1$ összefüggést.

$$\Phi_6(x) = \frac{x^6-1}{\Phi_3(x)\Phi_2(x)\Phi_1(x)} = \frac{x^6-1}{(x^3-1)\Phi_2(x)} = \frac{x^3+1}{x+1} = x^2 - x + 1$$

5.2. Feladat. *Az előző feladat alapján most állapítsuk meg $n = 12$ esetén a körosztási polinomot.*

Megoldás: $o(\eta) = 12$ ebben az esetben a rendre vonatkozó képlet alapján, a hatványai között lesz négy tizenkettedrendű, két hatodrendű, két negyedrendű, két harmadrendű, egy másodrendű és egy elsőrendű elem. Így:

$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)$$

A 6 osztóihoz tartozó körosztási polinomok szorzata $x^6 - 1$ így:

$$x^{12} - 1 = \frac{x^{12}-1}{\Phi_1\Phi_2\Phi_3\Phi_6\Phi_4} = \frac{x^{12}-1}{x^6-1\Phi_4(x)} = \frac{x^6+1}{x^2+1} = x^4 - x^2 + 1 \quad .$$

Tehát:

$$\Phi_{12} = x^4 - x^2 + 1$$

A két példa alapján most általánosan is felépítem a megoldáshoz vezető utat.

Ehhez szükségünk van a következő lemmára:

5.0.5. Lemma. *Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$.*

Melynek a bizonyítása a következő:

Bizonyítás: Legyen $\eta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Ekkor η primitív n-edik egységgyök, és ezért hatványai az n-edik egységgyököket adják meg. Ezek éppen az $x^n - 1$ gyökei, és mivel n különböző számról van a szó, az $x^n - 1$ gyöktényezős alakja:

$$x^n - 1 = (x - \eta)(x - \eta^2) \dots (x - \eta^n) \quad .$$

Ismét a megfelelő egységgyökök rendjei szerint csoportosítjuk a gyöktényezőket. Jelölje f_d a d rendű egységgyökökhöz tartozó gyöktényezők szorzatát. Így:

$$x^n - 1 = \prod_d f_d(x) \quad .$$

Elég belátni, hogy az itt fellépő d számok pontosan n osztói, és hogy ezekre $f_d = \Phi_d$.

Ha egy d szám fellép, vagyis ha $d = o(\eta^m)$ teljesül valamelyik m-re, akkor $(\eta^m)^n = (\eta^n)^m = 1^m = 1$ miatt n jó kitevője η^m-nek, és így $d|n$. Tehát a fellépő d számok tényleg csak n osztói lehetnek. Tegyük föl, hogy $d|n$. Ekkor Φ_d gyöktényezős felbontásában az összes d rendű komplex szám szerepel, f_d felbontásában pedig az olyan d rendű komplex számok szerepelnek, amik egyben n-edik egységgyökök is. De ezek ugyanazok a számok: mindegyik d-edik egységgyök egyben n-edik egységgyök is. Hiszen ha egy ξ számra $d = o(\xi)|n$, akkor $\xi^n = 1$, ezért ξ egy n-edik egységgyök. Beláttuk tehát, hogy $f_d = \Phi_d$.

Az előző lemma következménye a következő:

5.0.6. Következmény. *Ha $n \geq 1$, akkor a Φ_n körosztási polinom egész együtthatós.*

Bizonyítás: Indirekten bizonyítunk. Tegyük föl, hogy az állítás nem igaz, és legyen n a legkisebb olyan pozitív egész, melyre Φ_n nem egész együtthatós. Az előbbi lemma miatt:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n d \neq n} \Phi_d(x)} \quad .$$

Az n minimalitása miatt a nevezőben csupa egész együtthatós polinom van, amik normáltak is. Ezért a nevező maga is normált, és egész együtthatós. A nevező osztója a számlálónak $\mathbb{C}$ fölött és $\mathbb{Z}[x]$-ben is. Azaz Φ_n mégis egész együtthatós. Ez az ellentmondás igazolja az állítást.

Korábban már említettük, hogy $x^n - 1$ polinom irreducibilis komponensei a körosztási polinomok. Most ezt fogjuk tételben kimondani és bizonyítani.

5.0.3. Tétel:. *Mindegyik körosztási polinom irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ fölött.*

Bizonyítás: Tudjuk a 4.0.2. tételből, hogy Φ_n körosztási polinom ugyanakkor irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ fölött, hiszen primitív és nem konstans. Bontsuk föl $\mathbb{Z}$ fölött irreducibilisek szorzatára: $\Phi_n(x) = f_1(x) \dots f_s(x)$. Az f_s tényezők főegyütthatója csak ± 1 lehet, tehát egyik sem konstans, és így mindegyik f_i irreducibilis $\mathbb{Q}[x]$ fölött is. Azt kell megmutatnunk, hogy ebben a felbontásban csak egy tényező szerepel.

A teljes bizonyításhoz szükségünk van a következő lemmára és annak bizonyítására is.

5.0.6. Lemma. *Legyen $p \nmid n$ prím. Ha egy ε számra $f_1(\varepsilon) = 0$, akkor $f_1(\varepsilon^p) = 0$*

Bizonyítás: Tegyük fel, hogy $f_1(\varepsilon) = 0$, de $f_1(\varepsilon^p) \neq 0$. Mivel $p \nmid n$, az ε^p is primitív egységgyök, azaz gyöke a Φ_n-nek. Ezért ε^p gyöke valamelyik f_j polinomnak, ahol $j \neq 1$. Az indexek számozásával feltehetjük, hogy $j = 2$, tehát $f_2(\varepsilon^p) = 0$. Az $f_1(x)$ és az $f_2(x^p)$ polinomnak ε közös gyöke $\mathbb{Q}$-ban. Mivel f_1 irreducibilis $\mathbb{Q}$ fölött, $f_1(x)$ osztója $f_2(x^p)$ polinomnak $\mathbb{Q}[x]$-ben. De akkor osztója $\mathbb{Z}[x]$-ben is, hiszen f_1 főegyüttthatója ± 1, és így amikor a $g(x) = \frac{f_2(x^p)}{f_1(x)}$ osztást elvégezzük, akkor végig $\mathbb{Z}[x]$-ben maradunk (Első Gauss-lemma második következményére hivatkozva).Vegyük a szereplő polinomok együtthatóit mod p, és jelölje fölül vonással a kapott polinomokat. Ekkor $\overline{f_1}(x)\overline{g}(x) = \overline{f_2}(x^p)$. A $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni. Beláttuk, hogy $\overline{f_2}(x^p) = \overline{f_2}(x)^p$, tehát $\overline{f_1}|\overline{f_2}^p$, ahol az oszthatóság $\mathbb{Z}_p[x]$-ben értendő. Mivel f_1 főegyüttthatója ± 1, az $\overline{f_1}$ polinom sem konstans. Ez a polinom $\mathbb{Z}_p$ fölött nem biztos, hogy irreducibilis, de mindenképp van $\mathbb{Z}_p$ fölött irreducibilis k osztója. Ekkor $k|\overline{f_1}|\overline{f_2}^p$, és mivel az irreducibilis polinomok $\mathbb{Z}_p[x]$-ben prímtulajdonságúak, hiszen $\mathbb{Z}_p$ test, azt kapjuk, hogy $k|\overline{f_2}$. Találtunk tehát egy olyan $k \in \mathbb{Z}_p$ nem konstans polinomot, ami $\overline{f_1}$-nek és $\overline{f_2}$-nek is osztója. Ezért $k^2|\overline{f_1 f_2}$, visztont $f_1 f_2|\Phi_n$, és $\Phi_n(x)|x^n - 1$. Ezért végül is $k^2|\overline{x^n - 1}$. Ez azonban ellentmond annak, hogy $p \nmid n$ esetén $x^n - 1$ polinomnak nincs többszörös tényezője mod p. Ezzel bizonyítottuk a lemmánkat és vele együtt a tételünket is.

5.3. Feladat. *Bontsuk a $x^{12} - 1$ polinomot irreducibilisek szorzatára $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ fölött.*

Megoldás: Megvizsgáljuk testek fölött és felírjuk a körosztási polinomokat, amelyek az irreducibilis tényezők.

1. $\mathbb{Z}$ fölött
$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) =$$
$$= (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)$$

2. $\mathbb{Z}_2$ fölött
$$\Phi_4(x) = (x+1)^2, \Phi_{12}(x) = (x^2+x+1)^2$$
$$x^{12} - 1 = (x+1)^4(x^2+x+1)^4$$

3. $\mathbb{Z}_3$ fölött
$$\Phi_3(x) = (x-1)^2, \Phi_6(x) = (x+1)^2, \Phi_{12}(x) = (x^2+1)^2$$
$$x^{12} - 1 = (x-1)^3(x+1)^3(x^2+1)^3$$

4. $\mathbb{Z}_5$ fölött
$$\Phi_4(x) = (x-2)(x+2), \Phi_{12}(x) = (x^2+2x-1)(x^2-2x-1)$$

6. fejezet

Köszönetnyilvánítás

Szeretném ezúton is megköszönni konzulensemnek Zábrádi Gergelynek a segítségét és a konzultációkat, hogy a szakdolgozatom létrejöhessen. Ezen kívül, hogy általa betekintést nyerhettem a Newton-poligonok témakörébe.

7. fejezet

Irodalomjegyzék

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

[2] Kiss Emil: Bevezetés az algebrába - A gyakorlatok és feladatok megoldása, Typotex Budapest, 2007

[3] Zábrádi Gergely: Racionális együtthatós polinomok Newton-poligonja
Interneten elérhető jegyzet `http://www.cs.elte.hu/~zger/Jegyzetek/Newton_poligon.pdf`

[4] Surányi László: Algebra testek, gyűrűk, polinomok, Typotex Budapest, 1996