УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

Наташа Н. Милошевић

КРИТЕРИЈУМИ НЕРАСТАВЉИВОСТИ РЕЦИПРОЧНИХ ПОЛИНОМА У $\mathbb{Q}[X]$

мастер рад

Београд, 2023.

Ментор:

проф. др Горан Ђанковић, ванредни професор
Универзитет у Београду, Математички факултет

Чланови комисије:

проф. др Марко Радовановић, ванредни професор
Универзитет у Београду, Математички факултет

др Никола Лелас, асистент са докторатом
Универзитет у Београду, Математички факултет

Датум одбране: септембар 2023.

Хвала Милошу Милошевићу на стрпљењу и подршци коју сам имала у тренуцима када сам хтела да одустанем. Хвала мојој деци Магдалени и Филипу на разумевању.

Такође се захваљујем и ментору професору Горану Ђанковићу на конструктивним критикама, као и осталим члановима комисије на саветима који су помогли да рад буде бољи.

Наслов мастер рада: Критеријуми нерастављивости реципрочних полинома у Q[x]

Резиме: Нерастављивост у комутативним прстенима је један од основних алгебарских концепата. Од великог је значаја продубити знање и стећи интуицију у конкретним прстенима или на конкретним фамилијама полинома. Овај рад има за циљ да изложи неколико критеријума нерастављивости реципрочних полинома над пољем рационалних бројева, а затим да их примени и повеже са факторизацијом фамилија полинома Чебишева прве и друге врсте. Такође одредићемо минималне полиноме тригонометријских функција $\cos(2\pi/n)$ и $\sin(2\pi/n)$.

Кључне речи: полиноми, реципрочни, нерастављивост, критеријум, факторизација

Садржај

Глава 1

Увод

Представљам Вам критеријуме за одређивање нерастављивости реципрочних полинома над пољем рационалних бројева. Ово поглавље је уводног карактера. У њему ћемо дефинисати основне појмове које користимо у раду, навести дефиниције, теореме и тврђења који ове појмове повезују и тако дати основу за проучавање теме. За почетак ћемо увести појам полинома, прстен полинома, објаснићемо шта су реципрочни полиноми на којима је рад и базиран, факторизацију полинома, растављивост и нерастављивост. Такође ћемо добити неке комбинаторне резултате који се тичу нерастављивости реципрочних полинома. Као последицу оваквог приступа, можемо се бавити и другим проблемима као што су факторизација фамилија Чебишевљевих полинома прве и друге врсте, као и за одређивање минималних полинома разних алгебарских вредности тригонометријских функција.

1.1 Прстен полинома

Нека је $(\mathbb{K}, +, \cdot)$ поље које ћемо означавати са $\mathbb{K}$ и нека су 0 и 1 неутрални елементи у односу на операције $+$ и $\cdot$, респективно. Уместо $a \cdot b$ $(a, b \in \mathbb{K})$ писаћемо једноставно ab. Нека је, даље, операција степеновања уведена на уобичајен начин помоћу

$$(\forall x \in \mathbb{K}) \quad x^0 = 1,\ x^k = xx^{k-1} \quad (k \in \mathbb{N}).$$

Дефиниција 1. *Алгебарски полином по x над пољем $\mathbb{K}$ је израз облика:*

$$P(x) = a_0 + a_1x + ... + a_nx^n = \sum_{k=0}^{n} a_kx^k \tag{1.1}$$

ɡде су $a_0, a_1, ..., a_{n-1}, a_n$ *елеменɡи ɡоља* $\mathbb{K}$*,* x *је ɡроменљива,* n *је ненеɡаɡиван цео број и* $a_n \neq 0$*. За елеменɡе* a_k *кажемо да су коефицијенɡи ɡолинома* $P(x)$*. За ɡолином* $P(x)$ *кажемо да је сɡеɡена* n *и ɡо означавамо са* $\deg P(x) = n$*. Коефицијенɡ* $a_n \neq 0$ *називамо водећи или најсɡарији коефицијенɡ ɡолинома* $P(x)$*.*

Дакле, степен полинома $P(x)$ је највиши степен од x који се појављује у изразу за $P(x)$ са ненула коефицијентима.

Дефиниција 2. *За ɡолином*

$$O(x) = 0 + 0x + ... + 0x^{n-1} + 0x^n$$

кажемо да је нула ɡолином и означавамо ɡа ɡросɡо са 0*.*

Степен нула полинома $O(x)(\equiv 0)$ се не дефинише.

Полиноми степена нула се називају константе и то су елементи поља $\mathbb{K}$. Елемент x може се интерпретирати као полином првог степена дефинисан са $P(x) = x$.

Дефиниција 3. *За ɡолином чији је водећи коефицијенɡ једнак јединици кажемо да је моничан.*

Дакле, монични полином има облик

$$P(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n.$$

Скуп свих полинома над $\mathbb{K}$ означавамо са $\mathbb{K}[x]$.

У скуп $\mathbb{K}[x]$ можемо увести релацију једнакост као и операције: *сабирање* и *множење* полинома на следећи начин:

Дефиниција 4. *Полиноми*
$P(x) = a_0 + a_1x + ... + a_nx^n$ *и* $Q(x) = b_0 + b_1x + ... + b_mx^m$
су једнаки ако и само ако је $a_k = b_k$ *за свако* $k \geq 0$*, ɡј. када су њихови коефицијенɡи једнаки.*

Дефиниција 5. *За два ɡолинома*
$P(x) = a_0 + a_1x + ... + a_nx^n$ *и* $Q(x) = b_0 + b_1x + ... + b_mx^m$
збир и ɡроизвод су редом

$$(P + Q)(x) = P(x) + Q(x) = c_0 + c_1x + ... + c_rx^r$$

и

$$(PQ)(x) = P(x)Q(x) = d_0 + d_1x + ... + d_sx^s,$$

где су

$$c_k = a_k + b_k \quad (0 \leq k \leq r = \max(n, m))$$

и

$$d_k = \sum_{i=0}^{k} a_i b_{k-i} \quad (0 \leq k \leq s = n + m).$$

Напоменимо да за ненула полиноме $P(x)$ и $Q(x)$ важи

$$\deg(PQ)(x) = \deg P(x) + \deg Q(x).$$

Такође, ако $P(x), Q(x) \in \mathbb{K}[x]$ и $P(x) + Q(x) \neq 0$, тада је

$$\deg(P + Q)(x) \leq \max\{\deg P(x), \deg Q(x)\}.$$

Као специјални случај производа полинома имамо производ полинома $P(x)$ скаларом $\alpha \in \mathbb{K}$, који се може третирати као полином нултог степена. Дакле,

$$\alpha P(x) = \alpha(a_0 + a_1x + ... + a_nx^n) = (\alpha a_0) + (\alpha a_1)x + ... + (\alpha a_n)x^n.$$

Теорема 1. *Скуп $\mathbb{K}[x]$ снабдевен сабирањем и множењем полинома чини комутативни прстен са јединицом.*

Дефиниција 6. *Елемент a комутативног прстена $\mathbb{K}$ назива се јединица прстена $\mathbb{K}$ ако постоји неко b из $\mathbb{K}$ такво да важи $a \cdot b = b \cdot a = 1$.*

У скупу $\mathbb{Q}$ сваки рационални број различит од нуле је јединица.

У односу на операцију сабирања, супротни елемент од елемента $Q(x) = \sum_{k=0}^{m} b_k x^k (\in \mathbb{K}[x])$ је $\sum_{k=0}^{m}(-b_k)x^k$, који ћемо означавати са $-Q(x)$. Тада можемо дефинисати *одузимање* полинома помоћу

$$(P - Q)(x) = P(x) + (-Q(x)).$$

Напоменимо да за полиноме у скупу $\mathbb{K}[x]$ не постоји операција дељења, тј. операција инверзна операцији множења.

На основу (1.1) може се дефинисати пресликавање $P : \mathbb{K} \to \mathbb{K}$, помоћу

$$t \mapsto P(t) = a_0 + a_1t + ... + a_nt^n,$$

и уочити хомоморфизам $P(x) \mapsto P(t)$. Пресликавање P називамо полиномска функција.

Теорема 2. *Хомоморфизам $P(x) \mapsto P(t)$ је изоморфизам ако и само ако је поље $\mathbb{K}$ бесконачно.*

Дакле, за бесконачна поља једноставно нећемо правити разлику између полинома и полиномске функције. Таква бесконачна поља су, на пример, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$. Међутим, у коначним пољима из једнакости полиномских функција не следује једнакост полинома.

Ако се у изразу $f(\alpha)$ дозволи да се мења f а α да остане фиксирано, добија се пресликавање $\varphi_\alpha : \mathbb{K}[x] \to \mathbb{K}$ које се назива евалуација (израчунавање) у тачки α. Непосредно се види да је евалуација хомоморфизам прстена:

$$(f+g)(\alpha) = f(\alpha) + g(\alpha) \quad \text{и} \quad (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha).$$

Дефиниција 7. *Елемент $\alpha \in \mathbb{K}$ је корен (нула) полинома $f \in \mathbb{K}[x]$ ако је $f(\alpha) = 0$.*

Ако је $\alpha \in \mathbb{K}$ и $f \in \mathbb{K}[x]$, можемо поделити f полиномом $x - \alpha$ степена 1: $f = (x-\alpha) \cdot g + r$. При том је $\deg r < \deg(x-\alpha) = 1$, одакле следи да је $r \in \mathbb{K}$ константа. Ако применимо хомоморфизам евалуације, добијамо $f(\alpha) = (\alpha - \alpha) \cdot g(\alpha) + r(\alpha) = 0 + r$ па следи да је $r = f(\alpha)$. Тиме смо доказали врло корисну чињеницу.

Теорема 3. *Безуова теорема*
Број $\alpha \in \mathbb{K}$ је корен полинома $f \in \mathbb{K}[x] \Leftrightarrow (x-\alpha) | f$.

□

Ако је α нула полинома $f \neq 0$ из $\mathbb{K}[x]$, тај полином има елементарни делитељ облика $(x-\alpha)^r$, степена r. Наиме, то r је највећи природан број за који полином $(x-\alpha)^r$ дели f, то јест за који постоји и полином Q такав да је

$$f = (x-\alpha)^r Q \ \text{ и } \ Q(\alpha) \neq 0.$$

Наравно, ту $Q(\alpha) \neq 0$ управо значи да $x - \alpha$ не дели и Q. Тако одређен број r зовемо и вишеструкошћу уочене нуле $\alpha \in \mathbb{K}$ полинома f, уз напомену да за његове нуле вишеструкости $r = 1$ такође кажемо и да су просте.

Нека је надаље $\mathbb{K} = \mathbb{Q}$.

1.2 Примитивни полиноми

Над пољем $\mathbb{Q}$ имамо много нерастављивих полинома сваког степена и проверавање нерастављивости полинома је тешко у односу на полиноме над $\mathbb{R}$ или $\mathbb{C}$. Полазна тачка за све резултате у $\mathbb{Q}[x]$ је чињеница да је факторизација у $\mathbb{Q}[x]$ „једнака" факторизацији у $\mathbb{Z}[x]$.

Нека су $f(x)$ и $g(x)$ два полинома са коефицијентима у пољу $\mathbb{K}$ и ако постоји не-нулти елемент $c \in \mathbb{K}$ такав да је $f(x) = cg(x)$, онда су полиноми $f(x)$ и $g(x)$ асоцирани. Асоцирани полиноми имају једнаку факторизацију у облику производа нерастављивих полинома.

Ако је $f(x) = a_n x^n + ... + a_1 x + a_0$ полином са рационалним коефицијентима $(a_n, ..., a_1, a_0 \in \mathbb{Q})$, онда можемо помножити $f(x)$ са најмањим заједничким садржаоцем именилаца коефицијената, назовимо тај број s. Множењем добијамо полином $g(x) = sf(x)$ којем су коефицијенти цели бројеви и који је асоциран са полиномом $f(x)$ у $\mathbb{Q}[x]$. Ако имамо факторизацију од $f(x)$, множењем једног од фактора са s добићемо факторизацију полинома $g(x)$. Директно следи да полиноми $f(x)$ и $g(x)$ имају једнаке факторизације у $\mathbb{Q}[x]$ до на инверзни елемент s. Дакле, када посматрамо факторизацију полинома из $\mathbb{Q}[x]$ увек можемо претпоставити да полином има целобројне коефицијенте, то неће утицати на факторизацију.

Дефиниција 8. *Кажемо да је полином $f(x) \in \mathbb{Q}[x]$ примитиван ако има целобројне коефицијенте и највећи заједнички делилац тих коефицијената је једнак* 1.

Сваки полином $f(x)$ са целобројним коефицијентима асоциран је са неким примитивним полиномом: једноставно поделимо $f(x)$ са највећим заједничким делиоцем његових коефицијената, добијени полином је примитиван и асоциран је са $f(x)$. Закључујемо да је сваки полином у $\mathbb{Q}[x]$ асоциран са примитивним полиномом. Пример, полином који је примитиван и асоциран са $3x^3 + \frac{7}{2}x + \frac{4}{3}$ је

$$18x^3 + 21x + 8 = 6\left(3x^3 + \frac{7}{2}x + \frac{4}{3}\right).$$

Погодан начин за одређивање примитивних полинома је конгруенцијом по модулу p.

Нека је p прост број. Ако имамо полином $f(x)$ са целобројним коефицијентима лако можемо добити полином са коефицијентима из $\mathbb{Z}/p\mathbb{Z}$ тако што

заменимо коефицијенте од $f(x)$ са класама конгруенције тих коефицијената модуло p. Нека је γ_p пресликавање које слика коефицијенте из $\mathbb{Z}$ у коефицијенте из $\mathbb{Z}/p\mathbb{Z}$. Ако имамо полином

$$a_n x^n + ... + a_1 x + a_0$$

са целобројним коефицијентима, онда је

$$\gamma_p(a_n x^n + ... + a_1 x + a_0) = [a_n]x^n + ... + [a_1]x + [a_0],$$

где је $[a_i] = \{a_i + kp : k \in \mathbb{Z}\}, i = 0, ..., n$. Полином $f(x)$ у $\mathbb{Z}[x]$ је примитиван ако и само ако не постоји прост број који дели све његове коефицијенте, односно ако и само ако за сваки прост број p важи $\gamma_p(f(x)) \neq 0$. Погледајмо како делује пресликавање γ_3,

$$\gamma_3(18x^3 + 21x + 8) = [2]_3.$$

Приметимо да је пресликавање $\gamma_p : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ хомоморфизам, јер важи

$$\gamma_p(f(x) + g(x)) = \gamma_p(f(x)) + \gamma_p(g(x)),$$

$$\gamma_p(f(x)g(x)) = \gamma_p(f(x)) \cdot \gamma_p(g(x)),$$

за све полиноме $f(x), g(x)$ из $\mathbb{Z}[x]$.

Коришћењем пресликавања γ_p лако доказујемо:

Тврђење 1. *Производ два примитивна полинома је примитиван полином.*

Доказ. Нека су $f(x)$ и $g(x)$ примитивни. Тада је за сваки прост број p, $\gamma_p(f(x)) \neq 0$ и $\gamma_p(g(x)) \neq 0$. Како је $\mathbb{Z}/p\mathbb{Z}$ поље, онда у $\mathbb{Z}/p\mathbb{Z}[x]$ нема правих делитеља нуле. Следи да је $\gamma_p(f(x)g(x)) = \gamma_p(f(x)) \cdot \gamma_p(g(x)) \neq 0$. Како то важи за сваки прост број p, полином $f(x)g(x)$ је примитиван. □

Лема 1. *Нека је $g(x)$ примитиван, $f(x)$ полином у $\mathbb{Z}[x]$ и $f(x) = ag(x)$ за неки рационалан број a, тада је $a \in \mathbb{Z}$. Ако је $f(x)$ такође примитиван, онда је $a = 1$ или $a = -1$.*

Доказ. Нека је $a = r/s$, где су r и s узајамно прости цели бројеви. Тада

$$sf(x) = rg(x).$$

Будући да су r и s узајамно прости цели бројеви, s мора делити све коефицијенте полинома $g(x)$. Међутим, како је $g(x)$ примитиван следи да је $s = 1$ или $s = -1$. Ако је $f(x)$ примитиван полином следи да r мора бити 1 или -1, јер r мора да дели све коефицијенте полинома $f(x)$. Стога, $a = 1$ или $a = -1$. □

Теорема 4. *(Гаусова лема)*
Нека је $f(x)$ полином са целобројним коефицијентима и $f(x) = g(x)h(x)$, где су $g(x)$ и $h(x)$ из $\mathbb{Q}[x]$. Тада постоје полиноми $g_1(x)$ и $h_1(x)$ из $\mathbb{Z}[x]$, који су асоцирани са полиномима $g(x)$ и $h(x)$, такви да је $f(x) = g_1(x)h_1(x)$.

Гаусова лема нам говори да ако желимо да пронађемо факторизацију полинома са целобројним коефицијентима, треба да тражимо само факторе који имају целобројне коефицијенте.

Доказ. Нека је $f(x) \in \mathbb{Z}[x]$, и претпоставимо да је $f(x) = g(x)h(x)$, где су $g(x), h(x) \in \mathbb{Q}[x]$. Нека су $g_1(x)$ и $h_1(x)$ примитивни полиноми из $\mathbb{Z}[x]$ асоцирани са $g(x)$, $h(x)$. Имамо

$$g(x) = cg_1(x),\ h(x) = dh_1(x),$$

где су $c, d \in \mathbb{Q}$. Тада је

$$f(x) = cdg_1(x)h_1(x).$$

Из Тврђења 1, следи да је $g_1(x)h_1(x)$ примитиван полином, а према Леми 1 је $cd \in \mathbb{Z}$. Следи

$$f(x) = (cdg_1(x))h_1(x).$$

Добили смо факторизацију у $\mathbb{Z}[x]$ у којој су полиноми $cdg_1(x)$ и $h_1(x)$ асоцирани, редом, са полиномима $g(x)$ и $h(x)$. Тиме смо доказали тврђење. □

Пример 1. *Размотримо полином*

$$x^4 - 2x^2 + x + 3.$$

Тражимо факторизацију тог полинома такву да су фактори полинома другог степена:

$$x^4 - 2x^2 + x + 3 = (x^2 + ax + b)(x^2 + cx + d).$$

Ако постоји таква факторизација у $\mathbb{Q}[x]$, онда према Гаусовој леми постоји факторизација у којој су коефицијенти a, b, c, d цели бројеви. Множењем десне стране добијамо:

$$x^4 - 2x^2 + x + 3 = x^4 + (c + a)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.$$

Изједначавањем коефицијената уз x^3 добијамо $c = -a$. Ако то искористимо и изједначимо коефицијенте уз x^2, x и 1 добијамо:

$$-2 = b + d - a^2,$$

$$1 = ad - ab = a(d - b),$$

$$3 = bd.$$

Како су a, b и d цели бројеви, из друге једначине добијамо $d - b = 1$ или $d - b = -1$, односно d и b се разликују за 1; док из треће једначине добијамо $b = \pm 1$, $d = \pm 3$ или $b = \pm 3$, $d = \pm 1$. Тиме смо добили контрадикцију јер се d и b не разликују за 1, па не постоји тражена факторизација датог полинома.

Да нисмо могли претпоставити да су a, b и d цели бројеви, имали бисмо бесконачно могућности за a, b и d, те би показивање да једначине немају решења за све могуће a, b и d било знатно теже.

1.3 Реципрочни полиноми

Дефиниција 9. *Дат је полином $f(t) \in \mathbb{Q}[t]$. Обрнути полином полинома $f(t)$ је дефинисан као следећи полином из $\mathbb{Q}[t]$:*

$$f_{obr}(t) = t^{\deg f} f\left(\frac{1}{t}\right). \tag{1.2}$$

Неформално речено, обрнути полином $f_{obr}(t)$ има исте коефицијенте као и полином $f(t)$ али у обрнутом редоследу.

Пример 2. *Као једноставан пример имамо полином $f(t) = t^2 - t + 2$. Његов обрнути полином је*

$$f_{obr}(t) = t^2\left(\frac{1}{t^2} - \frac{1}{t} + 2\right) = 1 - t + 2t^2.$$

Пример 3. *За било који моном $f(t) = t^n$, његов обрнути полином ће бити*

$$f_{obr}(t) = t^n \cdot \frac{1}{t^n} = 1.$$

Можемо приметити да када полином f има корен 0, степени полинома f_{obr} и f нису једнаки.

Дефиниција 10. *Полином $f(t) \in \mathbb{Q}[t]$ је рециprочан полином ако је*

$$f_{obr}(t) = f(t). \tag{1.3}$$

Реципрочне полиноме називамо још и самореципрочни, палиндроми итд. Пример реципрочног полинома је $f(t) = t^6 - 2t^5 + 5t^4 - t^3 + 5t^2 - 2t + 1$.

Пример 4. *Полином $f(t) = at^2 + bt + a,\ a, b \in \mathbb{Q},\ a \neq 0$ је пример једног реципрочног полинома другог степена. Пример реципрочног полинома трећег степена је полином $f(t) = at^3 + bt^2 + bt + a,\ a, b \in \mathbb{Q},\ a \neq 0$.*

Пример 5. *Докажимо да је полином $f(t) = t^3 + 4t^2 + 4t + 1$ реципрочан полином.*
Да бисмо доказали, потребно је показати да важи једнакост $f(t) = t^n f\left(\frac{1}{t}\right)$, где је n степен полинома $f(t)$.
Прво израчунамо полином $f\left(\frac{1}{t}\right)$, тако што t заменимо са $\frac{1}{t}$ у изразу $f(t)$:
$f\left(\frac{1}{t}\right) = \left(\frac{1}{t}\right)^3 + 4 \cdot \left(\frac{1}{t}\right)^2 + 4 \cdot \frac{1}{t} + 1 = \frac{1}{t^3} + 4 \cdot \frac{1}{t^2} + 4 \cdot \frac{1}{t} + 1.$
Затим израчунамо $t^n f\left(\frac{1}{t}\right)$, $n = 3$.
$f_{obr}(t) = t^3 f\left(\frac{1}{t}\right) = t^3\left(\frac{1}{t^3} + 4 \cdot \frac{1}{t^2} + 4 \cdot \frac{1}{t} + 1\right) = 1 + 4t + 4t^2 + t^3.$
Приметимо да су изрази $f(t)$ и $t^n f\left(\frac{1}{t}\right)$ једнаки, што доказује да је $f(t)$ реципрочан полином.

Дефиниција 11. *Реципрочно пресликавање $\mathbf{R}$ додељује сваком реципрочном полиному $f(t) \in \mathbb{Q}[t]$ парног степена јединствени полином $p(x) = \mathbf{R}(f) \in \mathbb{Q}[x]$ који задовољава једначину*

$$f(t) = t^{\deg p} p\left(t + \frac{1}{t}\right). \tag{1.4}$$

За сваки реципрочни полином $f(t) \in \mathbb{Q}[t]$ степена $2n$, методом замене променљиве $x = t + \frac{1}{t}$ добијамо полином $f(x)$ из $\mathbb{Q}[x]$ степена n. Корени полинома $f(x)$ су облика $\alpha + \frac{1}{\alpha}$, где је α корен полинома $f(t)$. Под претпоставком да је могуће израчунати n корена полинома $f(x)$, корене полинома $f(t)$ можемо добити решавањем n квадратних једначина.

Пример 6. *Нека је дат полином $f(t) = t^6 - 3t^5 - 3t^4 + 11t^3 - 3t^2 - 3t + 1$. Одредимо јединствени полином $p(x)$ датог полинома $f(t)$.*
Како је степен полинома паран број, можемо применити реципрочно пресликавање.
Примењујући реципрочно пресликавање, треба да нађемо полином $p(x)$, где је $x = t + \frac{1}{t}$, такав да је $f(t) = t^{\deg p} p\left(t + \frac{1}{t}\right)$. У овом случају, степен полинома $p(x)$ ће бити половина степена полазног полинома $f(t)$, што је $6/2 = 3$.
$f(t) = t^6 - 3t^5 - 3t^4 + 11t^3 - 3t^2 - 3t + 1 = t^3\left(t^3 - 3t^2 - 3t + 11 - \frac{3}{t} - \frac{3}{t^2} + \frac{1}{t^3}\right)$
$f(t) = t^3\left(t^3 + \frac{1}{t^3} - 3\left(t^2 + \frac{1}{t^2}\right) - 3\left(t + \frac{1}{t}\right) + 11\right).$
$p\left(t + \frac{1}{t}\right) = t^3 + \frac{1}{t^3} - 3\left(t^2 + \frac{1}{t^2}\right) - 3\left(t + \frac{1}{t}\right) + 11$

Уводимо смену $x = t + \frac{1}{t}$.
$t^2 + \frac{1}{t^2} = \left(t + \frac{1}{t}\right)^2 - 2 = x^2 - 2$
$t^3 + \frac{1}{t^3} = \left(t + \frac{1}{t}\right)^3 - 3\left(t + \frac{1}{t}\right) = x^3 - 3x.$
Следи
$p(x) = x^3 - 3x - 3(x^2 - 2) - 3x + 11 = x^3 - 3x^2 - 6x + 17 = \mathbf{R}(f).$

Обрнуто, примећујемо да је за свако $p \in \mathbb{Q}[x]$ полином $f = \mathbf{R}^{-1}(p)$, где је $\mathbf{R}^{-1}$ инверзно пресликавање, управо дефинисан као реципрочни полином парног степена.

Пример 7. *Нека је дат полином* $p(x) = x^2 - 4x + 3 \in \mathbb{Q}[x]$. *Увођењем смене* $x = t + \frac{1}{t}$ *ћемо показати да је полином* $f(t)$ *реципрочан полином парног степена.*
$f(t) = t^2((t + \frac{1}{t})^2 - 4(t + \frac{1}{t}) + 3)$
$f(t) = t^2(t^2 - 4t + 5 - \frac{4}{t} + \frac{1}{t^2})$
$f(t) = t^4 - 4t^3 + 5t^2 - 4t + 1.$
Полином f(t) јесте реципрочан полином парног степена.

Пример 8. *Нека је дат полином* $p(x) = ax^3 - bx^2 + cx + d \in \mathbb{Q}[x], a \neq 0$. *Увођењем смене* $x = t + \frac{1}{t}$ *ћемо показати да је полином* $f(t)$ *реципрочан полином парног степена.*
$f(t) = t^3\left(a \cdot \left(t + \frac{1}{t}\right)^3 - b \cdot \left(t + \frac{1}{t}\right)^2 + c \cdot \left(t + \frac{1}{t}\right) + d\right)$
$f(t) = t^3\left(at^3 + 3at + \frac{3a}{t} + \frac{a}{t^3} - bt^2 - 2b - \frac{b}{t^2} + ct + \frac{c}{t} + d\right)$
$f(t) = at^6 - bt^5 + (3a + c)t^4 + (d - 2b)t^3 + (3a + c)t^2 - bt + a.$
Полином f(t) јесте реципрочан полином парног степена.

Да бисмо могли да размотримо следећи пример потребно је да уведемо појам циклотомичних полинома. Можемо рећи да су циклотомични полиноми Φ_n за $n > 1$ најпознатији примери реципрочних полинома са рационалним коефицијентима.

Дефиниција 12. *За дати број* $n \in \mathbb{N}$, *дефинишемо n-ти корен из јединице, као комплексан број* θ *који задовољава једнакост* $\theta^n = 1$.

Дефиниција 13. *Нека је* θ *n-ти корен из јединице, за произвољно* $n \in \mathbb{N}$. *Тада најмањи природан број* k *такав да важи* $\theta^k = 1$ *називамо поретком броја* θ *и означавамо га са* $ord(\theta)$.

Дефиниција 14. *Нека је θ n-ти корен из јединице, за неко $n \in \mathbb{N}$. Уколико важи $ord(\theta) = n$, онда θ називамо примитивним n-тим кореном из јединице.*

Дефиниција 15. *Нека је n произвољан природан број. Тада n-тим циклотомичним полиномом називамо моничан полином чији су сви корени примитивни n-ти корени из јединице (и притом нема двоструких нула):*

$$\Phi_n(x) = \prod_{\substack{ord(\theta)=n \\ \theta^n=1}} (x - \theta)$$

Теорема 5. *Нека је $n \in \mathbb{N}$. Тада важи:*

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

Доказ. Све нуле полинома $x^n - 1$ су n-ти корени из јединице. Нека је θ један од тих корена и нека је $ord(\theta) = d$. Тада је θ примитивни d-ти корен из јединице, па је самим тим и нула полинома $\Phi_d(x)$. Такође, пошто $d|n$, то је θ нула и полинома са десне стране једнакости у претходној теореми. Пошто су оба полинома у теореми монична и имају све једнаке нуле, следи да су и они сами једнаки, па је једнакост задовољена. □

Да бисмо одредили у ком пољу се налазе коефицијенти циклотомичног полинома, потребна нам је наредна лема.

Лема 2. *Претпоставимо да су $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$ и $g(x) = x^n + b_{n-1}x^{n-1} + ... + b_0$ полиноми са рационалним коефицијентима. Ако су сви коефицијенти полинома $f(x) \cdot g(x)$ целобројни, онда су и коефицијенти полинома $f(x)$ и $g(x)$ такође целобројни.*

Доказ. Дати су полиноми $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$ и $g(x) = x^n + b_{n-1}x^{n-1} + ... + b_0$. Нека су M и N најмањи заједнички садржаоци именилаца коефицијената $a_0, ..., a_{m-1}$ и $b_0, ..., b_{n-1}$, редом. Коефицијенти полинома $Mf(x)$ и $Nf(x)$ су целобројни. Нека је $A_i = Ma_i$ за $i \in \{0, ..., m-1\}, B_j = Nb_j$ за $j \in \{0, ..., n-1\}$ и $A_m = M, B_n = N$. Тада

$$MNf(x)g(x) = A_mB_nx^{m+n} + ... + A_0B_0.$$

Пошто $f(x)g(x) \in \mathbb{Z}[x]$, сви коефицијенти полинома $MNf(x)g(x)$ су дељиви са MN. Претпоставимо да је $MN > 1$ и нека је p прост делилац од MN. Тада

постоји цео број $i \in \{0, ..., m\}$ такав да $p \nmid A_i$. Заиста, ако $p \nmid M$, тада $p \nmid A_m$ и ако $p \mid M$, тада $p \mid A_i$ за $i \in \{0, ..., m\}$, одакле следи да $A_i/p = (M/p)a_i \in \mathbb{Z}$ што представља контрадикцију минималности M. На сличан начин, постоји цео број $j \in \{0, ..., n\}$ такав да $p \nmid B_j$. Нека су I и J највећи цели бројеви међу бројевима i и j, редом. Тада коефицијент уз полином x^{I+J} у $MNf(x)g(x)$ има облик

$$[x^{I+J}] = ... + A_{I+1}B_{J-1} + A_IB_J + A_{I-1}B_{J+1} + ... = A_IB_J + p \cdot R$$

где је R цео број, и није дељив са p што је у супротности са чињеницом да су коефицијенти полинома $MNf(x)g(x)$ дељиви са MN. □

Теорема 6. *Нека је n произвољан природан број. Тада полином $\Phi_n(x)$ има целобројне коефицијенте, $\Phi_n(x) \in \mathbb{Z}[x]$.*

Доказ. Доказујемо индукцијом по n. Тврђење је тачно за $n = 1$ пошто је $\Phi_1(x) = x - 1$. Претпоставимо да је тврђење тачно за свако $k < n$. Тада из Теореме 5 следи

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

На основу индукцијске хипотезе знамо да су сви полиноми $\Phi_d(x)$ са целобројним коефицијентима па следи да су коефицијенти полинома $\Phi_n(x)$ рационални бројеви. Позивајући се на Лему 2 следи да су коефицијенти полинома $\Phi_n(x)$ цели бројеви. □

За $n = 1$, $\Phi_1(x) = x-1$. За $n = 2$ имамо $x^2-1 = (x-1)(x+1)$ што значи да је $\Phi_2(x) = x+1$. За $n = 3$, $x^3-1 = (x-1)(x^2+x+1)$, па је $\Phi_3(x) = x^2+x+1$. За $n = 4$, $x^4-1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1)$, па је $\Phi_4(x) = x^2+1$.

Издвојмо првих 12 циклотомичних полинома:

$\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = x^2 + x + 1$
$\Phi_4(x) = x^2 + 1$
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
$\Phi_6(x) = x^2 - x + 1$
$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_8(x) = x^4 + 1$
$\Phi_9(x) = x^6 + x^3 + 1$

$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$
$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_{12}(x) = x^4 - x^2 + 1.$
Приметимо да број примитивних n-тих корена из јединице је једнак броју природних бројева мањих од n који су узајамно прости са n. То је управо дефиниција Ојлерове функције $\varphi(n)$. Односно важи,

$$\deg(\Phi_n(t)) = \varphi(n). \tag{1.5}$$

Ојлерову функцију $\varphi(n)$ можемо израчунати преко производа

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

а производ узима само вредности различитих простих бројева p који деле n.

Пример 9. *Нека је* $n = 6$. *Степен циклотомичног полинома* $\Phi_6(t)$ *једнак је вредности Ојлерове функције* $\varphi(6)$. *Односно* $\deg(\Phi_6(t)) = \varphi(6)$. *Узајамно прости бројеви са* 6 *су* 1 *и* 5. *Стога је* $\varphi(6) = 2$. *Односно, можемо израчунати и преко производа* $\varphi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 2$.

Пример 10. *Узмимо за пример циклотомични полином* $\Phi_7(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$. *Овај полином је парног степена јер је* $\deg(\Phi_7(t)) = \varphi(7) = 7\left(1 - \frac{1}{7}\right) = 6$.

Тврђење 2. *За* $n > 1$, $\Phi_n(x)$ *је реципрочан полином, тј.* $\Phi_n(\frac{1}{x}) \cdot x^{\varphi(n)} = \Phi_n(x)$.

Доказ. Доказујемо индукцијом по n. Тврђење је тачно за $n = 2$, јер је $\Phi_2(x) = x + 1$.

$$x^{\varphi(2)}\Phi_2\left(\frac{1}{x}\right) = x\left(\frac{1}{x} + 1\right) = x + 1 = \Phi_2(x).$$

Претпоставимо да је тврђење тачно за $n < m$. Ако заменимо x са $\frac{1}{x}$ у

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

добићемо

$$\left(\frac{1}{x}\right)^m - 1 = \prod_{d|m} \Phi_d\left(\frac{1}{x}\right)$$

$$= \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d\left(\frac{1}{x}\right)\right) \cdot \Phi_m\left(\frac{1}{x}\right) \cdot \left(\frac{1}{x} - 1\right).$$

Помножимо леву и десну страну једнакости са $x^m = \sum_{d|m}^{x} \varphi(d) = \prod_{d|m} x^{\varphi(d)}$. Добићемо

$$1 - x^m = \left(\prod_{\substack{1<d<m \\ d|m}} x^{\varphi(d)} \Phi_d\left(\frac{1}{x}\right) \right) \cdot x^{\varphi(m)} \Phi_m\left(\frac{1}{x}\right) \cdot x\left(\frac{1}{x} - 1\right)$$

$$-(x^m - 1) = \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d(x) \right) \cdot x^{\varphi(m)} \Phi_m\left(\frac{1}{x}\right) \cdot (1 - x)$$

$$-\prod_{d|m} \Phi_d(x) = \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d(x) \right) \cdot x^{\varphi(m)} \Phi_m\left(\frac{1}{x}\right) \cdot (-\Phi_1(x)).$$

Скраћивањем фактора добијамо

$$\Phi_m(x) = \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)},$$

што је и требало доказати индукцијом. □

Пример 11. *Размотримо реципрочни полином* $\Phi_{11}(t) = \sum_{i=0}^{10} t^i$, *једанаести циклотомични полином. Записујући*

$$\Phi_{11}(t) = t^5 \left(1 + \sum_{k=1}^{5} \left(t^k + \frac{1}{t^k}\right)\right)$$

можемо изразити $t^k + 1/t^k$ *као линеарну комбинацију степена* $x = t + 1/t$ *на следећи начин:*

$$\begin{aligned}
t^2 + \tfrac{1}{t^2} &= \left(t + \tfrac{1}{t}\right)^2 - 2 \\
t^3 + \tfrac{1}{t^3} &= \left(t + \tfrac{1}{t}\right)^3 - 3\left(t + \tfrac{1}{t}\right) \\
t^4 + \tfrac{1}{t^4} &= \left(t + \tfrac{1}{t}\right)^4 - 4\left(t + \tfrac{1}{t}\right)^2 + 2 \\
t^5 + \tfrac{1}{t^5} &= \left(t + \tfrac{1}{t}\right)^5 - 5\left(t + \tfrac{1}{t}\right)^3 + 5\left(t + \tfrac{1}{t}\right).
\end{aligned}$$

Са овим једнакостима, добијамо да је циклотомични полином

$$\Phi_{11}(t) = t^5 p\left(t + \frac{1}{t}\right) \quad \text{са} \quad p(x) = \mathbf{R}(\Phi_{11}) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

Узимајући ову идеју као полазну тачку, главни циљ овог рада је да пружи јединствен оквир у коме се могу разматрати различити проблеми везани за реципрочне полиноме.

Наше реципрочно пресликавање има много занимљивих својстава које нам омогућавају да уобичајену замену променљивих искористимо као системско решење. Основни метод ћемо називати методом реципрочне замене, а њени детаљи су објашњени у глави 3. Чињеница је да овај метод даје поред информација о коренима реципрочног полинома и информације о његовој факторизацији. Дакле, факторизација фамилија реципрочних полинома парног степена се пресликава у факторизацију фамилија њихових слика и обрнуто.

Дефиниција 16. *Полином $p(x) \in \mathbb{K}[x]$ је нерастављив ако $p(x)$ није јединица, и ако $p(x) = f(x)g(x)$, тада $f(x)$ или $g(x)$ мора бити јединица, односно константан полином.*

Тврђење 3. *Ако је p нерастављив полином, и ако је f полином који није дељив са p, тада је највећи заједнички делилац полинома p и f број* 1.

Доказ. Претпоставимо да је $d = (f, p)$. Пошто је p нерастављив полином и d дели p, или је d јединица тј. константа различита од нуле, или је d асоцирано са p. У другом случају, p дели f. У првом случају, p и f су узајамно прости бројеви, односно највећи заједички делилац им је 1, асоциран са d. □

Примери нерастављивих полинома:
$x + a$ је нерастављив у $\mathbb{K}[x]$ за било које поље $\mathbb{K}$ и било које $a \in \mathbb{K}$;
$x^2 + 1$ је нерастављив у $\mathbb{R}[x]$, али није у $\mathbb{C}[x]$;
$x^3 - 2$ је нерастављив у $\mathbb{Q}[x]$, али није у $\mathbb{R}[x]$;
$x^2 + 1$ је нерастављив у $\mathbb{Z}/3\mathbb{Z}[x]$, али није у $\mathbb{Z}/5\mathbb{Z}[x]$.

Када тражимо нерастављиве полиноме над неким пољем, можемо ограничити нашу пажњу на моничне полиноме. Сваки полином је асоциран моничним полиномом. Одговор на питање, који су полиноми нерастављиви, искључиво зависи од поља $\mathbb{K}$ у ком се налазе коефицијенти. На пример, размотримо полином $x^3 - 2$. Овај полином има коефицијенте у $\mathbb{Q}$, и $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, па можемо испитати нерастављивост у $\mathbb{Q}$, у $\mathbb{R}$ и у $\mathbb{C}$.
У $\mathbb{Q}[x]$, $x^3 - 2$ је нерастављив.
У $\mathbb{R}[x]$, $x^3 - 2 = (x - 2^{\frac{1}{3}})(x^2 + 2^{\frac{1}{3}}x + 4^{\frac{1}{3}})$.
У $\mathbb{C}[x]$, $x^3 - 2 = (x - 2^{\frac{1}{3}})(x - \omega 2^{\frac{1}{3}})(x - \omega^2 2^{\frac{1}{3}})$, где је $\omega = e^{\frac{2\pi}{3}} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ комплексан корен полинома $x^3 - 1$.

Помоћу методе реципрочне замене можемо да одредимо неке критеријуме за одређивање нерастављивости реципрочних полинома у $\mathbb{Q}[t]$ (видети Теорему 8).

Критеријум из овог рада нам дозвољава да покажемо да су полиноми облика

$$g_{2p}(t) = \frac{(t+1)^{2p} - t^{2p} - 1}{t}$$

нерастављиви над $\mathbb{Q}$ када је p непаран прост број (видети Пример 16). Позивамо се на Ајзенштајнов критеријум да покажемо нерастављивости слике g_{2p}.

Са комбинаторне тачке гледишта, занимљиво је проценити „пропорцију" реципрочних полинома са датим обрасцем факторизације. Познато је да су „скоро сви" полиноми са целим коефицијентима нерастављиви над $\mathbb{Q}$. Помоћу методе реципрочне замене, комбинаторне верзије за реципрочне полиноме се изводе из њихових супротних бројева у $\mathbb{Q}[x]$ (видети одељак 6).

Глава 2

Својства факторизације реципрочних полинома

Започећемо овај одељак низом последица које произилазе из дефиниције (1.2).

- Ако је α комплексни ненула корен полинома f, онда је $\frac{1}{\alpha}$ корен реципрочног полинома f_{obr}.
- Нека је k вишеструкост броја нула као корен полинома f. Тада је степен реципрочног полинома f_{obr} једнак $\deg f - k$. Ако је $f(0) \neq 0$, тада је $(f_{obr})_{obr} = f$.
- $(fg)_{obr} = f_{obr} g_{obr}$.
- Ако је $f(0) \neq 0$, онда је f нерастављив у $\mathbb{Q}[t]$ ако и само ако је f_{obr} нерастављив у $\mathbb{Q}[t]$.

Претпоставимо сада да је $f(t) \in \mathbb{Q}[t]$ реципрочни полином непарног степена. Из својстава реципрочних полинома, уочавамо да је -1 корен полинома $f(t)$ и да се полином $f(t)$ факторише на $(t+1)g$, где је $g \in \mathbb{Q}[t]$ реципрочни полином парног степена. Стога је смислено да се фокусирамо на скуп реципрочних полинома парног степена, са рационалним коефицијентима. Узмимо пример полинома степена $n = 5$, $f(t) = a_5t^5 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$. Обрнути полином полинома $f(t)$ је облика $f_{obr}(t) = a_0t^5 + a_1t^4 + a_2t^3 + a_3t^2 + a_4t + a_5$. Да би $f_{obr}(t) = f(t)$ мора да важи $a_5 = a_0 = a, a_4 = a_1 = b, a_3 = a_2 = c$, где су $a, b, c \in \mathbb{Q}$, $a \neq 0$. Тада $f(t) = at^5 + bt^4 + ct^3 + ct^2 + bt + a$ факторишемо

груписањем и добијамо $f(t) = (t+1)(at^4-(a-b)t^3+(a-b+c)t^2-(a-b)t+a)$, следи на основу Безуовог става да је корен датог полинома -1, а полином $g(t) = at^4 - (a-b)t^3 + (a-b+c)t^2 - (a-b)t + a$ јесте реципрочан полином парног степена.

Даље ћемо посматрати скуп реципрочних полинома са рационалним коефицијентима и парним степенима. У тексту ћемо користити следећу ознаку:

$$\mathcal{R} := \{f \in \mathbb{Q}[t] : f(t) \text{ реципрочан и парног степена}\}.$$

Сви циклотомични полиноми $\Phi_n(t)$, осим $\Phi_1(t) = t-1$ и $\Phi_2(t) = t+1$, припадају скупу $\mathcal{R}$, за $n \geq 3$.

У уводном делу смо објаснили да је степен циклотомичног полинома једнак Ојлеровој функцији:

$$\deg(\Phi_n(t)) = \varphi(n).$$

Функција $\varphi(n)$ је парна за свако $n > 2$. Ако посматрамо групу примитивних корена из јединице модуло n приметићемо да је ред те групе једнак $\varphi(n)$, што је увек паран број за $n > 2$.

Следи да је општи циклотомични полином $\Phi_n(t)$ парног степена. У Тврђењу 2 смо доказали да је сваки циклотомични полином $\Phi_n(t)$, $n > 1$ реципрочан полином, а из степена циклотомичног полинома уочавамо да је сваки циклотомични полином $\Phi_n(t)$, $n > 1$, парног степена, па закључујемо да $\Phi_n(t)$ припада скупу $\mathcal{R}$.

Сада ћемо навести нека корисна својства која се односе на факторизацију реципрочних полинома и која су нам потребна за доказивање наредног тврђења.

Лема 3. *Важе следећа тврђења:*

- *Производ реципрочних полинома је реципрочан.*
- *Ако је $f(t) = g(t)h(t)$ и $f(t)$, $g(t)$ су реципрочни, онда је и $h(t)$ реципрочан.*

Доказ. Нека су $f(t)$ и $g(t)$ два реципрочна полинома степена n и m, редом. Производ, $f(t)g(t) = h(t)$ је полином степена $n+m$. Доказаћемо да је полином $h(t)$ реципрочан, односно да је облика $h(t) = t^{n+m}h\left(\frac{1}{t}\right)$. Знамо да је $f(t) = t^n f\left(\frac{1}{t}\right)$ и $g(t) = t^m g\left(\frac{1}{t}\right)$. Следи

$$h(t) = f(t)g(t) = t^n f\left(\frac{1}{t}\right) t^m g\left(\frac{1}{t}\right) = t^{n+m} f\left(\frac{1}{t}\right) g\left(\frac{1}{t}\right) = t^{n+m} h\left(\frac{1}{t}\right).$$

Следи да је производ два рециprочна полинома $f(t)$ и $g(t)$ рециprочни полином $h(t)$.

Ако су $f(t)$ и $g(t)$ два рециprочна полинома степена n и m, редом и $f(t) = g(t)h(t)$, односно $h(t) = \frac{f(t)}{g(t)}$, $n > m$ и $g(t)$ је фактор полинома $f(t)$. Тада

$$h(t) = \frac{t^n f\left(\frac{1}{t}\right)}{t^m g\left(\frac{1}{t}\right)} = t^{n-m}\frac{f\left(\frac{1}{t}\right)}{g\left(\frac{1}{t}\right)} = t^{n-m}h\left(\frac{1}{t}\right).$$

□

Следеће тврђење даје еквивалентну карактеризацију рециprочног полинома.

Тврђење 4. *Полином $f \in \mathbb{Q}[t]$ је рециprочан ако и само ако задовољава следећа два услова:*

1. *Ако је 1 корен полинома $f(t)$, тада је вишеструкост парна.*
2. *Ако је $\alpha \neq \pm 1$ корен полинома $f(t)$ вишеструкости r, тада је и $\frac{1}{\alpha}$ корен вишеструкости r.*

Доказ. ($\Rightarrow$) Прво ћемо доказати тврђење 2. Претпоставимо да је $f(t)$ рециprочан полином степена d. $f(t) = a(t-\alpha_1)^{r_1} \cdot \ldots \cdot (t-\alpha_n)^{r_n}$, где су $\alpha_i \neq \pm 1$ различити корени полинома $f(t)$ са вишеструкошћу r_i.

$$f(t) = f_{obr}(t) = t^{\deg f} f\left(\frac{1}{t}\right) = t^{\deg f} a\left(\frac{1}{t}-\alpha_1\right)^{r_1} \cdot \ldots \cdot \left(\frac{1}{t}-\alpha_n\right)^{r_n} =$$

$$= (-1)^d a\alpha_1^{r_1} \cdot \ldots \cdot$$
$$\alpha_n^{r_n}\left(t-\frac{1}{\alpha_1}\right)^{r_1} \cdot \ldots \cdot \left(t-\frac{1}{\alpha_n}\right)^{r_n}.$$

Следи да за било који корен α_i вишеструкости r_i полинома $f(t)$, $\frac{1}{\alpha_i}$ је такође корен полинома $f(t)$ вишеструкости r_i.

Пошто смо доказали да ако је $\alpha_i \neq \pm 1$ корен полинома $f(t)$, тада је $\frac{1}{\alpha_i}$ такође корен полинома и имају исту вишеструкост, r_i, сада ћемо доказати да ако је 1 корен полинома $f(t)$, тада је вишеструкост парна. Ако означимо вишеструкост корена (-1) са n_{-1}(може бити 0) и вишеструкост корена 1 са m, полином $f(t)$ можемо записати у облику:

$$f(t) = (t-1)^m(t+1)^{n_{-1}}(t^2-(\alpha_1+\frac{1}{\alpha_1})t+1)^{n_1}\cdots(t^2-(\alpha_m+\frac{1}{\alpha_m})t+1)^{n_m}.$$

Ако сада претпоставимо да је вишеструкост од 1 непарна, $m = 2k+1, k \geq 0$, и знамо да је $(t-1)^2 = t^2 - 2t + 1$ рециprочан полином, можемо уочити да је

$$f(t) = (t-1)^{2k+1}(t+1)^{n-1}\left(t^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)t + 1\right)^{n_1} \cdot \cdot$$

$$\left(t^2 - \left(\alpha_m + \frac{1}{\alpha_m}\right)t + 1\right)^{n_m}$$

$$= (t-1)(t^2-2t+1)^k(t+1)^{n-1}\left(t^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)t + 1\right)^{n_1} \cdot \cdot$$

$$\left(t^2 - \left(\alpha_m + \frac{1}{\alpha_m}\right)t + 1\right)^{n_m},$$

где су $(t^2-2t+1)^k, (t+1)^{n-1}$ и $(t^2 - (\alpha_i + \frac{1}{\alpha_i})t + 1)^{n_i}$ рециprочни полиноми за $i = 1, ..., m$. То значи да је и њихов производ исто рециprочни полином, па њихов производ има 1 као константан члан. Али када се помножи са последњим фактором $(x-1)$, полинома $f(t)$, видимо да се константни члан мења у -1. Стога, $f(t)$ не може бити рециprочан, што је контрадикторно са нашом претпоставком да је корен 1 непарне вишеструкости.

($\Leftarrow$) Хоћемо да докажемо чињеницу да ако $\alpha_i \neq \pm 1$ је корен полинома $f(t) \in \mathbb{Q}[t]$ вишеструкости r_i, тада $\frac{1}{\alpha_i}$ је исто корен полинома $f(t)$ вишеструкости r_i, и ако је вишеструкост корена 1 парна, тада је $f(t)$ рециprочан полином. Нека су r и s вишеструкости корена 1 и -1, редом и нека су $\alpha_1, \frac{1}{\alpha_1}, \alpha_2, \frac{1}{\alpha_2}, ..., \alpha_m, \frac{1}{\alpha_m}$ остали корени са вишеструкошћу $n_1, n_1, n_2, n_2, ..., n_m, n_m$, редом. Тада имамо

$$f(t) = (t-1)^r(t+1)^s \prod_{i=1}^{m}\left(t^2 - \left(\alpha_i + \frac{1}{\alpha_i}\right)t + 1\right)^{n_i}.$$

Под претпоставком да је r парно, $r = 2k, k \geq 0$, полином $(t-1)^r = (t-1)^{2k} = (t^2-2t+1)^k$ је рециprочан полином на основу Леме 3. Такође су $(t+1)^s$ и производ $\prod_{i=1}^{m}\left(t^2 - \left(\alpha_i + \frac{1}{\alpha_i}\right)t + 1\right)^{n_i}$ рециprочни полиноми, што значи да полином $f(t)$ добијамо као производ рециprочних полинома, па на основу Леме 3 и он мора бити такође рециprочан полином.

Дакле, доказали смо нашу прву тврдњу и настављамо доказујући следећу; да ако је -1 корен, вишеструкост је увек непарна ако је полином непарног степена, односно увек парна ако је полином парног степена.

Из основне теореме алгебре знамо да сваки полином степена n има n комплексних корена, рачунајући са вишеструкошћу. Дакле, ако је n непарно,

сваки полином степена n има непаран број корена. Али из горњег резултата знамо да сваки други корен од -1 долази у инверзним паровима $\{\alpha, \frac{1}{\alpha}\}$ са парном вишеструкошћу (пар, пошто је вишеструкост корена α и $\frac{1}{\alpha}$ иста).

Из прве тврдње знамо да ако је 1 корен, он је корен парне вишеструкости $2k$, где k може бити 0. Нека је $2n_1$ вишеструкост пара корена $\{\alpha_1, \frac{1}{\alpha_1}\}$, $2n_2$ вишеструкост пара корена $\{\alpha_2, \frac{1}{\alpha_2}\}$, и тако даље, до „последњег" корена $\{\alpha_r, \frac{1}{\alpha_r}\}, (r \leq n)$. Нека је вишеструкост од (-1) означена са n_{-1}. Тада је број корена

$$\left(\sum_{i=1}^{r} 2n_i\right) + 2k + n_{-1} = \left(2\sum_{i=1}^{r} n_i\right) + 2k + n_{-1}.$$

А пошто је n непарно и оба $(2\sum_{i=1}^{r} n_i)$ и $2k$ су парни, морамо имати n_{-1} које је непарно.

Сада, у случају полинома парног степена, n би било парно, па пошто $(2\sum_{i=1}^{r} n_i)$ и $2k$ су парни, мора бити и n_{-1} парно.

□

Лема 4. *Нека је $f \in \mathbb{Q}[t]$ такав да је $f(0) \neq 0$. Тада је $ff_{obr} \in \mathcal{R}$.*

Доказ. Користећи последице са почетка овог одељка можемо доказати лему. Ако је $f(0) \neq 0$, онда ff_{obr} има степен једнак $2\deg f$ и $(ff_{obr})_{obr} = ff_{obr}$. □

Следеће тврђење ће окарактерисати образац факторизације реципрочног полинома у $\mathbb{Q}[t]$. Прво ћемо приметити да ако је f било који реципрочни полином из $\mathbb{Q}[t]$, из Тврђења 4 следи да ако је 1 корен полинома $f(t)$, онда ће имати парну вишеструкост, рецимо r. Следи да је $(t-1)^r$ реципрочан полином, а одатле $f(t) = (t-1)^r g(t)$, где је $g(t) \in \mathbb{Q}[t]$ реципрочан, па можемо изоставити случај у коме је $f(1) = 0$.

Полином $f(t)$ називамо реципрочним ако је $f(t) = f_{obr}(t)$, а ако није називамо га нереципрочни полином. Дефинишемо нереципрочни део моничног полинома $f(t)$ у $\mathbb{Z}[t]$ тако што уклонимо реципрочне нерастављиве факторе и оно што остане представља нереципрочни део полинома $f(t)$. Више о нереципрочном делу полинома $f(t)$ можете наћи у раду [10].

Тврђење 5. *Нека је $f \in \mathbb{Q}[t]$ произвољан реципрочни полином са $f(1) \neq 0$ и нека је g нерастављиви фактор из $\mathbb{Q}[t]$ полинома $f(t)$. Ако полином g није реципрочан, онда је $f = gg_{obr}h$, где је $h \in \mathbb{Q}[t]$ реципрочан.*

Доказ. Нека је $g \in \mathbb{Q}[t]$ нерастављиви нерециprочни фактор полинома f. Конкретно, g није ни полином $t-1$, ни полином $t+1$. Имамо да је g_{obr} такође нерастављив у $\mathbb{Q}[t]$. За сваки корен α полинома g знамо да је $1/\alpha$ корен полинома g_{obr}. Пошто је f реципрочан, $1/\alpha$ је такође корен полинома f. Дакле, испоставља се да је g_{obr} такође нерастављив фактор полинома f (узајамно прост са g) и стога је gg_{obr} фактор полинома f. Из Леме 4 следи да gg_{obr} припада $\mathcal{R}$, а према Леми 3 закључујемо да се полином f факторише као $gg_{obr}h$, где је $h \in \mathbb{Q}[t]$ реципрочни полином. □

Фактор gg_{obr} из Тврђења 5 је повезан са нерециprочним делом полинома f.

Сада уводимо појам нерастављивости у скупу $\mathcal{R}$.

Дефиниција 17. *Ако полином $f(t) \in \mathcal{R}$ не можемо да добијемо као производ фактора два неконстантна полинома из $\mathcal{R}$, онда кажемо да је $f(t)$ нерастављив у $\mathcal{R}$.*

На основу ове дефиниције, видимо да t^2-2t+1 је нерастављив у $\mathcal{R}$, али не и у $\mathbb{Q}[t]$. Следи да нерастављивост над $\mathcal{R}$ не повлачи нерастављивост над $\mathbb{Q}[t]$. Међутим, сваки полином $f(t) \in \mathcal{R}$ који је нерастављив у $\mathbb{Q}[t]$ је такође нерастављив и у $\mathcal{R}$. За даљи рад увешћемо следеће ознаке:

$$Irred(\mathcal{R}) = \{f(t) \in \mathcal{R} : f(t) \text{ је нерастављив над } \mathcal{R}\},$$

$$Red(\mathcal{R}) = \{f(t) \in \mathcal{R} : f(t) \text{ је растављив над } \mathcal{R}\}.$$

Као последица Тврђења 5, можемо у потпуности да окарактеришемо факторизацију над $\mathbb{Q}$ нерастављивог елемента $f(t) \in \mathcal{R}$.

Последица 1. *Нека је $f(t) \in Irred(\mathcal{R})$. Или је $f(t)$ нерастављив у $\mathbb{Q}[t]$ или је $f = agg_{obr}$, где је $g \in \mathbb{Q}[t]$ нерастављив и $a \in \mathbb{Q}^*$.*

Из Последице 1 следи да се $Irred(\mathcal{R})$ дели на два скупа $\mathcal{R}_1 \cup \mathcal{R}_2$ где је

$$\mathcal{R}_1 = \{f(t) \in Irred(\mathcal{R}) : f(t) \text{ је нерастављив над } \mathbb{Q}\},$$

$$\mathcal{R}_2 = \{f(t) \in Irred(\mathcal{R}) : f = agg_{obr}, a \in \mathbb{Q}^*, g(t) \text{ је нерастављив над } \mathbb{Q}\}.$$

Приметимо да ако је $f(t) \in Irred(\mathcal{R})$, $\deg f = 2$ и $f(1) = 0$, онда је $f(t) = a(t-1)(-t+1)$ и тада $f(t)$ припада $\mathcal{R}_2$.

Напомена 1. *У случају када полином $f(t) \in \mathcal{R}_2$ има целобројне коефицијенте, као последица Гаусове леме 4, можемо претпоставити да је $f = agg_{obr}$, $a \in \mathbb{Z}$, $g \in \mathbb{Z}[t]$. Посебно, ако је $f(t)$ примитивни полином, онда је $f = \pm gg_{obr}$, где је $g(t)$ примитивни полином. Ово је битно за испитивање нерастављивости над $\mathbb{Q}$ јер увек можемо претпоставити да је $f(t)$ примитиван полином.*

Глава 3

Метода реципрочне замене

Дато је $f(t) \in \mathcal{R}$ степена $2n$, заменом променљивих $x = t + 1/t$, добијамо полином из $\mathbb{Q}[x]$ степена n, чији су корени облика $\alpha+1/\alpha$, при чему је α корен полинома $f(t)$. Претпоставимо да можемо израчунати n корена полинома $f(x)$, добијеног заменом променљивих $x = t+1/t$, тада можемо добити корене полинома $f(t)$ решавањем n квадратних једначина. Ово је класичан метод израчунавања корена реципрочних полинома.

Нека је $f(t) \in \mathcal{R}$ полином степена $2n$. Полином $f(t)$ можемо записати на следећи начин:

$$f(t) = a_n t^{2n} + ... + a_1 t^{n+1} + a_0 t^n + a_1 t^{n-1} + ... + a_n,$$

односно

$$f(t) = a_0 t^n + \sum_{k=1}^{n} a_k (t^{n+k} + t^{n-k})$$

где су $a_0, ..., a_n$ из $\mathbb{Q}$. Индукцијом по k, може се показати да $t^k + 1/t^k$ можемо изразити преко x јединственим моничним полиномом $f_k \in \mathbb{Z}[x]$ степена k. Ови полиноми се могу рекурзивно израчунати уз помоћ следећих понављања:

$$f_n(x) = x f_{n-1}(x) - f_{n-2}(x), \qquad f_0(x) = 2, \quad f_1(x) = x. \tag{3.1}$$

Први чланови рекурзије (3.1) су полиноми:

$$f_2(x) = x^2 - 2, \quad f_3(x) = x^3 - 3x, \quad f_4(x) = x^4 - 4x^2 + 2, \quad f_5(x) = x^5 - 5x^3 + 5x.$$

Дакле, за било које $f(t) \in \mathcal{R}$

$$f(t) = a_0 t^n + \sum_{k=1}^{n} a_k (t^{n+k} + t^{n-k}) = a_0 t^n + t^n \sum_{k=1}^{n} a_k \left(t^k + \frac{1}{t^k} \right)$$

$$f(t) = a_0 t^n + t^n \sum_{k=1}^{n} a_k f_k \left(t + \frac{1}{t} \right)$$

$$f(t) = t^n \left(a_0 + \sum_{k=1}^{n} a_k f_k \left(t + \frac{1}{t} \right) \right),$$

одатле закључујемо да је

$$p(x) = a_0 + \sum_{k=1}^{n} a_k f_k(x) \in \mathbb{Q}[x]$$

једини полином који задовољава функционалну једначину

$$f(t) = t^{\deg f/2} p(x(t)), \quad x(t) = t + \frac{1}{t}. \tag{3.2}$$

Ово нам обезбеђује ефикасан начин израчунавања полинома $p \in \mathbb{Q}[x]$ за свако $f(t) \in \mathcal{R}$. Одатле имамо пресликавање $\mathbf{R}$ из $\mathcal{R}$ у $\mathbb{Q}[x]$ дефинисано на следећи начин:

$$\begin{aligned} \mathbf{R} \quad : \quad \mathcal{R} &\to \quad\quad\quad \mathbb{Q}[x] \\ f(t) &\mapsto a_0 + a_1 f_1(x) + \ldots + a_n f_n(x). \end{aligned}$$

Посебно, приметимо да за свако $k \in \mathbb{N}$ имамо

$$\mathbf{R}(t^{2k} + 1) = f_k.$$

Назваћемо низ $(f_n)_{n \in \mathbb{N}}$ низ реципрочне замене и пресликавање $\mathbf{R}$ реципрочно пресликавање.

Следећа својства реципрочног пресликавања $\mathbf{R}$ можемо директно добити из једначине (3.2).

Тврђење 6. $\mathbf{R}$ *задовољава следећа својства.*

1. $\mathbf{R}$ *је бијективно пресликавање.*

2. $\mathbf{R}(fg) = \mathbf{R}(f)\mathbf{R}(g)$ *за свако* $f, g \in \mathcal{R}$.

Коначно ћемо показати да постоји матрични запис у којем можемо разумети реципрочно пресликавање $\mathbf{R}$.

Нула вектор $\vec{0}$ не припада скупу $\mathcal{R}$, јер нула полином $f(t) \equiv 0$ има степен који се не дефинише, односно нула вектор није парног степена. Следи да $\mathcal{R}$ није $\mathbb{Q}$-векторски простор.

Иако $\mathbf{R}$ није линеарно пресликавање јер $\mathcal{R}$ није $\mathbb{Q}$-векторски простор, када се ограничи на елементе из $\mathcal{R}$ степена $2n$ можемо записати матрицу за $\mathbf{R}$. Ово је корисна особина која ће нам омогућити да добијемо укупан број нерастављивих реципрочних полинома.

Фиксирајмо $n \in \mathbb{N}$. Свако $f \in \mathcal{R}$ степена $2n$ можемо записати као вектор коефицијената $n+1$ координата које означавамо са $[f]$:

$$[f] = (a_n, a_{n-1}, ..., a_0) \in \mathbb{Q}^{n+1}, \quad a_n \neq 0.$$

Размотримо $(n+1) \times (n+1)$ матрицу $\mathbf{R}_n$ чији су елементи a_{ij} коефицијенти уз x^{n-i+1} у полиному f_{n-j+1}, осим елемента $a_{n+1,n+1}$ који је једнак 1 (уместо 2). Важи једнакост

$$[\mathbf{R}(f)]^T = \mathbf{R}_n \cdot [f]^T, \tag{3.3}$$

где је $[\mathbf{R}(f)]$ вектор коефицијената $\mathbf{R}(f)$ са моничном базом $\{x^n, ..., x^2, x, 1\}$, а $[\mathbf{R}(f)]^T$ транспонована матрица.

Матрица $\mathbf{R}_n$ је доња троугаона целобројна матрица.

На пример, ако је $n = 5$, имамо

$f_0 = 1$

$f_1 = t + \frac{1}{t} = x$

$f_2 = t^2 + \frac{1}{t^2} = (t + \frac{1}{t})^2 - 2 = x^2 - 2$

$f_3 = t^3 + \frac{1}{t^3} = (t + \frac{1}{t})^3 - 3(t + \frac{1}{t}) = x^3 - 3x$

$f_4 = t^4 + \frac{1}{t^4} = \left(t + \frac{1}{t}\right)^4 - 4\left(t + \frac{1}{t}\right)^2 + 2 = x^4 - 4x^2 + 2$

$f_5 = t^5 + \frac{1}{t^5} = \left(t + \frac{1}{t}\right)^5 - 5\left(t + \frac{1}{t}\right)^3 + 5\left(t + \frac{1}{t}\right) = x^5 - 5x^3 + 5x.$

Матрица $\mathbf{R}_5$ ће имати облик

$$\mathbf{R}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -5 & 0 & 1 & 0 & 0 & 0 \\ 0 & -4 & 0 & 1 & 0 & 0 \\ 5 & 0 & -3 & 0 & 1 & 0 \\ 0 & 2 & 0 & -2 & 0 & 1 \end{pmatrix}.$$

Позивајући се на Пример 11 из Увода, векторски коефицијент циклотомичног полинома Φ_{11} је $[\Phi_{11}] = (1, 1, 1, 1, 1, 1)$ и следи да се векторски коефицијент од $\mathbf{R}(\Phi_{11})$ добија израчунавањем

$$[\mathbf{R}(f)]^T = \mathbf{R}_5 \cdot (1, 1, 1, 1, 1, 1)^T =$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -5 & 0 & 1 & 0 & 0 & 0 \\ 0 & -4 & 0 & 1 & 0 & 0 \\ 5 & 0 & -3 & 0 & 1 & 0 \\ 0 & 2 & 0 & -2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ -4 \\ -3 \\ 3 \\ 1 \end{pmatrix} = (1, 1, -4, -3, 3, 1)^T,$$

одакле добијамо

$$\mathbf{R}(f) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

Глава 4

Критеријуми нерастављивости над $\mathbb{Q}$

Почињемо ову главу прецизним дефинисањем критеријума нерастављивости. Критеријум којим ћемо се бавити је критеријум нерастављивости у $\mathcal{R}$ и њиме завршавамо карактеризацију дату у Последици 1.

Тврђење 7. *Нека је $f \in \mathcal{R}$. Тада је f нерастављив у $\mathcal{R}$ ако и само ако је $\mathbf{R}(f)$ нерастављив у $\mathbb{Q}[x]$.*

Доказ. Нека је $f = f_1 f_2$ факторизација у $\mathcal{R}$ таква да је $2 \leq \deg f_i < \deg f$, $i = 1, 2$. Тада је $\mathbf{R}(f) = \mathbf{R}(f_1)\mathbf{R}(f_2)$ факторизација из $\mathbb{Q}[x]$ таква да је $1 \leq \deg \mathbf{R}(f_i) < \deg f/2$.

Узајамно, ако $\mathbf{R}(f)$ садржи факторе у $\mathbb{Q}[x]$, својства пресликавања од $\mathbf{R}$ подразумевају да f садржи факторе у $\mathcal{R}$. □

Тврђење 7 нам говори о повезаности између нерастављивости у скупу $\mathcal{R}$ и у $\mathbb{Q}[x]$. Можемо га преформулисати и записати преко реципрочног пресликавања. Означићемо са $Irred(\mathbb{Q})$ и $Red(\mathbb{Q})$, редом, скупове нерастављивих и растављивих елемената из $\mathbb{Q}[x]$, односно, имамо да је

$$\mathbf{R}(Irred(\mathcal{R})) = Irred(\mathbb{Q}), \quad \mathbf{R}(Red(\mathcal{R})) = Red(\mathbb{Q}). \tag{4.1}$$

Пример 12. *Нека је $f \in \mathbb{Z}[t]$ моничан реципрочни полином степена 4 такав да $\mathbf{R}(f)$ нема рационалне корене. Користећи Тврђење 7 и Последицу 1 закључујемо да је тај полином нерастављив над $\mathbb{Q}$ осим у случају кад је $f = t^4 - (b^2+2)t^2 + 1, b \in \mathbb{Z}$. У овом случају имамо факторизацију $f = -gg_{obr}$, где је $a = -1, g = t^2 + bt - 1$, и $g_{obr} = 1 + bt - t^2$.*

Следећи пример показује да не можемо одредити нерастављивост полинома f из $\mathbb{Q}[t]$ ако је $\mathbf{R}(f)$ из $\mathbb{Q}[x]$.

Пример 13. *Ако је* $f = t^6 - 3t^5 - 3t^4 + 11t^3 - 3t^2 - 3t + 1$, *онда је* $[\mathbf{R}(f)]^T = \mathbf{R}_3(1, -3, -3, 11)^T = (1, -3, -6, 17)^T$, *следи* $\mathbf{R}(f) = x^3 - 3x^2 - 6x + 17$. *Нерастављивост* $\mathbf{R}(f)$ *над* $\mathbb{Q}$ *се види, јер да би полином трећег степена био растављив у* $\mathbb{Q}$ *мора да има рационалне нуле. Потенцијалне рационалне нуле су* $\pm 17, \pm 1$, *међутим заменом добијамо да ови бројеви нису нуле датог полинома и одатле следи да је* f *нерастављиво над* $\mathcal{R}$. *Међутим,* f *није нерастављиво над* $\mathbb{Q}$ *јер има факторе* $(t^3 - 3t + 1)(t^3 - 3t^2 + 1)$. *На основу Последице 1, видимо да је* $f = gg_{obr}$ *са* $g = t^3 - 3t + 1$ *један нерастављиви елемент из* $\mathbb{Q}[t]$.

Теорема 7. *(Ајзенштајнов критеријум нерастављивости)*
Нека је $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ *и нека постоји прост број* p *такав да* $p \nmid a_n$, $p | a_{n-1}, a_{n-2}, ..., a_1, a_0$ *и* $p^2 \nmid a_0$. *Тада је* $f(x)$ *нерастављив у* $\mathbb{Q}[x]$.

Доказ теореме можете наћи у књизи [3].
Следећа теорема је главна теорема овог рада и односи се на критеријум нерастављивости реципрочних полинома.

Теорема 8. *Нека је* $f(t) \in \mathcal{R}$, *односно нека је* $f(t)$ *реципрочан полином парног степена и нека је* $f(t)$ *примитивни полином и претпоставимо да је* $\mathbf{R}(f)$ *нерастављив у* $\mathbb{Q}[x]$.

1. *Ако* $|f(1)|$ *или* $|f(-1)|$ *нису потпуни квадрати, онда је полином* $f(t)$ *нерастављив у* $\mathbb{Q}[t]$.

2. *Ако* $f(1)$ *и средњи коефицијент полинома* $f(t)$ *имају различите знаке, тада је* $f(t)$ *нерастављив у* $\mathbb{Q}[t]$.

3. *Ако је средњи коефицијент полинома* $f(t)$ $0, 1$ *или* -1, *тада је* $f(t)$ *нерастављив у* $\mathbb{Q}[t]$.

Доказ. На основу Тврђења 7, имамо да је $f(t)$ нерастављив у $\mathcal{R}$, док год је $\mathbf{R}(f)$ нерастављиво. Из Последице 1 следи да је полином $f(t)$ нерастављив у $\mathbb{Q}$ или, претпостављајући да је полином $f(t)$ примитиван, онда је полином облика $f = \pm gg_{obr}, g \in \mathbb{Z}[t]$ нерастављив полином над $\mathbb{Q}$. Претпоставимо да $f(t)$ није нерастављив над $\mathbb{Q}$. Показаћемо да ова претпоставка доводи до контрадикције.

Како је $g(1) = g_{obr}(1)$, тада $|f(1)| = |g(1)|^2$, што је контрадикторно са чињеницом да $|f(1)|$ није потпун квадрат. Слично, из $g(-1) = \pm g_{obr}(-1)$ имамо да је $|f(-1)| = |g(-1)|^2$. Следи да је 1. услов задовољен.

У 2. услову, ако је $f(1) > 0$ тада је $f = gg_{obr}$. Ако запишемо $g(t)$ у облику $g(t) = a_n t^n + a_{n-1}t^{n-1} + ... + a_1 t + a_0$ добићемо да је средњи коефицијент полинома $f(t)$ једнак $a_0^2 + a_1^2 + ... + a_{n-1}^2 + a_n^2$. Ово није могуће јер средњи коефицијент има негативну вредност. Слично доказујемо и за $f(1) < 0$.

Услов 3. је директна последица средњег коефицијента датог у услову 2. □

У наставку ћемо видети примену ове теореме на примере.

Пример 14. *Размотримо полином* $f = t^8+6t^7+2t^6+22t^5-8t^4+22t^3+2t^2+6t+1$. *Имамо да је* $\mathbf{R}(f) = x^4+6x^3-2x^2+4x-10$. *На основу Ајзенштајновог критеријума, докажимо да је* $\mathbf{R}(f)$ *нерастављив над* $\mathbb{Q}[x]$. *Посматрајмо прост број* $p = 2$ *и* $a_4 = 1, a_3 = 6, a_2 = -2, a_1 = 4, a_0 = -10$ *коефицијенти из полинома* $\mathbf{R}(f)$. $2 \nmid 1, 2 \mid 6, -2, 4, -10, 2^2 \nmid -10$ *што задовољава услове Ајзенштајновог критеријума, одакле следи да је* $\mathbf{R}(f)$ *нерастављив над* $\mathbb{Q}[x]$. *Полином* f *је примитиван јер садржи целобројне коефицијенте и* $(1, 6, 2, 22, -8) = 1$. $|f(1)| = 54$ *и* $|f(-1)| = 58$, *па на основу Теореме 8 закључујемо да је* f *нерастављив над* $\mathbb{Q}$.

Пример 15. *Нека је* $f \in \mathcal{R}$ *са коефицијентима* 0 *или* 1. *Ако је* $\mathbf{R}(f)$ *нерастављив у* $\mathbb{Q}[x]$, *одатле следи да је* f *нерастављив у* $\mathbb{Q}[t]$.

Пример 16. *Посматрајмо следећи низ полинома из* $\mathbb{Q}[t]$ *за* $n \geq 2$:

$$g_n(t) = \frac{(t+1)^n - t^n - 1}{t}.$$

Сваки полином g_n *има степен* $n-2$. *Записаћемо* g_n *преко биномне формуле*

$$(t+1)^n = \binom{n}{0}t^n + \binom{n}{1}t^{n-1} + \binom{n}{2}t^{n-2} + ... + \binom{n}{n-1}t + \binom{n}{n}$$

$$g_n(t) = \frac{t^n + \binom{n}{1}t^{n-1} + \binom{n}{2}t^{n-2} + ... + \binom{n}{n-1}t + 1 - t^n - 1}{t}$$

$$g_n(t) = \binom{n}{1}t^{n-2} + \binom{n}{2}t^{n-3} + ... + \binom{n}{n-2}t + \binom{n}{n-1}.$$

Једна од особина биномних коефицијената је $\binom{n}{k} = \binom{n}{n-k}$, *па следи да је* g_n *реципрочан полином. Када је* n *парно, полином* g_n *припада* $\mathcal{R}$. *Дефинисањем*

$m := (n-2)/2$, *имамо да је*

$$\mathbf{R}(g_n) = \binom{n}{1} f_m + \binom{n}{2} f_{m-1} + ... + \binom{n}{n/2-1} f_1 + \binom{n}{n/2},$$

где су $f_1, ..., f_m$ *првих* m *полинома реципрочне замене низа.*

Нека је $n = 2p$, *где је* p *непаран прост број. Следи да је*

$$\mathbf{R}(g_{2p}) = \binom{2p}{1} f_{p-1} + \binom{2p}{2} f_{p-2} + ... + \binom{2p}{p-1} f_1 + \binom{2p}{p}.$$

Приметимо да

$$\binom{2p}{j} \equiv 0 \pmod{p},\ j = 1, ..., p-1,$$

јер $p | \binom{2p}{j} - 0$, *за* $j = 1, ..., p-1$, *и*

$$\binom{2p}{p} \not\equiv 0 \pmod{p},$$

односно $p \nmid \binom{2p}{p} - 0$.

Користећи претходну чињеницу на основу Ајзенштајновог критеријума видимо да је $\mathbf{R}(g_{2p})_{obr}$ *нерастављив над* $\mathbb{Q}$, *па следи да је* $\mathbf{R}(g_{2p})$ *нерастављив над* $\mathbb{Q}$. *Пошто* $g_{2p}(1) = 2^{2p} - 2$ *није потпун квадрат, наш критеријум показује да* g_{2p} *јесте нерастављив над* $\mathbb{Q}$.

Глава 5

Нумеричко понашање реципрочног пресликавања

За наше комбинаторне резултате потребан нам је увид у то како се увећавају коефицијенти од $\mathbf{R}(f)$ у односу на полином f. Такође, бавићемо се проблемом релације броја коефицијената датог полинома g и производа gg_{obr}. На тај начин добићемо интересантне резултате који се односе на низ реципрочне замене $(f_n)_{n\in\mathbb{N}}$.

Дато је $f(x)=\sum_{k=0}^{n} a_k x^k \in \mathbb{Q}[x]$. 1−норма $||f||_1$ и max-норма $||f||_\infty$ полинома $f(x)$, су редом, бројеви

$$||f||_1 \;=\; \sum_{i=0}^{n} |a_i|,$$

$$||f||_\infty \;=\; \max\{|a_i| \;:\; i=0,1,...,n\}.$$

Посматрајмо низ 1−норми чланова низа реципрочне замене $(||f_n||_1)_{n\in\mathbb{N}}$ (низ реципрочне замене има редом елементе $f_0(x)=2, f_1(x)=x, f_2(x)=x^2-2, f_3(x)=x^3-3x, f_4(x)=x^4-4x^2+2, f_5(x)=x^5-5x^3+5x...$). Први чланови 1−норме низа су

$||f_0||_1 = |a_0| = |2| = 2,$
$||f_1||_1 = |a_0| + |a_1| = |1| = 1,$
$||f_2||_1 = |a_0| + |a_1| + |a_2| = |1| + |0| + |-2| = 3,$
$||f_3||_1 = |a_0| + |a_1| + |a_2| + |a_3| = |1| + |0| + |-3| + |0| = 4,$
$||f_4||_1 = |a_0| + |a_1| + |a_2| + |a_3| + |a_4| = |1| + |0| + |-4| + |0| + |2| = 7,$
$||f_5||_1 = |a_0| + |a_1| + |a_2| + |a_3| + |a_4| + |a_5| = |1| + |0| + |-5| + |0| + |5| + |0| = 11.$

Дефиниција 18. *Нека је низ L_n задат следећом рекурентном једначином:*

$$L_n = L_{n-1} + L_{n-2}$$

$$L_1 = 1, L_2 = 3 \text{ или } L_0 = 2, L_1 = 1.$$

Низ L_n називамо Лукасов низ. Лукасови бројеви су елементи Лукасовог низа. То су бројеви: $2, 1, 3, 4, 7, 11, 18, 29....$

Више о Лукасовим бројевима можете наћи у раду [9]. Треба уочити да је низ реципрочне замене подударан са низом Лукасових бројева. Рекурзијом (3.1) која дефинише низ реципрочне замене долазимо до рекурзије за $||f_n||_1$:

$$||f_n||_1 = ||f_{n-1}||_1 + ||f_{n-2}||_1, \qquad ||f_0||_1 = 2,\ ||f_1||_1 = 1, \tag{5.1}$$

дакле до доказивања једнакости ова два низа.

Тврђење 8. *Целобројни низ $(||f_n||_1)_{n\in\mathbb{N}}$ је низ Лукасових бројева.*

Сада ћемо анализирати понашање $||f||_\infty$ при пресликавању $\mathbf{R}$ и добићемо неке интересантне резултате у вези са низом реципрочне замене $(f_n)_{n\in\mathbb{N}}$. Да би одредили горњу границу од $||\mathbf{R}(f)||_\infty$ за било које $f \in \mathcal{R}$ степена $2n$ које има max-норму $||f||_\infty \leq B$, биће згодно позвати се на матричну репрезентацију $\mathbf{R}_n$ од $\mathbf{R}$ дефинисану у (3.3).

Ако матричну норму индукујемо векторском нормом, добијамо да је max-норма од $\mathbf{R}_n$ као оператора, број

$$||\mathbf{R}_n||_\infty = \max_{1\leq i\leq n+1} \sum_{j=1}^{n+1} |a_{ij}|.$$

Наша матрична репрезентација нам дозвољава да израчунамо $\mathbf{R}(f)$ израчунавањем производа $\mathbf{R}_n \cdot [f]^T$ и одатле следи

$$||\mathbf{R}(f)||_\infty \leq ||\mathbf{R}_n||_\infty ||f||_\infty.$$

Из Тврђења 8 следи горња граница max-норме $\mathbf{R}_n$. За $n \in \mathbb{N}$ важи следећа неједнакост:

$$||\mathbf{R}_n||_\infty = \max_{1\leq i\leq n+1} \sum_{j=1}^{n+1} |a_{ij}| \leq \sum_{j=1}^{n+1}\sum_{i=1}^{n+1} |a_{ij}| = 1 + \sum_{j=1}^{n} ||f_j||_1 = 1 + \sum_{j=1}^{n} L_j.$$

Из особине о Лукасовим бројевима, $\sum_{j=0}^{n} L_j = L_{n+2} - 1$ (пример: $\sum_{j=0}^{3} L_j = 2 + 1 + 3 + 4 = 10, L_5 - 1 = 11 - 1 = 10$), можемо закључити да

$$||\mathbf{R}(f)||_\infty \leq ||\mathbf{R}_n||_\infty ||f||_\infty \leq L_{n+2} B.$$

На овај начин смо показали следеће тврђење.

Тврђење 9. *Нека је $f \in \mathcal{R}$ степена $2n$ и $||f||_\infty = B$. Тада*

$$||\mathbf{R}(f)||_\infty \leq L_{n+2} B.$$

Остаје нам да наведемо још једно тврђење које се односи на max-норму датог полинома g на основу Последице 1.

Тврђење 10. *Нека је $f \in \mathcal{R}_2$, где је скуп $\mathcal{R}_2 = \{f(t) \in Irred(\mathcal{R}) : f = agg_{obr}, a \in \mathbb{Q}^*, g(t)$ је нерастављив над $\mathbb{Q}\}$ са целобројним коефицијентима степена $2n$ и* max*-нормом $||f||_\infty \leq B$. Тада нерастављиви полином $g \in \mathbb{Z}[t]$ степена n такав да важи $f = agg_{obr}, a \in \mathbb{Z}$ има* max*-норму $||g||_\infty$ највише $\sqrt{B}$.*

Доказ. Нека је $g = a_n t^n + ... + a_1 t + a_0$ (са $a_n \neq 0$) и претпоставимо да је $||g||_\infty = |a_i|, 0 \leq i \leq n$. Средњи коефицијент полинома f је једнак $a(a_0^2 + a_1^2 + ... + a_n^2)$ и одатле следи

$$||g||_\infty^2 = |a_i|^2 \leq \sum_{i=0}^{n} |a_i|^2 \leq ||f||_\infty \leq B.$$

□

Глава 6

Број елемената растављивих и нерастављивих реципрочних полинома

У овој глави ћемо објаснити како добијамо горња ограничења за број елемената у скупу $Red(\mathcal{R})$ и $Irred(\mathcal{R})$. Интересантна карактеристика је да реципрочни полиноми могу имати нереципрочне факторе. Међутим, показаћемо да је број таквих полинома мали. Филасетине белешке [10] су добра референца за овај део рада.

Нека је n фиксиран природни број. Сваки полином степена n са целобројним коефицијентима може се представити као тачка $(a_n, a_{n-1}, ..., a_1, a_0)$ из $(n+1)$-димензионе решетке $\mathbb{Z}^{n+1}$. За позитивно B посматрамо оне тачке решетке које леже у $(n+1)$-коцки $[-B, B]^{n+1}$:

$$S_n(B) := \{f \in \mathbb{Z}[t] : \deg f = n, ||f||_\infty \leq B\}.$$

На овај начин $S_n(B)$ представља скуп полинома степена n са целобројним коефицијентима у интервалу $[-B, B]$. Имамо да је број $|S_n(B)| = 2B(2B+1)^n$ за целобројно B.

Важи следеће ограничење:

$$|Red(\mathbb{Q}) \cap S_n(B)| \ll_n B^n \log^2 B, \tag{6.1}$$

где ознака $\ll_n$ значи да постоји константа која зависи само од n у горњем ограничењу. Ова граница се први пут појављује у класичној књизи Georga Polya и Gabora Szego као вежба 266 у Одељку VIII. Више објашњења се може наћи

у радовима K. Dorge, Abschatzung der anzahl der reduziblen polynome, Math. Ann. 160 (1965) 59–63, G. Kuba, On the distribution of reducible polynomials, Math. Slovaca 59 (2009) 349–356. [12] и Dubickas, On the number of reducible polynomials of bounded naive height, Manuscripta Math. 144 (2014) 439–456. За потребе овог рада је довољно разматрати горње ограничење дато у (6.1).

Из горњег ограничења (6.1) такође можемо добити горње ограничење пропорције:

$$\frac{|Red(\mathbb{Q}) \cap S_n(B)|}{|S_n(B)|} \ll_n \frac{B^n \log^2 B}{2B(2B+1)^n} \ (B \in \mathbb{N}). \tag{6.2}$$

$$\lim_{B\to\infty} \frac{B^n \log^2 B}{2B(2B+1)^n} = \lim_{B\to\infty} \frac{B^n \log^2 B}{2B \cdot B^n(2+\frac{1}{B})^n} = \lim_{B\to\infty} \frac{\log^2 B}{2^{n+1}B} = 0.$$

Ова пропорција тежи ка 0 када B тежи бесконачности.

Теорема 9. *Вероватноћа да је полином са целобројним коефицијентима одређеног степена растављив је једнака нули.*

Доказ теореме можете пронаћи у раду мађарских математичара Џорџа Поља и Габора Сеге.

Из теореме следи да су скоро сви полиноми у $\mathbb{Z}$ нерастављиви над $\mathbb{Q}$.

Наш циљ је да искористимо претходни резултат како бисмо добили неке процене о броју растављивих и нерастављивих реципрочних полинома.

Скуп $Red(\mathcal{R}) \cap S_{2n}(B)$ је скуп растављивих целобројних реципрочних полинома степена $2n$ и max-норме највише B. Наш први резултат је горње ограничење броја $|Red(\mathcal{R}) \cap S_{2n}(B)|$.

Теорема 10. *Нека је B позитиван цео број. Тада*

$$|Red(\mathcal{R}) \cap S_{2n}(B)| \ll_n B^n \log^2 B.$$

Доказ. Из (4.1) и Тврђења 9 следи да је

$$\mathbf{R}(Red(\mathcal{R}) \cap S_{2n}(B)) \subset Red(\mathbb{Q}) \cap S_n(B'),$$

где је $B' = L_{n+2}B$ и одатле следи

$$|Red(\mathcal{R}) \cap S_{2n}(B)| \leq |Red(\mathbb{Q}) \cap S_n(B')|.$$

Примењујући (6.1) на десну страну претходне неједнакости, закључујемо да

$$|Red(\mathcal{R}) \cap S_{2n}(B)| \ll_n (L_{n+2}B)^n (\log(L_{n+2}B))^2.$$

□

Подсећајући се да је било које $f(t) \in \mathcal{R}$ степена $2n$ дато вектором коефицијената $[f] = (a_n, a_{n-1}, ..., a_1, a_0) \in \mathbb{Q}^{n+1}$, са $a_n \neq 0$, имамо да је

$$|\mathcal{R} \cap S_{2n}(B)| = 2B(2B+1)^n, \quad B \in \mathbb{N},$$

а затим из Теореме 10 добијамо пропорцију

$$\frac{|Red(\mathcal{R}) \cap S_{2n}(B)|}{|\mathcal{R} \cap S_{2n}(B)|} \ll_n \frac{B^n (\log B)^2}{2B(2B+1)^n}, \tag{6.3}$$

који тежи ка 0 када B тежи бесконачности. Инспирисани уобичајеном терминологијом, рећи ћемо да су скоро сви полиноми у $\mathcal{R}$ са целобројним коефицијентима нерастављиви у $\mathcal{R}$.

Напомена 2. *Можемо тврдити да је скривено константно ограничење из Теореме 10 грубо. Наш приступ се састоји од уграђивања $(n+1)$-димензионалне коцке $[-B, B]^{n+1}$ у $(n+1)$-димензионалну коцку $[-L_{n+2}B, L_{n+2}B]$ и тада обухватамо више нерастављивих полинома него што је потребно. Међутим, у пропорцији је најбитније да тежи нули док B тежи бесконачности.*

Као последица Последице 1 знамо да је $Irred(\mathcal{R}) = \mathcal{R}_1 \cup \mathcal{R}_2$. Наш циљ је да покажемо да је већина нерастављивих полинома у $\mathcal{R}$ већ нерастављива у $\mathbb{Q}[t]$. Другим речима, показаћемо да $\mathcal{R}_2$ има врло мало елемената.

Нека је f полином из $\mathcal{R}_2 \cap S_{2n}(B)$. Пре свега, уочимо, позивајући се на критеријум нерастављивости (Теорема 7) да можемо одбацити случај $B = 1$. У том случају је скуп $\mathcal{R}_2 \cap S_{2n}(B)$ празан. Тако да можемо претпоставити да је B цео број већи или једнак 2.

Теорема 11. *Нека је $B \in \mathbb{Z}$ и $B \geq 2$. Тада*

$$|\mathcal{R}_2 \cap S_{2n}(B)| \leq 4B\sqrt{B}(2\sqrt{B}+1)^n.$$

Доказ. Према Тврђењу 10 знамо да за полином $f \in \mathcal{R}_2 \cap S_{2n}(B)$ постоји нерастављиви полином $g \in \mathbb{Z}[t]$ са max-нормом $||g||_\infty \leq \sqrt{B}$ такав да је $f = agg_{obr}$ за неко ненула целобројно $a \in [-B, B]$. Из Леме 4 имамо

$$|\mathcal{R}_2 \cap S_{2n}(B)| \leq 2B|\{gg_{obr} : g \in Irred(\mathbb{Q})\} \cap S_n(\sqrt{B})|.$$

Пошто важи следеће ограничење:

$$|\{gg_{obr} : g \in Irred(\mathbb{Q})\} \cap S_n(\sqrt{B})| \leq 2\sqrt{B}(2\sqrt{B}+1)^n$$

одатле следи наша теорема. □

Као непосредну последицу Теореме 11, изводимо следећу пропорцију:

$$\frac{|\mathcal{R}_2 \cap S_{2n}(B)|}{|\mathcal{R} \cap S_{2n}(B)|} \leq 2\sqrt{B}\left(\frac{2\sqrt{B}+1}{2B+1}\right)^n \leq \frac{2\sqrt{B}}{(\sqrt{B}-1/2)^n}. \tag{6.4}$$

Претходна једначина показује да је број нерастављивих полинома у $\mathcal{R}$ који припадају $\mathcal{R}_2$ скоро ирелевантан броју реципрочних полинома за $n \geq 2$. (Подсетимо се да је $\mathcal{R}_2$ празан за $B = 1$.) Из пропорција (6.3) и (6.4), долазимо до закључка да је већина полинома из $\mathcal{R} \cap S_{2n}(B)$ нерастављива над $\mathbb{Q}$ када B тежи бесконачности.

Теорема 12. *Скоро сви полиноми $f \in \mathcal{R}$ са целобројним коефицијентима су нерастављиви над $\mathbb{Q}$.*

Укратко, када разматрамо полином из $\mathcal{R}$, треба очекивати да је он нерастављив над $\mathbb{Q}$. Стога је важно да имамо на располагању критеријуме за утврђивање његове нерастављивости.

Глава 7

Примене

У овој глави примењујемо метод реципрочне замене и наше критеријуме нерастављивости на проучавање класичних примера.

7.1 Обрасци факторизације Чебишевљевих полинома

Осврнимо се на својства факторизације Чебишевљевих полинома прве и друге врсте, T_n и U_n над $\mathbb{Q}$.
Чебишевљеви полиноми прве врсте n-тог степена, T_n, за $n \geq 0$, су дефинисани идентитетом

$$T_n(\cos\alpha) = \cos(n\alpha).$$

Уводећи смену $x = \cos\alpha$ добијамо експлицитну формулу за рачунање Чебишевљевих полинома прве врсте.

$$T_n(x) = \cos(n \arccos x), x \in [-1, 1].$$

Рекурзивна релација Чебишевљевих полинома прве врсте се добија на следећи начин. Будући да важи

$$\cos((n+1)\alpha) + \cos((n-1)\alpha) = \cos(n\alpha + \alpha) + \cos(n\alpha - \alpha)$$

$$= \cos(n\alpha)\cos(\alpha) - \sin(n\alpha)\sin(\alpha) + \cos(n\alpha)\cos(\alpha) + \sin(n\alpha)\sin(\alpha)$$

$$= 2\cos(n\alpha)\cos(\alpha)$$

и ако уведемо смену $\alpha = \arccos x$, тада добијамо

$$\cos((n+1)\arccos x) + \cos((n-1)\arccos x) = 2\cos(n\arccos x)\cos(\arccos x).$$

Претходни израз нам даје рекурзивну релацију

$$T_{n+1}(x) - 2xT_n(x) + T_{n-1}(x) = 0,$$

уз почетне услове $T_0(x) = 1$ и $T_1(x) = x$, односно

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x),$$

уз почетне услове $T_0(x) = 1, T_1(x) = x$.
Првих шест Чебишевљевих полинома прве врсте су:
$T_0(x) = 1$
$T_1(x) = x$
$T_2(x) = 2x^2 - 1$
$T_3(x) = 4x^3 - 3x$
$T_4(x) = 8x^4 - 8x^2 + 1$
$T_5(x) = 16x^5 - 20x^3 + 5x.$
Оно што је интересантно за Чебишевљеве полиноме прве врсте јесте да имају широку примену у математици, физици, инжењерству и рачунарству. Примена у математици је код апроксимације функција, што је корисно у нумеричкој анализи и анализи података, затим се користе у проучавању расподеле простих бројева, користе се и у квантној механици, посебно у опису осцилаторних стања, такође и код дигиталне обраде сигнала, пројектовању филтера и анализи спектра сигнала. Ово су само неке од многобројних примена Чебишевљевих полинома прве врсте.

Везу између реципрочне замене низа (3.1) и низа Чебишевљевих полинома прве врсте T_n можемо записати следећим идентитетом:

$$T_n(x) = \frac{1}{2} f_n(2x).$$

На основу идентитета одредимо $T_2(x)$, $T_3(x)$ и $T_4(x)$.
$T_2(x) = \frac{1}{2} f_2(2x) = \frac{1}{2}((2x)^2 - 2) = \frac{4x^2}{2} - 1 = 2x^2 - 1;$
$T_3(x) = \frac{1}{2} f_3(2x) = \frac{1}{2}((2x)^3 - 3(2x)) = \frac{8x^3}{2} - \frac{6x}{2} = 4x^3 - 3x;$
$T_4(x) = \frac{1}{2} f_4(2x) = \frac{1}{2}((2x)^4 - 4(2x)^2 + 2) = \frac{1}{2}(16x^4 - 16x^2 + 2) = 8x^4 - 8x + 1.$

Чебишевљеви полиноми друге врсте n-тог степена, U_n, за $n \geq 0$, су дефинисани идентитетом

$$U_n(x) = \frac{\sin((n+1)\arccos(x))}{\sin(\arccos(x))}, x \in (-1,1), n \in \mathbb{N}_0.$$

Да бисмо добили рекурзивну релацију Чебишевљевих полинома друге врсте крећемо од идентитета

$$\sin((n+1)\alpha) + \sin((n-1)\alpha) = 2\sin(n\alpha)\cos(\alpha).$$

Затим уводимо смену $\alpha = \arccos x$ и добијамо рекурзивну релацију за Чебишевљеве полиноме друге врсте

$$U_{n+1}(x) - 2xU_n(x) + U_{n-1}(x) = 0$$

уз почетне услове $U_0(x) = 1$ и $U_1(x) = 2x$, односно

$$U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$$

уз почетне услове $U_0(x) = 1$ и $U_1(x) = 2x$.

Првих шест Чебишевљевих полинома друге врсте су:
$U_0(x) = 1$
$U_1(x) = 2x$
$U_2(x) = 4x^2 - 1$
$U_3(x) = 8x^3 - 4x$
$U_4(x) = 16x^4 - 12x^2 + 1$
$U_5(x) = 32x^5 - 32x^3 + 6x$.
Реципрочна замена низа (3.1) је повезана са низом U_n следећим идентитетом:

$$U_{n-1}(x) = \frac{1}{2n} f_n'(2x),\ n \in \mathbb{N},$$

где је f_n' први извод функције f_n.

На основу идентитета можемо одредити $U_3(x)$.
Узмимо пети члан рекурзије (3.1) $f_4(x) = x^4 - 4x^2 + 2$. Први извод функције $f_4(2x)$ је $f_4'(2x) = 64x^3 - 32x$.
$\frac{1}{2\cdot 4} f_4'(2x) = \frac{1}{8}(64x^3 - 32x) = 8x^3 - 4x = U_3(x)$.
На овај начин, свако својство факторизације T_n и U_n над рационалним бројевима може се добити из функција f_n и f_n'.

Подсетимо се, из дефиниције реципрочног пресликавања $\mathbf{R}$ следи да је $f_n = \mathbf{R}(t^{2n}+1)$. Можемо записати први извод било ког члана низа f_n рекурзивно по n на следећи начин

$$f_n' = \begin{cases} n(f_1 + f_3 + ... + f_{n-1}) & n \quad \text{парно} \\ n(1 + f_2 + ... + f_{n-1}) & n \quad \text{непарно} \end{cases}$$

и отуда закључујемо да

$$f_n' = n\,\mathbf{R}(t^{2(n-1)} + t^{2(n-2)} + ... + t^2 + 1).$$

Полиноме $t^{2n}+1$ и $t^{2(n-1)} + t^{2(n-2)} + ... + t^2 + 1$ из $\mathbb{Q}[t]$ можемо записати као производ чији су фактори циклотомични полиноми парног степена:

$$t^{2n}+1 = \prod_{\substack{d|4n \\ d\nmid 2n}} \Phi_d \qquad t^{2(n-1)} + t^{2(n-2)} + ... + t^2 + 1 = \prod_{\substack{d|2n \\ d\neq 1,2}} \Phi_d.$$

Сада ћемо показати да су циклотомични полиноми $\Phi_n(x)$ нерастављиви над пољем рационалних бројева. Нека је θ примитивни n-ти корен из јединице, и нека је $f(t)$ моничан полином.

Лема 5. *Ако је p било који прост број такав да важи $(p,n)=1$, $n = \deg f$ и ако је α било који примитивни корен из јединице од $f(x)=0$, тада је α^p исто примитивни корен из јединице тог полинома.*

Доказ ове леме можемо наћи у Нивеновој књизи [14].

Теорема 13. *Циклотомични полиноми $\Phi_n(x)$ су нерастављиви над пољем рационалних бројева.*

Доказ. Нека је θ примитивни n-ти корен из јединице, и дефинишимо $f(x)$ као минимални полином од θ. (Више о минималним полиномима у примеру 7.2) Минимални полином $f(x)$ је дефинисан идентично као и $\Phi_n(x)$. $f(x)$ је нерастављив док год је минимални полином (доказ можемо наћи у Carus Monograph of Harry Pollard, The Theory of Algebraic Number, pp. 35-36). Било који примитивни n-ти корен из јединице је корен од $f(x)=0$, и одатле следи да је $f(x) = \Phi_n(x)$, што доказује теорему. Заиста било који примитивни n-ти корен из јединице се може записати као степен одређеног корена θ који је коришћен за дефинисање $f(x)$, θ^t где су t и n узајамно прости бројеви. Ако

је факторизација од t записана као производ (не нужно различитих) простих бројева $t = p_1 p_2 \cdots p_s$, тада $(p_i, n) = 1$ за свако индексно i. Тада на основу Леме 5, θ^{p_i} је корен од $f(x) = 0$, и итерацијом аргумената $\theta^{p_1 p_2}$ је корен полинома $f(x) = 0$, па индукцијом добијамо да је θ^t корен полинома $f(x) = 0$.

□

Конкретно, полиноми $t^{2n} + 1$ и $t^{2(n-1)} + t^{2(n-2)} + ... + t^2 + 1$ су производ фактора нерастављивих елемената у $\mathcal{R}$. Дакле, следи

$$f_n = \prod_{\substack{d|4n \\ d\nmid 2n}} \mathbf{R}(\Phi_d) \quad \text{и} \quad \frac{1}{n} f_n' = \prod_{\substack{d|2n \\ d\neq 1,2}} \mathbf{R}(\Phi_d) \tag{7.1}$$

су нерастављиве факторизације полинома f_n и f_n' над $\mathbb{Q}$. На основу ове чињенице могу се извести нека својства факторизације од f_n и f_n'.

Пример 17. *$t^m + 1$ је нерастављив над $\mathbb{Q}$ ако и само ако је m степена 2, одакле следи да је f_n нерастављив над $\mathbb{Q}$ ако и само ако је $n = 2^k, k \in \mathbb{N}$. Дакле, ово пружа још један доказ да је Чебишевљев полином прве врсте T_n нерастављив над $\mathbb{Q}$ ако и само ако је $n = 2^k$.*

Слично, закључујемо да Чебишевљев полином друге врсте U_{n-1} никада није нерастављив над $\mathbb{Q}$ за $n \geq 3$, пошто f_n' никада није нерастављиво над $\mathbb{Q}$ за $n \geq 3$.

7.2 Минимални полиноми тригонометријских функција $\cos(2\pi/n)$ и $\sin(2\pi/n)$

Алгебарски број је неки број који задовољава једначину облика

$$x^n + a_1 x^{n-1} + ... + a_n = 0,$$

са рационалним коефицијентима. За сваки алгебарски број a постоји јединствена полиномска једначина најмањег степена коју тај број задовољава. Полином који одређује ту једначину се назива минимални полином за a и његов степен се назива степен од a. Дакле, рационални бројеви се подударају са алгебарским бројевима степена 1. Такође, минимални полином од a је нерастављив над скупом $\mathbb{Q}$, и он је делилац било ког другог полинома са рационалним коефицијентима који имају a као нулу, и то је једини монични

полином који има ова својства. Доказе ових једноставних својстава о алгебарским бројевима можемо наћи у Carus Monograph of Hary Polland, The Theory of Algebraic Numbers, pp. 35-36.

Ако алгебарски број a задовољава једначину $x^n + a_1x^{n-1} + ... + a_n = 0$ са целобројним коефицијентима, кажемо да је a алгебарски цео број. На пример, од алгебарских бројева $\sqrt{3}$ и $\sqrt{3/2}$, само први број је алгебарски цео број. Минимални полином алгебарског целог броја је такође моничан полином. Ово се може доказати Гаусовом лемом 4.

Приметимо да су вредности тригонометријских функција алгебарски бројеви са аргументима који су рационални садржаоци броја π. Прво приметимо $\cos\alpha$ са $\alpha = 2\pi k/n$, где су k и n релативно прости цели бројеви. На основу Де Моаврове теореме имамо $(\cos\alpha + i\sin\alpha)^n = 1$. Записујући леву страну једначине биномном формулом, изједначавамо реалне делове да бисмо добили полиномску једначину по $\cos\alpha$ и $\sin\alpha$, при чему се ово последње односи само на парне степене. Када заменимо $\sin^2\alpha$ са $1 - \cos^2\alpha$, добићемо алгебарску једначину по $\cos\alpha$. Такође $\sin\alpha$ је алгебарски број, пошто $\sin\alpha = \cos(\alpha - \pi/2)$.

Означићемо са C_n и S_n минималне полиноме над $\mathbb{Q}$ бројева $2\cos(2\pi/n)$ и $2\sin(2\pi/n)$, редом.

Нека је $\xi_n := \cos(2\pi/n) + i\sin(2\pi/n)$ примитивни n-ти корен из јединице, који задовољава рационални полином степена $\varphi(n)$, где је $\varphi(n)$ Ојлерова функција и нека је циклотомични полином реда n, Φ_n његов минимални полином над $\mathbb{Q}$ дефинисан у Теореми 5. Тада $\Phi_9(x)$, на пример, може да се израчуна на следећи начин:

$x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x)$,

$x^3 - 1 = \Phi_1(x)\Phi_3(x)$,

па следи,

$$\Phi_9(x) = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1.$$

Сада посматрајмо реални и имагинарни део од ξ_n, редом $\cos(2\pi/n)$ и $\sin(2\pi/n)$. Оба дела су алгебарски бројеви, али да ли можемо да израчунамо њихове минималне полиноме? Један од начина је израчунавањем преко циклотомичних полинома. Представићемо идентитете, аналогне Теореми 5, за минималне полиноме $\Psi_n(x)$ полинома $\cos(2\pi/n)$, користећи Чебишевљеве полиноме $T_s(x)$, који су дефинисани са

$$T_s(\cos\alpha) = \cos(s\alpha),$$

за позитивно целобројно s и све реалне α. Степен $T_s(x)$ је s и водећи коефицијент је 2^{s-1}.

Теорема 14. *Нека је $\Psi_n(x)$ минимални полином полинома $\cos(2\pi/n)$ и нека је са $T_s(x)$ означен s-ти Чебишевљев полином.*
а) Ако је $n = 2s + 1$ непарно, тада важи

$$T_{s+1}(x) - T_s(x) = 2^s \prod_{d|n} \Psi_d(x), \tag{7.2}$$

и
б) ако је $n = 2s$ парно, тада важи

$$T_{s+1}(x) - T_{s-1}(x) = 2^s \prod_{d|n} \Psi_d(x). \tag{7.3}$$

Доказ ове теореме можемо наћи у чланку „A note on trigonometric algebraic numbers", Am. Math. Mon., 40, (1933) 165-166, америчког математичара Лехмера.

На пример, показаћемо како да израчунамо $\Psi_9(x)$ (минимални полином полинома $\cos(2\pi/9)$). Узећемо $s = 4$ и $s = 1$ и заменити у једнакост (7.2) да би добили

$$T_5(x) - T_4(x) = 16\Psi_1(x)\Psi_3(x)\Psi_9(x),$$

и

$$T_2(x) - T_1(x) = 2\Psi_1(x)\Psi_3(x).$$

Тада

$$8\Psi_9(x) = \frac{T_5(x) - T_4(x)}{T_2(x) - T_1(x)}.$$

Ова четири Чебишевљева полинома можемо израчунати. На пример,

$$\begin{aligned} T_5(\cos\alpha) &= \cos(5\alpha) \\ &= Re\left((\cos\alpha + i\sin\alpha)^5\right) \\ &= \cos^5\alpha - 10\cos^3\alpha\sin^2\alpha + 5\cos\alpha\sin^4\alpha \\ &= \cos^5\alpha - 10\cos^3\alpha(1-\cos^2\alpha) + 5\cos\alpha(1-\cos^2\alpha)^2 \\ &= 16\cos^5\alpha - 20\cos^3\alpha + 5\cos\alpha, \end{aligned}$$

па је

$$T_5(x) = 16x^5 - 20x^3 + 5x.$$

Слично,

$$T_4(x) = 8x^4 - 8x^2 + 1,$$

$$T_2(x) = 2x^2 - 1,$$

и

$$T_1(x) = x.$$

Следи

$$8\Psi_9(x) = \frac{T_5(x) - T_4(x)}{T_2(x) - T_1(x)} = 8x^3 - 6x + 1.$$

Из Тврђења 7, следи да је

$$C_n = \mathbf{R}(\Phi_n) \in \mathbb{Q}[x] \tag{7.4}$$

минимални полином над $\mathbb{Q}$ од $2\cos(2\pi/n)$ када је $n \geq 3$. Одавде следи да је минимални полином (до на умножак рационалним бројем различитим од нуле) полинома $\cos(2\pi/n)$ једнак $C_n(2x)$.

Пронаћи ћемо нерастављиви реципрочни полином који има корен $\sin(2\pi/n) + i\cos(2\pi/n)$. Дакле, S_n ће бити слика из $\mathbf{R}$ овог траженог полинома.

Размотримо комплексан број

$$i\bar{\xi} = \sin(2\pi/n) + i\cos(2\pi/n).$$

Пошто је $i\bar{\xi}$ примитивни корен из јединице за одговарајуће m, његов минимални полином над $\mathbb{Q}$ ће бити одређени циклотомични полином. Означимо са Ψ_n минимални полином над $\mathbb{Q}$ од $i\bar{\xi}$.

Тврђење 11. *Нека је n природан број. Минимални полином Ψ_n од $i\bar{\xi}$ се израчунава на следећи начин.*

1. *Ако је n непарно, онда је $\Psi_n = \Phi_{4n}$.*
2. *Ако је $n = 2m$ са непарним m, онда је $\Psi_n = \Phi_{2n}$.*
3. *Ако је $n = 4m$ са непарним $m \neq 1$, онда је $\Psi_n = \Phi_{\frac{n}{2}}$ и за $n = 4$, $\Psi_4 = \Phi_1$.*
4. *Ако је $n = 8m$ са непарним m, онда је $\Psi_n = \Phi_n$.*

Као последицу Тврђења 11 добијамо да је $S_n = \mathbf{R}(\Psi_n)$ минимални полином над $\mathbb{Q}$ од $2\sin(2\pi/n)$.

Тврђење 12. *Нека је n природан број. Тада се минимални полином S_n од $2\sin(2\pi/n)$ израчунава на следећи начин.*

1. *Ако је n непарно, тада је $S_n = \mathbf{R}(\Phi_{4n})$.*

2. *Ако је* $n = 2m$ *са непарним* m, *тада је* $S_n = \mathbf{R}(\Phi_{2n})$.

3. *Ако је* $n = 4m$ *са непарним* $m \neq 1$, *тада је* $S_n = \mathbf{R}(\Phi_{\frac{n}{2}})$ *и за* $n = 4$, $S_4 = \mathbf{R}(\Phi_1)$.

4. *Ако је* $n = 8m$ *са непарним* m, *тада је* $S_n = \mathbf{R}(\Phi_n)$.

Глава 8

Закључак

У овом раду смо намеравали да покажемо како би метода реципрочне замене могла да представља систематски начин проучавања проблема који укључују факторизацију реципрочних полинома над пољем рационалних бројева. Добили смо два критеријума нерастављивости, комбинаторно израчунавање броја елемената растављивих и нерастављивих реципрочних полинома, као и примере неких фамилија полинома.

Приметимо да би овај приступ могао да се користи код дизајнирања алгоритама за факторизацију реципрочних полинома. Колико нам је познато, време извршавања факторизације примитивних полинома $f \in \mathbb{Z}[t]$ степена n са ефикасним алгоритмом је реда $C(f) = n^u + n^v \log_2 ||f||_\infty$, где је $u \geq v+1 \geq 3$. Међутим, када је улаз реципрочни полином, ови алгоритми не користе ову чињеницу. Сада ћемо видети како би исписали алгоритам за факторизацију примитивних реципрочних полинома у $\mathcal{R}$.

1. Израчунати $\mathbf{R}(f)$ као производ матричног вектора.
2. Разложити примитивни полином $\mathbf{R}(f)$ степена n и $||\mathbf{R}(f)||_\infty \leq L_{n+2}B$ користећи стандардни алгоритам.
3. Добити нерастављиве целобројне факторе из $\mathcal{R}$ множењем са $\mathbf{R}_n^{-1}$.

Грубо говорећи, наведени алгоритам израчунава нерастављиве факторе у $\mathcal{R}$ са временским извршавањем алгоритма $n^u + n^v(\log_2 L_{n+2} + \log_2 B)$. Ова процедура тече асимптотски 2^u пута брже од директног факторисања f са стандардним алгоритмом. Обратимо пажњу да реципрочно пресликавамо полиноме степена n уместо $2n$.

Овај поступак прво даје нерастављиву факторизацију f у $\mathcal{R}$. Тако остаје да се утврди да ли нерастављиви реципрочни фактори полинома f припадају $\mathcal{R}_1$ или $\mathcal{R}_2$. Показали смо случај када они морају припадати $\mathcal{R}_1$. Следи, за већину полинома факторизације у $\mathcal{R}$ и $\mathbb{Z}[t]$ се поклапају.

Остаје отворена детаљна анализа временске сложености овог алгоритма у најгорем и просечном случају.

Библиографија

[1] Antonio Cafure and Eda Cesaratoo, *The American Mathematical Monthly*, Springer-Verlag, No1, January, 2017. 37-55.

[2] Милан А. Ковачевић, Градимир В. Миловановић, Радосав Ж. Ђорђевић, *Математика 1*, Свен, Ниш 2012.

[3] L. N. Childs, *A Concrete Introductio to Higher Algebra*, Springer-Verlag, 3rd ed., New York, 2009.

[4] Гојко Калајџић, *Алгебра*, Математички факултет, 2. издање, Београд, 2000.

[5] Александар Липковски, *Линеарна алгебра и аналитичка геометрија*, Завод за уџбенике, 1. издање, 2007.

[6] Yimin Ge, *Elementary Properties of Cyclotomic Polynomials* Mathematical Reflections 2, Vienna, Austria, 2008

[7] Градимир В. Миловановић, Милан А. Ковачевић, Миодраг М. Спалевић, *Нумеричка математика, Збирка решених проблема* Ниш/Крагујевац, 2002.

[8] William Watkins, Joel Zeitlin, *The Minimal Polynomial of* $\cos(2\pi/n)$ The American Mathematical Monthly, Vol. 100, No. 5 (May, 1993), pp. 471-474

[9] `https://pdfcoffee.com/qdownload/diskretna-matematika-2-predavanja-matf-pdf-fre`
`html`

[10] Michael Filaseta, Douglas B. Meade, *Irreducibility Testing of Lacunary 0, 1- Polynomials* Mathematics Department, University of South Carolina, Columbia SC 29208

[11] http://www.matf.bg.ac.rs/p/files/65-Ojlerova_funkcija.pdf

[12] Gerald Kuba, *On the distribution of reducible polynomials* Mathematica Slovaca 59 2009, 349-356

[13] https://ocw.mit.edu/courses/18-781-theory-of-numbers-spring-2012/7312c3e8e2dbb9af9a1677425fc3a0e7_MIT18_781S12_lec12.pdf

[14] Ivan Niven, *Irrational numbers* The Carus Mathematical Monographs, The Mathematical Association Of America, 1956.

Биографија аутора

Наташа Милошевић (*12.05.1988.*) је дипломирани професор математике и рачунарства Универзитета у Београду. Рођена је у Београду, општина Вождовац. Завршила основну школу „Јанко Веселиновић" након које је уписала VIII Београдску гимназију, природно-математички смер. Након завршетка гимназије, 2007. године, уписује Природно-математички факултет, Универзитет у Београду. Већ као апсолвент почиње да предаје у основној школи, и до сада има преко 10 година радног стажа. Године 2019. је била рецезент збирке из математике за 7. разред основне школе чији је издавач Герундијум. Тренутно ради у основној школи „Десанка Максимовић" у Београду.