(не)разложимост на полиноми с рационални коефициенти

Велико Дончев

Допълнителен материал за студентите по Висша алгебра и Алгебра 2 на ФМИ

1 Предварителни сведения и твърдения

Както е ясно от основната теорема на Алгебрата и нейните следствия [1, гл. III, §17], всеки полином с реални (или комплексни) коефициенти от степен n има точно n (комплексни) корена, броени с техните кратности. Тъй като за всеки реален полином $f \in \mathbb{R}[x]$ ако числото $a \in \mathbb{C}\backslash\mathbb{R}$ е корен на f, то и комплексно спрегнатото му $\overline{a}$ е корен (на f) и

$$\mathbb{R}[x] \ni x^2 - (a + \overline{a})x + a\overline{a} \mid f,$$

тоест f се разлага **над** $\mathbb{R}$ в произведение на линейни и/или квадратни полиноми. За $f \in \mathbb{C}[x]$ ситуацията е "по-проста": f се разлага на линейни полиноми над $\mathbb{C}$ (друг е въпросът как се намират !).

Когато става въпрос за (не)разложимост на полиноми $f \in \mathbb{Q}[x]$, ситуацията коренно се променя. Съществуват неразложими полономи за всяка степен n. Освен някои отделни резултати (като критерия на Айзенщайн) в общия случай не съществува критерии дали даден полином $f \in \mathbb{Q}[x]$ е разложим или не над $\mathbb{Q}$.

Твърдение 1.1. *Разложимостта на* $f \in \mathbb{Q}[x]$ **над** $\mathbb{Q}$ *се свежда до разложимост на целочислен полином* **над** $\mathbb{Q}$

Наистина, нека $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Q}[x]$ и q е *най-големият общ знаменател* на коефициентите. Тогава

$$f = \frac{1}{q}g,$$

където $g \in \mathbb{Z}[x]$ и f и g са еднакво (не)разложими над $\mathbb{Q}$.

Пример 1. $f = \frac{1}{2} + \frac{2}{3}x + x^2 = \frac{1}{6}(3 + 4x + 6x^2)$

Дефиниция 1.1. *Нека* $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Q}[x]$. *Казваме, че* f *е примитивен, ако НОД*$(a_0, \ldots, a_n) = 1$.

Всеки рационален полином може да се представи като произведение на рационално число и примитивен полином. Наистина, нека $f \in \mathbb{Q}[x]$ и q е *най-големият общ знаменател*

на коефициентите. Тогава $f = \frac{1}{q}g$ и $g \in \mathbb{Z}[x]$. Да изнесем сега НОД-а d на коефициентите на g. Получаваме

$$f = \frac{d}{q}r,$$

където $r \in \mathbb{Z}[x]$ е примитивен.

Пример 2. $f = \frac{2}{7} + \frac{2}{3}x + 4x^2 = \frac{1}{21}(6 + 14x + 84x^2) = \frac{2}{21}(3 + 7x + 42x^2)$

Твърдение 1.2. *Нека f е примитивен и $c \in \mathbb{Q}$ и $ch \in \mathbb{Z}[x]$. Тогава $c \in \mathbb{Z}$.*

Твърдение 1.3. *(Лема на Гаус) Нека f и g са примитивни. Тогава fg е примитивен.*

Следствие: Ако $f \in \mathbb{Z}[x]$ е разложим над $\mathbb{Q}$, то той е разложим и над $\mathbb{Z}$. Наистина, нека $f = f_1 f_2$ е разлагане на $f \in \mathbb{Q}[x]$ над $\mathbb{Q}$. Тогава представяме $f_i = \frac{d_i}{q_i} r_i, i = 1, 2$, където r_1, r_2 са примитивни. Следователно

$$f = f_1 f_2 = \left(\frac{d_1}{q_1}\frac{d_2}{q_2}\right)(r_1 r_2),$$

където $r_1 r_2$ е примитивен (Лема Гаус), $q = \frac{d_1 d_2}{q_1 q_2} \in \mathbb{Q}$ и от 1.2 следва, че $q \in \mathbb{Z}$. Тогава

$$f = (qf_1)f_2$$

е разлагане на f над $\mathbb{Z}$.

2 Някои методи

Твърдение 2.1. *Нека p е просто число и $\pi_p : \mathbb{Z} \to \mathbb{Z}_p$ е естественият хомоморфизъм от $\mathbb{Z}$ върху $\mathbb{Z}_p$. Този хомоморфизъм* **индуцира** *хомоморфизъм, $\varphi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ действащ по следния начин:*

$$\varphi_p(a_0 + a_1 x + \ldots + a_n x^n) = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n.$$

Работно следствие: Нека $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x], p \nmid a_n$. Тогава ако f е разложим над $\mathbb{Z}$, то $\overline{f} = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n$ е от степен n и е разложим над $\mathbb{Z}_p$. Всъщност ползваме твърдението във формата:

Нека $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x], p \nmid a_n$. Тогава ако $\overline{f}$ е неразложим над $\mathbb{Z}_p$, то f е неразложим **и над** $\mathbb{Z}$.

Пример 3. *Да се докаже, че $f = x^3 + 20x^2 + 6x + 11$ е неразложим над $\mathbb{Q}$.*

Решение. *Да разгледаме образа на f под действие на хомоморфизма φ за простото число $p = 5$. Получаваме*

$$\varphi_5(f) = x^3 + x + \overline{1}.$$

Понеже полиномът $\overline{f}$ е от трета степен, то ако се разлага над $\mathbb{Z}_5$, то в разлагането му има поне един линеен полином. Следователно $\overline{f}$ трябва да има корен в $\mathbb{Z}_5$. Но $\overline{f}(\overline{0}) = \overline{1}, \overline{f}(\overline{1}) = \overline{3}, \overline{f}(\overline{2}) = \overline{11} = \overline{1}, \overline{f}(\overline{3}) = \overline{31} = \overline{1}, \overline{f}(\overline{4}) = \overline{69} = \overline{4}$. Следователно $\overline{f}$ няма корен в $\mathbb{Z}_5$, следователно е неразложим над $\mathbb{Z}_5$, следователно е неразложим над $\mathbb{Z}$, следователно е неразложим над $\mathbb{Q}$.

Забележка: Няма рецепта кое просто число да се "препоръча" при използване на този метод. Въпреки това, често той е успешно приложим. Неразложимостта над крайно поле $\mathbb{Z}_p$ се свежда до нерешимост на система алгебрични уранения над крайно поле. На теория това е много по-лесно, т.к. нерешимосттада може да се установи с краен брой проверки (виж "brute force" метода в края).

Забележка: Ако $\overline{f}$ е разложим над $\mathbb{Z}_p$, това не означава задължително, че f е разложим над $\mathbb{Z}$. Например $f = x^2 + x + 1$, е неразложим над $\mathbb{Q}$ (проверете!), но ако разгледаме $\varphi_3(f) = \overline{f}$ за $p = 3$ ще получим, че

$$\varphi_3(f) = \overline{f} = x^2 + x + \overline{1} = (\overline{2}x + 1)^2,$$

т.е. $\overline{f}$ е разложим над $\mathbb{Z}_3$.

Твърдение 2.2. *(Критерий на Айзенщайн) Нека $f = a_0 + a_1x + \ldots + a_nx^n, a_n \neq 0$ целочислен полином. Нека p е такова просто число, че*

- $p \nmid a_n$,
- $p \mid a_0, a_1, \ldots, a_n$,
- $p^2 \nmid a_0$.

Тогава f е неразложим над $\mathbb{Z}$ (а следователно и над $\mathbb{Q}$).

Пример 4. *[2, зад. 9.12а)] Да се докаже, че полиномът $f = 2x^5 - 21x^2 + 42x + 63$ е неразложим над $\mathbb{Q}$.*

Решение. *Прилагаме критерия на Айзенщайн за $p = 7$. Забележете, че не можем да приложим критерия за $p = 3$.*

Пример 5. *Да се докаже, че полиномът $f = x^n + 2$ е неразложим над $\mathbb{Q}$ за всяко $n > 1$.*

Решение. *Прилагаме критерия на Айзенщайн за $p = 2$. Така излиза, че над $\mathbb{Q}$ има неразложими полиноми от произволна степен.*

Често критерия на Айзенщайн не е директно приложим. В помощ понякога идва следното

Твърдение 2.3. *Нека $f \in \mathbb{Q}[x]$ и $a, b \in \mathbb{Q}, a \neq 0$. Тогава полиномите $f(x)$ и $f(ax + b)$ са едновременно (не)разложими. Еквивалентно е да кажем, че (не)разложимостта на полиноми над $\mathbb{Q}$ е* **инвариантна** *относно* **линейна** *смяна на променливата.*

Пример 6. *[2, зад. 9.12в)] Да се докаже, че полиномът $f = x^4 - 8x^3 + 21x^2 - 11x - 11$ е неразложим над $\mathbb{Q}$.*

Решение. *Да разгледаме полинома $g = f(x + 2) = 3 + 9x - 3x^2 + x^4$. За него прилагаме критерия на Айзенщайн за $p = 2$ и заключваме, че g, а следователно и f са неразложими над $\mathbb{Q}$.*

Забележка: И тук отново няма универсална рецепта как да се сетим каква смяна да направим.

Забележка: За генерализации на критерия на Айзенщайн виж [2, зад. 9.10]

Още един важен инструмент при разложимостта на рационални полиноми е

Твърдение 2.4. *Нека $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$. Тогава ако $\frac{b}{c} \in \mathbb{Q}, (b,c) = 1$ е корен на f, то $b|a_0, c|a_n$. Това училищно твърдение е работно, т.к. всъщст казва, че имаме само "краен брой" канидати за корени.*

Пример 7. *Да се намерят (ако има такива) рационалните корени на полинома $f = x^{100} - x^{50} - x^{24} - x^{14} - x^{12} - x^8 - x^6 + 1$*

Решение. *Според критерия единствените възможни корени са ± 1. Директно се вижда, че и двете са корени.*

Последният ("brute force") метод, който ще изложим свежда хипотезата за разложимост на рационален полином към множество от (в общия случай нелинейни) системи над $\mathbb{Q}$. Същността му се състои в следното: Нека $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Q}[x], a_n \neq 0, n > 1$ и предполагаме, че

$$f = (b_0 + \ldots b_mx^m)(c_0 + \ldots + c_qx^q), b_mc_q \neq 0, m + q = n.$$

Използвайки метода за сравняване на коефициентите съставяме система с $n+1$ (нелинейни) уравнения за $(m+1)(q+1)$ неизвестни. Същият алгоритъм може да се приложи и при разложимост над крайно поле $\mathbb{Z}_p$.

Пример 8. *Разгледайте решението на зад. 9.5в) от [2].*

Пример 9. */От писмен изпит по Алгебра 2, спец. Компютърни науки от 07.07.2014г./ Да се докаже, че полиномът*

$$f = x^5 + 3x^4 + 5x^3 + x^2 + 6x + 5$$

е неразложим над всяко от полетата $\mathbb{Z}_2$ и $\mathbb{Q}$.

Решение. *От работното следствие на редукционния критерий, ако докажем, че $\varphi_2(f) = \overline{f}$ е неразложим над $\mathbb{Z}_2$, то от тук ще следва, че той е неразложим и над $\mathbb{Q}$. Пресмятаме*

$$\varphi_2(f) = \overline{f} = x^5 + x^4 + x^3 + x^2 + \overline{1}.$$

Да допуснем, че $\overline{f}$ е разложим над $\mathbb{Z}_2$. Тъй като степента на $\overline{f}$ е 5, то той се разлага или като произведение на полиноми от 1 и 4 степени, или като произведение на полиноми от 2 и 3 степени. Веднага се вижда, че $\overline{f}(\overline{0}) = f(\overline{1}) = \overline{1}$ и следователно $\overline{f}$ няма корен в $\mathbb{Z}_2$, т.е. не е възможно в разлагането му да има линеен полином. Нека сега допуснем, че $\overline{f}$ се разлага в произведение на полином от 2 и полином от 3 степен.

$$\overline{f} = (x^3 + ax^2 + bx + c)(x^2 + dx + e), \qquad a, b, c, d, e \in \mathbb{Z}_2.$$

Да забележим, че коефициентите старшите коефициенти на двата полинома в разлагането са $\overline{1}$ (тъй като иначе биха били $\overline{0}$, а тогава полиномите не биха със степени 2 и 3). Разкривайки скобите и събирайки подобните едночлени в последното равенство получаваме

$$x^5 + x^4 + x^3 + x^2 + \overline{1} = x^5 + (a+d)x^4 + (ae + bd + c)x^2 + (be + cd)x + ce.$$

Приравнявайки свободните коефициенти получаваме $ce = \overline{1}$ от където като единствената възможност имаме $c = e = \overline{1}$. Приравнявайки коефициентите пред x получаваме, че $b + d = \overline{0}$, т.е. имаме 2 случая:

1 сл. $b = \overline{1}, d = \overline{1}$. *В този случай от* $a+d = \overline{1}$ *веднага получаваме* $a = \overline{0}$. *Сега замествайки* a, e, b, d, c *в* $ae + bd + c = \overline{1}$ *получаваме* $\overline{0} + \overline{1} + \overline{1} = \overline{1}$, *което е противоречие.*

2 сл. $b = \overline{0}, d = \overline{0}$. *В този случай от* $a + d = \overline{1}$ *веднага получаваме* $a = \overline{1}$. *Отново замествайки* a, e, b, d, c *в* $ae + bd + c = \overline{1}$ *получаваме* $\overline{1} + \overline{0} + \overline{1} = \overline{1}$, *което е противоречие.*

Следователно $\overline{f}$ *е неразложим над* $\mathbb{Z}_2$, *от където следва, че е неразложим и над* $\mathbb{Q}$.

Задачи за упражнение от [2]:

- **9.4-9.5**
- **9.12-9.14**
- **9.15-9.16**

Литература

[1] Пламен Сидеров, Керопе Чакърян *Записки по алгебра: Групи, пръстени, полиноми*, 2013, Веди

[2] Асен Божилов, Пламен Сидеров, Керопе Чакърян *Задачи по алгебра: Групи, пръстени, полиноми*, 2013, Веди