

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Б.В. Довгай

Комплексні числа та многочлени

Навчальний посібник

Факультет комп'ютерних наук та кібернетики

Київ

2023

ЗМІСТ

Розділ 1. Комплексні числа	4
1. Еволюція поняття числа	4
2. Комплексні числа	5
3. Дії над комплексними числами	5
4. Геометричний зміст комплексного числа	6
5. Тригонометрична форма комплексного числа	6
6. Множення комплексних чисел в тригонометричній формі .	7
7. Ділення комплексних чисел в тригонометричній формі . .	7
8. Формула Муавра	8
9. Корені з комплексних чисел	9
10. Корені з одиниці	10
11. Примітивні корені з одиниці	11
Розділ 2. Многочлени	13
1. Числові поля	13
2. Многочлени над числовими полями	15
3. Теорія ділення многочленів	15
4. Алгоритм Евкліда	17
5. Теорема про НСД	17
6. Теорема Безу	20
7. Схема Горнера та її застосування	20
8. Незвідні многочлени та основна теорема про подільність многочлена	21
9. Лема про похідну	24
10. Відокремлення кратних множників	25
11. Кратність коренів многочлена	27
12. Рівність многочленів	27

13.	Незвідні многочлени над полем комплексних чисел	28
14.	Незвідні многочлени над полем дійсних чисел	29
14.1.	Розклад многочлена з дійсними коефіцієнтами в добуток незвідних множників	32
15.	Звідні многочлени над полем \mathbb{Q} раціональних чисел	32
16.	Примітивні многочлени	35
17.	Ознака Ейзенштейна	36
18.	Границі дійсних коренів дійсних многочленів	38
19.	Число дійсних коренів дійсного многочлена на дійсному проміжку (теорема Штурма)	39
19.1.	Поняття знаковміни в системі дійсних чисел	40
19.2.	Система функцій Штурма	40
19.3.	Існування системи функцій Штурма	41
19.4.	Теорема Штурма	42
20.	Інтерполяційні многочлени	45

Розділ 1

Комплексні числа

1. Еволюція поняття числа

В основі всіх числових множин лежить натуральний ряд $1, 2, 3, \dots$ який позначається через \mathbb{N} . Елементи натурального ряду відображають найпростіші кількісні відношення.

Розглянемо рівняння $a+x = b$, $a, b \in \mathbb{N}$. Це рівняння не має розв'язків в натуральних числах при $a \geq b$, а тому, для отримання розв'язків цього рівняння при $\forall a, b \in \mathbb{N}$, були введені 0 і від'ємні числа, які разом з \mathbb{N} утворили \mathbb{Z} — цілі числа. Причому в цій множині рівняння $a + x = b$ має розв'язок при $\forall a, b \in \mathbb{Z}$.

Розглянемо інше рівняння $ax = b$, $a, b \in \mathbb{Z}$, $a \neq 0$. Це рівняння не має розв'язків в \mathbb{Z} , якщо b не ділиться на a . Тому, щоб отримати розв'язки при $\forall a, b \in \mathbb{Z}$, $a \neq 0$, були введені раціональні числа \mathbb{Q} .

Розглянемо квадрат, сторона якого $= 1$ і діагональ $= \sqrt{2}$. Покажемо, що $\sqrt{2}$ не є раціональним числом. Припустимо, супротивне $\sqrt{2} = \frac{p}{q}$, $p, q \in \mathbb{Z}$, p, q взаємно прості. Тоді $2 = \frac{p^2}{q^2}$, $p^2 = 2q^2 \implies 2|p^2 \implies 2|p \implies p = 2c$, $c \in \mathbb{Z}$. $2q^2 = 4c^2$, $q^2 = 2c^2$, $2|q^2 \implies 2|q$, таким чином числа p і q мають спільний дільник 2 , що суперечить умові.

Для того, щоб отримувати довжини відрізків в таких випадках було введено розширення \mathbb{Q} — множина дійсних чисел \mathbb{R} .

Кожне дійсне нераціональне число можна записати у вигляді нескінченного неперіодичного десяткового дробу. Наприклад, $n < z < n + 1$, $n \in \mathbb{Z}$. На числовій прямій відрізок $[n, n + 1]$ ділимо на 10 рівних частин і за a_1 беремо число, яке на 1 менше за номер відрізка, на якому знаходиться число z . Аналогічно цей відрізок ділимо на 10 рівних частин і за a_2 беремо число, яке на 1 менше за номер відрізка, на якому знаходиться число z і т.д. Отримаємо $\mathbb{Z} = n, a_1 a_2 a_3 \dots$

Розглянемо рівняння $x^2 = c$, $c \in \mathbb{R}$. Це рівняння має розв'язки в \mathbb{R} тільки якщо $c \geq 0$. Щоб одержати розв'язки цього рівняння при $\forall c$ треба ввести розширення \mathbb{R} , а саме комплексні числа \mathbb{C} . У цій множині рівняння $x^2 = c$ має розв'язки при $\forall c \in \mathbb{C}$. Якщо $f(x)$ — деякий многочлен, коефіцієнти якого є комплексними числами, то рівняння $f(x) = 0$ завжди має корінь з множини \mathbb{C} . В цьому полягає основна теорема алгебри.

2. Комплексні числа

Беремо рівняння $x^2 = -1$, це рівняння має розв'язок в множині \mathbb{C} , цей розв'язок позначимо через i . Тоді $i^2 = -1$. Множина \mathbb{C} є розширенням множини \mathbb{R} , тому $\mathbb{R} \subseteq \mathbb{C}$, $i \in \mathbb{C}$. Для елементів множини \mathbb{C} треба ввести арифметичні операції. $bi \in \mathbb{C}$, $\forall b \in \mathbb{R}$, $a + bi \in \mathbb{C}$, $\forall a, b \in \mathbb{R}$, тобто всі числа $a + bi$ складають множину \mathbb{C} .

Означення 1. Комплексним числом називається число вигляду $z = a + bi$, де $a, b \in \mathbb{R}$, а i — новий символ.

Якщо $z = a + bi$, то a називають дійсною частиною числа z , а b — уявною частиною. Якщо $b = 0$, отримуємо $z = a \in \mathbb{R}$, якщо $a = 0$, то число $z = bi$ називається чисто уявним.

Два комплексні числа $z_1 = a_1 + b_1i$ і $z_2 = a_2 + b_2i$ вважають рівними, якщо рівні їхні дійсні і уявні частини $a_1 = a_2$, $b_1 = b_2$.

Нехай $z = a + bi$, тоді комплексно спряженим для нього називається число $\bar{z} = a - bi$. Зрозуміло, що $\bar{\bar{z}} = z$, $z + \bar{z} \in \mathbb{R}$, $z - \bar{z}$ — чисто уявне.

3. Дії над комплексними числами

Введемо арифметичні операції на множині \mathbb{C} :

1) додавання: під сумою двох чисел $z_1 = a_1 + b_1i$ і $z_2 = a_2 + b_2i$ будемо розуміти $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i$;

2) віднімання: під різницею двох чисел $z_1 = a_1 + b_1i$ і $z_2 = a_2 + b_2i$ розуміємо число $z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)i$;

3) множення: під добутком двох чисел $z_1 = a_1 + b_1 i$ і $z_2 = a_2 + b_2 i$ будемо розуміти $z_1 z_2 = (a_1 + b_1 i)(a_2 + b_2 i) = a_1 a_2 + a_1 b_2 i + a_2 b_1 i + b_1 b_2 i^2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i$;

4) ділення: під часткою двох чисел $z_1 = a_1 + b_1 i$ і $z_2 = a_2 + b_2 i$, $z_2 \neq 0$ будемо розуміти $\frac{z_1}{z_2} = \frac{a_1 + b_1 i}{a_2 + b_2 i}$. Домножимо чисельник і знаменник на число комплексно спряжене до знаменника

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{(a_1 + b_1 i)(a_2 - b_2 i)}{(a_2 + b_2 i)(a_2 - b_2 i)} = \frac{(a_1 a_2 + b_1 b_2) + (a_1 b_2 - a_2 b_1) i}{a_2^2 - (b_2 i)^2} \\ &= \frac{(a_1 a_2 + b_1 b_2) + (a_1 b_2 - a_2 b_1) i}{a_2^2 + b_2^2} = \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + \frac{a_1 b_2 - a_2 b_1}{a_2^2 + b_2^2} i. \end{aligned}$$

4. Геометричний зміст комплексного числа

Як відомо, дійсні числа можна зобразити точками на прямій. Візьмемо на площині декартову прямокутну систему координат і кожному комплексному числу $z = a + bi$ поставимо у відповідність точку $A(a, b)$. Таким чином отримаємо взаємнооднозначну відповідність між комплексними числами і точками на площині.

З іншого боку, з кожною точкою на площині зв'язаний вектор $\overline{OA} = \{a, b\}$. Тому, з іншого боку, встановлено взаємно однозначну відповідність між комплексними числами і векторами на площині. Якщо $z_1 \rightarrow \overline{OA}$, а $z_2 \rightarrow \overline{OB}$, то $z_1 \pm z_2 \rightarrow \overline{OA} \pm \overline{OB}$, тобто додаванню і відніманню комплексних чисел відповідає додавання і віднімання векторів.

5. Тригонометрична форма комплексного числа

Кожному $x \in \mathbb{C}$ відповідає вектор на площині, а кожен ненульовий вектор задається довжиною і напрямком.

Напрямок вектора \overline{OA} можна задати, якщо задати кут, який цей вектор утворює з додатнім напрямом осі Ox . При цьому домовимось, що всі кути відраховуються від осі Ox проти годинникової стрілки.

Нехай $\overline{OA} = \{a, b\}$ відповідає $z = a + bi$. Позначимо через r довжину \overline{OA} , а через α кут, який цей вектор утворює з додатнім напрямом осі Ox . $r = \sqrt{a^2 + b^2}$, $a = r \cos \alpha$, $b = r \sin \alpha$, $z = r \cos \alpha + r \sin \alpha i =$

$r(\cos \alpha + i \sin \alpha)$ — це тригонометрична форма $z \in \mathbb{C}$. r називається модулем комплексного числа і позначається $|z|$, α називається аргументом комплексного числа і позначається $\arg(z)$. Якщо $z = 0$, то $|z| = 0$, $\arg(z)$ просто не визначається.

Нехай $z = a + bi = r(\cos \alpha + i \sin \alpha)$. Тоді $\bar{z} = a - bi = r(\cos \alpha - i \sin \alpha) = r(\cos(-\alpha) + i \sin(-\alpha))$.

Для даного комплексного числа z модуль визначається однозначно, а $\arg z$ точністю до періоду 2π . Таким чином 2 комплексних числа в тригонометричній формі вважаються рівними, якщо їхні модулі рівні, а \arg відрізняються на число кратне 2π .

6. Множення комплексних чисел в тригонометричній формі

Нехай $z_1 = r_1(\cos \alpha_1 + i \sin \alpha_1)$, $z_2 = r_2(\cos \alpha_2 + i \sin \alpha_2)$. Тоді $z_1 z_2 = r_1 r_2 (\cos \alpha_1 \cos \alpha_2 + i \cos \alpha_1 \sin \alpha_2 + i \sin \alpha_1 \cos \alpha_2 + i^2 \sin \alpha_1 \sin \alpha_2) = r_1 r_2 ((\cos \alpha_1 \cos \alpha_2 - \sin \alpha_1 \sin \alpha_2) + i(\cos \alpha_1 \sin \alpha_2 + \sin \alpha_1 \cos \alpha_2)) = r_1 r_2 (\cos(\alpha_1 + \alpha_2) + i \sin(\alpha_1 + \alpha_2))$.

Таким чином, щоб перемножити 2 числа в тригонометричній формі, треба їхні модулі перемножити, а аргументи додати.

Наприклад, $z = r(\cos \alpha + i \sin \alpha)$, $\bar{z} = r(\cos(-\alpha) + i \sin(-\alpha))$. $z \bar{z} = r^2(\cos(\alpha - \alpha) + i \sin(\alpha - \alpha)) = r^2$

7. Ділення комплексних чисел в тригонометричній формі

Нехай дано $z_1 = r_1(\cos \alpha_1 + i \sin \alpha_1)$, $z_2 = r_2(\cos \alpha_2 + i \sin \alpha_2)$, $z_2 \neq 0 \implies r_2 \neq 0$. Тоді $\frac{z_1}{z_2} = \frac{r_1(\cos \alpha_1 + i \sin \alpha_1)}{r_2(\cos \alpha_2 + i \sin \alpha_2)} \implies$ за правилом треба домножити чисельник і знаменник на число, комплексно-спряжене знаменнику \implies

$$\frac{z_1}{z_2} = \frac{r_1(\cos \alpha_1 + i \sin \alpha_1)r_2(\cos(-\alpha_2) + i \sin(-\alpha_2))}{r_2(\cos \alpha_2 + i \sin \alpha_2)r_2(\cos(-\alpha_2) + i \sin(-\alpha_2))} =$$

$$\frac{r_1 r_2 (\cos(\alpha_1 - \alpha_2) + i \sin(\alpha_1 - \alpha_2))}{r_2^2 (\cos 0 + i \sin 0)} = \frac{r_1}{r_2} (\cos(\alpha_1 - \alpha_2) + i \sin(\alpha_1 - \alpha_2)).$$

Таким чином, щоб поділити два числа в тригонометричній формі, потрібно їх модулі поділити і від аргументу чисельника відняти аргумент знаменника.

8. Формула Муавра

Нехай дано комплексне число $z = r(\cos \alpha + i \sin \alpha)$ і його треба піднести в натуральний степінь n . За правилом множення комплексних чисел одержимо $z^n = (r(\cos \alpha + i \sin \alpha))^n = r^n(\cos n\alpha + i \sin n\alpha)$, зокрема якщо $|z| = r = 1$ то $z^n = (\cos \alpha + i \sin \alpha)^n = \cos n\alpha + i \sin n\alpha$.

Доведемо, що формула вірна при піднесенні в будь-який цілий степінь n .

Припустимо, що $n \in \mathbb{N}$ і піднесемо $z = r(\cos \alpha + i \sin \alpha)$ в степінь $-n$, ($z \neq 0$), $z^{-n} = \frac{1}{z^n} = \frac{1}{r^n(\cos n\alpha + i \sin n\alpha)}$. Запишемо 1 в тригонометричній формі $1 = \cos 0 + i \sin 0$, тоді

$$z^{-n} = \frac{\cos 0 + i \sin 0}{r^n(\cos n\alpha + i \sin n\alpha)} = \frac{1}{r^n} (\cos(0 - n\alpha) + i \sin(0 - n\alpha))$$

$$= r^{-n} (\cos(-n\alpha) + i \sin(-n\alpha)).$$

Приклад 1 (застосування формули Муавра). Припустимо, стоїть задача виразити $\cos n\alpha, \sin n\alpha$ через $\cos \alpha, \sin \alpha$. Розглянемо комплексне число $z = (\cos \alpha + i \sin \alpha)$, тоді за формулою $z^n = (\cos n\alpha + i \sin n\alpha)$, з іншого боку, за формулою бінома Ньютона

$$\begin{aligned} z^n &= (\cos \alpha + i \sin \alpha)^n = \cos^n \alpha + C_n^1 \cos^{n-1} \alpha (i \sin \alpha) + \\ &+ C_n^2 \cos^{n-2} \alpha (i \sin \alpha)^2 + C_n^3 \cos^{n-3} \alpha (i \sin \alpha)^3 + \dots + (i \sin \alpha)^n \\ &= \cos^n \alpha + i(C_n^1 \cos^{n-1} \alpha \sin \alpha) - \\ &- C_n^2 \cos^{n-2} \alpha \sin^2 \alpha - i(C_n^3 \cos^{n-3} \alpha \sin^3 \alpha) + \dots + (i)^n \sin^n \alpha \end{aligned}$$

і порівнюємо дійсні та уявні частини:

$$\begin{aligned} \cos n\alpha &= \cos^n \alpha - C_n^2 \cos^{n-2} \alpha \sin^2 \alpha + C_n^4 \cos^{n-4} \alpha \sin^4 \alpha - \dots, \\ \sin n\alpha &= C_n^1 \cos^{n-1} \alpha \sin \alpha - C_n^3 \cos^{n-3} \alpha \sin^3 \alpha + C_n^5 \cos^{n-5} \alpha \sin^5 \alpha - \dots \end{aligned}$$

9. Корені з комплексних чисел

Припустимо зафіксоване деяке комплексне число c . Знайдемо всі корені степеня $n \in \mathbb{N}$ з числа c , якщо вони існують; запишемо c в тригонометричній формі $c = r(\cos \alpha + i \sin \alpha)$ і припустимо що комплексне число z є коренем n -го степеня з числа c (тобто $z^n = c$). Запишемо число z в тригонометричній формі $z = \rho(\cos \beta + i \sin \beta)$, тоді за формулою Муавра $\rho^n(\cos n\beta + i \sin n\beta) = r(\cos \alpha + i \sin \alpha)$, прирівнюємо модулі $\rho^n = r \implies \rho = \sqrt[n]{r}$ тобто модуль числа z визначається однозначно. Виконується $\cos n\beta = \cos \alpha, \sin n\beta = \sin \alpha$, звідки $n\beta = \alpha + 2\pi k, k \in \mathbb{Z}$, а тому $\beta = \frac{\alpha + 2k\pi}{n}, k \in \mathbb{Z}$.

$$\text{Беремо } k = 0, \beta = \frac{\alpha}{n}, z_0 = \sqrt[n]{r}(\cos \frac{\alpha}{n} + i \sin \frac{\alpha}{n});$$

$$k = 1, z_1 = \sqrt[n]{r}(\cos \frac{\alpha + 2\pi}{n} + i \sin \frac{\alpha + 2\pi}{n});$$

$$k = 2, z_2 = \sqrt[n]{r}(\cos \frac{\alpha + 4\pi}{n} + i \sin \frac{\alpha + 4\pi}{n}); \dots$$

$$k = n - 1, z_{n-1} = \sqrt[n]{r}(\cos \frac{\alpha + 2(n-1)\pi}{n} + i \sin \frac{\alpha + 2(n-1)\pi}{n});$$

$$\begin{aligned} k = n, z_n &= \sqrt[n]{r}(\cos \frac{\alpha + 2n\pi}{n} + i \sin \frac{\alpha + 2n\pi}{n}) \\ &= \sqrt[n]{r}(\cos(\frac{\alpha}{n} + 2\pi) + i \sin(\frac{\alpha}{n} + 2\pi)) = \sqrt[n]{r}(\cos \frac{\alpha}{n} + i \sin \frac{\alpha}{n}) = z_0; \end{aligned}$$

$$\begin{aligned} k = n + 1, z_{n+1} &= \sqrt[n]{r}(\cos \frac{\alpha + 2(n+1)\pi}{n} + i \sin \frac{\alpha + 2(n+1)\pi}{n}) \\ &= \sqrt[n]{r}(\cos(\frac{\alpha + 2\pi}{n} + 2\pi) + i \sin(\frac{\alpha + 2\pi}{n} + 2\pi)) \\ &= \sqrt[n]{r}(\cos \frac{\alpha + 2\pi}{n} + i \sin \frac{\alpha + 2\pi}{n}) = z_1. \end{aligned}$$

Покажемо, що для будь-якого k число $z_k = \sqrt[n]{r}(\cos \frac{\alpha + 2\pi k}{n} + i \sin \frac{\alpha + 2\pi k}{n})$ співпадає з одним з чисел z_0, z_1, \dots, z_{n-1} . Поділимо число k на n з залишком: $k = ln + q$, де $l, q \in \mathbb{Z}, 0 \leq q < n$, тоді

$$\begin{aligned} z_k &= \sqrt[n]{r}(\cos \frac{\alpha + 2(ln + q)\pi}{n} + i \sin \frac{\alpha + 2(ln + q)\pi}{n}) \\ &= \sqrt[n]{r}(\cos(\frac{\alpha + 2q\pi}{n} + 2l\pi) + i \sin(\frac{\alpha + 2q\pi}{n} + 2l\pi)) = \sqrt[n]{r}(\cos(\frac{\alpha + 2q\pi}{n}) + \end{aligned}$$

$i \sin\left(\frac{\alpha + 2q\pi}{n}\right) = z_q$, при цьому $0 \leq q < n$, тобто $q \in \{0, 1, \dots, n-1\}$ оскільки $q \in \mathbb{Z}$. Покажемо що всі z_k є коренями степеня n з числа c . За формулою Муавра $z_k^n = \left(\sqrt[n]{r}\left(\cos\frac{\alpha + 2k\pi}{n} + i \sin\frac{\alpha + 2k\pi}{n}\right)\right)^n = (\sqrt[n]{r})^n (\cos(\alpha + 2k\pi) + i \sin(\alpha + 2k\pi)) = r(\cos\alpha + i \sin\alpha) = c$. Оскільки при переході від кореня z_i до кореня z_{i+1} аргумент z_i зростає на $\frac{2\pi}{n}$, то z_0, z_1, \dots, z_{n-1} різні.

Таким чином для даного комплексного числа $c = r(\cos\alpha + i \sin\alpha) \neq 0$ існує в точності n комплексних коренів степеня n : z_0, z_1, \dots, z_{n-1} , які визначаються за правилом $z_k = \sqrt[n]{r}\left(\cos\frac{\alpha + 2k\pi}{n} + i \sin\frac{\alpha + 2k\pi}{n}\right)$, $k = 0, 1, \dots, n-1$. Точки, що відповідають комплексним числам z_0, \dots, z_{n-1} , знаходяться на колі радіуса $\sqrt[n]{r}$ і ділять коло на n рівних частин.

10. Корені з одиниці

Запишемо 1 в тригонометричній формі $1 = \cos 0 + i \sin 0$. Припустимо, що $\varepsilon_0, \varepsilon_1, \varepsilon_{n-1}$ — комплексні корені з 1. За правилом $\varepsilon_k = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$, $k = \overline{0, n-1}$, тому зрозуміло, що $\varepsilon_0 = 1$. Сформулюємо і доведемо деякі властивості коренів з 1.

1) Добуток двох коренів з 1 степеня n є коренем з 1 степеня n .

Дійсно, якщо $\varepsilon_i, \varepsilon_j$ — два кореня, то $(\varepsilon_i \varepsilon_j)^n = \varepsilon_i^n \varepsilon_j^n = 1 \cdot 1 = 1$.

2) Якщо ε — деякий корінь з 1 степеня n то $\frac{1}{\varepsilon}$ також корінь з 1 степеня n .

Дійсно, $(\varepsilon^{-1})^n = (\varepsilon^n)^{-1} = 1^{-1} = 1$.

3) Якщо ε — корінь степеня n з 1, то ε^l для $\forall l \in \mathbb{Z}$ — також корінь степеня n з 1.

Впливає з перших двох властивостей.

4) Якщо $c \neq 0$ — деяке комплексне число і z — деякий корінь степеня n з c , то всі корені степеня n з числа c можна одержати домножаючи z на всі корені з 1 степеня n .

Дійсно, нехай ε — деякий комплексний корінь степеня n з 1, тоді $(z\varepsilon)^n = z^n \varepsilon^n = c \cdot 1 = c$. Таким чином, $z\varepsilon$ є коренем степеня n з числа c . Тому послідовно домножаючи z на $\varepsilon_0, \varepsilon_1, \varepsilon_{n-1}$ ми одержимо n різних коренів степ n з c і ними вичерпуються всі корені степеня n з c .

11. Примітивні корені з одиниці

Нехай ε — деякий корінь степеня n з 1. Тоді це число буде коренем степеня l з 1 для будь-якого l , кратного n . Беремо всі корені з 1 степеня n $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}$: $\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$, тоді серед цих коренів можуть бути такі, що будуть коренями з 1 степеня n' , де n' — дільник числа n .

Означення 2. Корінь ε з 1 степеня n називається примітивним, якщо він не є коренем з 1 деякого меншого степеня.

Покажемо існування примітивних коренів. Візьмемо корінь ε_1 ; за формулою Муавра $\varepsilon_k = \varepsilon_1^k, \forall k \in \mathbb{Z}$; таким чином ε є примітивним коренем, тобто $\forall n \in \mathbb{N}$ корінь з 1 $\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ є примітивним.

Зрозуміло, якщо ε — примітивний корінь степеня n з 1 і $\varepsilon^k = 1$ то $n|k$. Дійсно, припустимо, що це не так. Поділимо k на n з залишком: $k = ln + q, l, q \in \mathbb{Z}, 0 \leq q < n$. Тоді $1 = \varepsilon^k = \varepsilon^{ln+q} = \varepsilon^{ln} \cdot \varepsilon^q = (\varepsilon^n)^l \cdot \varepsilon^q = 1 \cdot \varepsilon^q = \varepsilon^q$ тобто $\varepsilon^q = 1$, що суперечить примітивності кореня ε .

Доведемо деякі умови, яким задовольняють примітивні корені. В загальному випадку примітивним коренем з 1 може бути тільки ε_1 , тому наступні умови дають можливість визначати примітивні корені.

1) Корінь n -го степеня з 1 ε є примітивним \iff коли числа $\varepsilon^k, k = \overline{0, n-1}$ різні.

Дійсно, якщо всі числа ε^k різні, то зрозуміло, що ε — примітивний корінь. Припустимо, навпаки ε^k — примітивний корінь і доведемо, що всі ε^k різні.

Нехай маємо k і l такі, що $0 \leq k < l \leq n-1, \varepsilon^k = \varepsilon^l$, тоді $\varepsilon^{l-k} = 1$,

причому $0 \leq l - k \leq n - 1$, тобто ε є коренем степеня $l - k$ з 1, що суперечить його примітивності.

З цієї властивості випливає: якщо ε — примітивний корінь з 1 степеня n , то всі корені з 1 степеня n це числа $\varepsilon^0, \varepsilon^1, \dots, \varepsilon^{n-1}$.

2) Нехай ε — примітивний корінь з 1 степеня n . Число ε^k є примітивним коренем з 1 степеня $n \iff$ коли числа k і n є взаємнопростими.

(\implies) Нехай ε^k — примітивний корінь і $d = \text{НСД}(k, n)$. Припустимо, $d > 1$, тоді $k = k'd, n = n'd$, при цьому $k' < k, n' < n, k', n' \in \mathbb{Z}$.

З цього випливає, що $(\varepsilon^k)^{n'} = \varepsilon^{kn'} = \varepsilon^{k'dn'} = (\varepsilon^n)^{k'} = 1$, тобто ε^k є коренем з 1 степеня n' . Оскільки ε^k — примітивний корінь, то за доведеним $n|n'$ що суперечить умові $n' < n$.

(\impliedby) Припустимо, що $d = \text{НСД}(k, n) = 1$; Припустимо ε не є примітивним коренем. Тоді існує число $m \in \mathbb{Z}$ таке, що $0 < m < n$ і $(\varepsilon^k)^m = 1$ тобто $\varepsilon^{km} = 1$, але ε — примітивний корінь, тому за доведеним $n|km$. Оскільки $m < n$ то числа k і n не є взаємнопростими, що суперечить умові $d = \text{НСД}(k, n) = 1$.

Розділ 2

Многочлени

1. Числові поля

Означення 3. Числовим полем називається підмножина множини \mathbb{C} всіх комплексних чисел, яка містить 0 і 1 , замкнена відносно операцій додавання, віднімання, множення і ділення на ненульові числа.

Нехай F — деяке числове поле, оскільки $1 \in F$ і множина F замкнена відносно операції додавання, то всі натуральні числа належать F ($\mathbb{N} \subseteq F$). Оскільки $0 \in F$ і F замкнена відносно віднімання, то множина цілих чисел $\mathbb{Z} \subseteq F$. Оскільки F замкнена відносно ділення на ненульові числа, то множина раціональних чисел також належить F ($\mathbb{Q} \subseteq F$). Але множина \mathbb{Q} задовольняє умовам поля, таким чином \mathbb{Q} — це найменше числове поле, яке міститься в будь-якому числовому полі. Також зрозуміло, що умовам поля задовольняють множина комплексних чисел \mathbb{C} та множина дійсних чисел \mathbb{R} . Таким чином маємо три числових поля $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

З'ясуємо, чи існує числове поле F таке, що $\mathbb{R} \subseteq F \subseteq \mathbb{C}$ і $F \neq \mathbb{R}$, $F \neq \mathbb{C}$. Якщо F складається лише з дійсних чисел, то $F = \mathbb{R}$. Тому, припустимо що існує $a + bi \in F$, де $a, b \in \mathbb{R}$, $b \neq 0$. Оскільки $a, b \in \mathbb{R} \subseteq F$, то $(a + bi) - a = bi \in F$, $\frac{bi}{b} = i \in F$, тоді $\forall l \in \mathbb{R} : li \in F, \forall k, l \in \mathbb{R} : k + li \in F; F = \mathbb{C}$. Отже, якщо F задовольняє умові $\mathbb{R} \subseteq F \subseteq \mathbb{C} \implies F = \mathbb{R}$ або $F = \mathbb{C}$.

З'ясуємо, чи існує числове поле $F : \mathbb{Q} \subseteq F \subseteq \mathbb{R}, F \neq \mathbb{Q}, F \neq \mathbb{R}$. Візьмемо множину $F = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ покажемо, що множина F є полем. Умови:

$$1. a_1 + b_1\sqrt{2} \in F, a_2 + b_2\sqrt{2} \in F \implies (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in F;$$

$$2. a_1 + b_1\sqrt{2} \in F, a_2 + b_2\sqrt{2} \in F \implies (a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) =$$

$$(a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in F;$$

$$3. a_1 + b_1\sqrt{2} \in F, a_2 + b_2\sqrt{2} \in F \implies (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in F;$$

$$4. a_1 + b_1\sqrt{2} \in F, a_2 + b_2\sqrt{2} \in F, a_2 + b_2\sqrt{2} \neq 0 \implies \frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} = \frac{(a_1 + b_1\sqrt{2})(a_2 - b_2\sqrt{2})}{(a_2 + b_2\sqrt{2})(a_2 - b_2\sqrt{2})} = \frac{(a_1a_2 - 2b_1b_2) + (a_2b_1 - a_1b_2)\sqrt{2}}{a_2^2 - 2b_2^2} = \frac{a_1a_2 - 2b_1b_2}{a_2^2 - 2b_2^2} + \frac{a_2b_1 - a_1b_2}{a_2^2 - 2b_2^2}\sqrt{2}.$$

Залишається перевірити, що $a_2^2 - 2b_2^2 \neq 0$, тобто $(a_2 - b_2\sqrt{2})(a_2 + b_2\sqrt{2}) \neq 0$. За умовою $a_2 + b_2\sqrt{2} \neq 0$. Якщо $b_2 = 0$, то $a_2 \neq 0$, $a_2^2 - 2b_2^2 = a_2^2 \neq 0$. Якщо $b_2 \neq 0$, $a_2 - b_2\sqrt{2} = 0 \implies \sqrt{2} = \frac{a_2}{b_2}$, тобто $\sqrt{2}$

раціональне число, що не вірно. Таким чином, $\frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} \in F$.

Отже F — числове поле, позначимо його $F(\sqrt{2})$. $\mathbb{Q} \subseteq F(\sqrt{2}) \subseteq \mathbb{R}$, $F(\sqrt{2}) \neq \mathbb{Q}$, $F(\sqrt{2}) \neq \mathbb{R}$. Аналогічно можна скласти поле $F(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Q}\}$, тобто існує нескінченна кількість полів $F : \mathbb{Q} \subseteq F \subseteq \mathbb{R}$, $F \neq \mathbb{Q}$, $F \neq \mathbb{R}$.

Чи існує поле $F : F \neq \mathbb{C}$ та F не міститься в \mathbb{R} ? Комплексне число називається алгебраїчним, якщо воно є коренем деякого многочлена $f(x) = a_nx_n + a_{n-1}x_{n-1} + \dots + a_1x + a_0$ з цілими коефіцієнтами $a_n, a_{n-1}, \dots, a_0 \in \mathbb{Z}$. Наведемо деякі приклади алгебраїчних чисел. Всі цілі числа є алгебраїчними: наприклад $m \in \mathbb{Z}$ є коренем многочлена $f(x) = x - m$, всі раціональні числа є алгебраїчними: $\frac{p}{q} \in \mathbb{Q}$, $f(x) = qx - p$, $\sqrt{2}$ також є алгебраїчним: воно є коренем многочлена $f(x) = x^2 - 2$, число i алгебраїчне як корінь многочлена $f(x) = x^2 + 1$. Множина всіх многочленів з цілими коефіцієнтами є зліченною. Далі ми побачимо що будь-який многочлен навіть з комплексними коефіцієнтами має скінченне число коренів (число не перевищує степінь). З цього випливає, що множина всіх алгебраїчних чисел злічена, отже на співпадає з \mathbb{C} . Комплексні числа, які не є алгебраїчними, називаються трансцендентними.

Множина F всіх алгебраїчних чисел є числовим полем. F не міститься в \mathbb{R} .

2. Многочлени над числовими полями

Нехай F — числове поле, а x — деяка змінна, позначимо через $F[x]$ множину всіх многочленів з коефіцієнтами з поля F від змінної x . Множина $F[x]$ називається кільцем многочленів над полем F . Множина $F[x]$ має такі властивості:

1. $f_1, f_2 \in F[x] \implies f_1 + f_2 \in F[x], f_1 - f_2 \in F[x]$.
2. $f_1, f_2 \in F[x] \implies f_1 \cdot f_2 \in F[x]$.
3. Якщо степінь $g \in F[x]$ не перевищує степеня многочлена $f \in F[x]$, то многочлен f можна поділити на g із залишком: $f(x) = g(x) \cdot q(x) + r(x)$, степінь $r(x) <$ степеня $g(x)$ і $g, r \in F[x]$.

Кільце многочленів $F[x]$ замкнене відносно додавання, віднімання, множення многочленів і при діленні многочленів частка та залишок $\in F[x]$. Можна розглядати кільця многочленів $\mathbb{R}[x], \mathbb{Q}[x], \mathbb{C}[x]$.

3. Теорія ділення многочленів

Розглянемо кільце многочленів $F[x]$ над фіксованим числовим полем F .

Казатимемо, що многочлени $g(x)$ і $q(x)$ є дільниками $f(x)$, якщо існує многочлен $p(x) \in F[x] : f(x) = g(x) \cdot q(x) + p(x)$, цей факт позначатимемо $g(x)|f(x), q(x)|f(x)$.

Многочлен $p(x)$ називається спільним дільником многочленів $f(x), g(x)$ якщо $p(x)|f(x)$ і $p(x)|g(x)$.

Означення 4. Многочлен $d(x)$ називається найбільшим спільним дільником многочленів $f(x)$ і $g(x)$, якщо виконується:

1) $d(x)|f(x)$ і $d(x)|g(x)$;

2) якщо $p(x)$ такий, що $p(x)|f(x) \wedge p(x)|g(x) \implies p(x)|d(x)$

Позначатимемо це $d(x) = \text{НСД}(f(x), g(x))$; степінь многочлена f будемо позначати ст. $f(x)$.

Два многочлена $f(x)$ і $g(x)$ будемо називати асоційованими, якщо вони відрізняються лише числовим множником який не дорівнює 0, тобто $\exists \alpha \in F, \alpha \neq 0 : g(x) = \alpha \cdot f(x)$.

Якщо $g(x)|f(x)$, то $g(x)|\alpha f(x), \forall \alpha \in F$ і навпаки, якщо $g(x)|f(x)$, то $\forall \alpha, \alpha \neq 0 : \alpha g(x)|f(x)$.

Лема 1. Нехай $d(x) - \text{НСД } f(x) \text{ і } g(x)$.

Многочлен $d_1(x) = \text{НСД}(f(x), g(x)) \iff d(x) \text{ і } d_1(x) \text{ асоційовані.}$

Доведення. Якщо $d(x)$ і $d_1(x)$ асоційовані та $d(x) = \text{НСД}(f(x), g(x))$, то $d_1(x) = \text{НСД}(f(x), g(x))$.

Нехай, навпаки, виконується $d(x) = \text{НСД}(f(x), g(x))$,

$d_1(x) = \text{НСД}(f(x), g(x))$. За означенням $\text{НСД } d(x)|d_1(x) \implies d_1(x) = d(x)q(x), q(x) \in F[x]$. Аналогічно $d_1(x)|d(x)$ і $d(x) = d_1(x)r(x), r(x) \in F[x]$. Тоді $d_1(x) = d(x)g(x) = d_1(x)r(x)q(x)$. Оскільки при множенні степені додаються, то ст. $d_1(x) = \text{ст.}d_1(x) + \text{ст.}r(x) + \text{ст.}q(x) \implies \text{ст.}r(x) + \text{ст.}q(x) = 0 \implies \text{ст.}r(x) = 0, \text{ст.}q(x) = 0, r(x) = a = \text{const} \neq 0, q(x) = b = \text{const} \neq 0$. Отже, многочлени d та d_1 асоційовані. \square

З леми випливає, що НСД 2-х даних многочленів визначається з точністю до ненульового многочлена. Щоб уникнути цієї неоднозначності іноді НСД вважається той, старший коефіцієнт якого дорівнює одиниці.

Означення 5. Два многочлена $f(x)$ та $g(x)$ називаються взаємно простими, якщо $\text{НСД}(f(x), g(x)) = \text{const} \neq 0$. Враховуючи лему: $\text{НСД}(f(x), g(x)) = 1$.

Виникає запитання: чи для кожної пари многочленів існує НСД. Для відповіді опишемо алгоритм знаходження НСД, що називається алгоритмом Евкліда.

4. Алгоритм Евкліда

Нехай задано два ненульових многочлена $f(x)$ і $g(x)$, для визначеності покладемо ст. $f(x) \geq$ ст. $g(x)$. Поділимо $f(x)$ на $g(x)$ із залишком:

$$f(x) = g(x) \cdot q(x) + r_1(x), \text{ де ст. } r_1 < \text{ ст. } g;$$

якщо $r_1 = 0$, процес закінчується; інакше поділимо $g(x)$ на $r_1(x)$:

$$g(x) = r_1(x)q_2(x) + r_2(x), \text{ ст. } r_2 < \text{ ст. } r_1;$$

якщо $r_2 = 0$, процес закінчується, інакше ділимо r_1 на r_2 :

$$r_1(x) = r_2(x)q_3(x) + r_3(x), \text{ ст. } r_3 < \text{ ст. } r_2 \text{ і т. д.}$$

Оскільки на кожному кроці степінь многочлена зменшується, то через скінченну кількість кроків процес закінчиться. Нехай

$$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x), \text{ ст. } r_k < \text{ ст. } r_{k-1}, r_k \neq 0;$$

$$r_{k-1}(x) = r_k(x)q_{k+1}(x) + r_{k+1}(x), \text{ ст. } r_{k+1} < \text{ ст. } r_k, r_{k+1} \neq 0;$$

$$r_k(x) = r_{k+1}(x)q_{k+2}(x).$$

Покажемо, що $d(x) = \text{НСД}(f(x), g(x)) = r_{k+1}(x)$, для цього треба перевірити дві умови НСД.

1) Покажемо, $r_{k+1}(x)|f(x), r_{k+1}(x)|g(x)$. З останньої рівності $r_{k+1}(x)|r_k(x)$, тоді з передостанньої $r_{k+1}(x)|r_{k-1}(x)$. Далі піднімемось знизу догори і одержимо $r_{k+1}(x)|r_{k-2}(x), \dots, r_{k+1}(x)|r_1(x), r_{k+1}(x)|g(x)$, тому $r_{k+1}(x)|f(x)$.

2) Нехай $p(x)|f(x)$ і $p(x)|g(x)$. Ідемо по рівностям зверху вниз. Оскільки $r_1(x) = f(x) - g(x)q(x)$, то $p(x)|r_1(x)$. З другої рівності $p(x)|r_2(x), \dots, p(x)|r_{k-1}(x) \implies p(x)|r_k(x) \implies p(x)|r_{k+1}(x)$. Таким чином умови НСД виконуються, $r_{k+1}(x) = \text{НСД}(f(x), g(x))$.

5. Теорема про НСД

Теорема 1. *Нехай $d(x)$ є НСД многочленів $f(x)$ і $g(x)$, тоді існують такі многочлени $f_1(x)$ і $g_1(x)$, що $d(x) = f_1(x)f(x) + g_1(x)g(x)$. При цьому, якщо ст. $f(x) > 0$, ст. $g(x) > 0$, то множники f_1 і g_1 можна вибрати так, що ст. $f_1(x) <$ ст. $g(x)$, а ст. $g_1(x) <$ ст. $f(x)$.*

Доведення. Нехай $d(x) = \text{НСД}(f(x), g(x))$, $f(x), g(x)$ — ненульові мно-

члени. Довести це можна двома способами:

1 спосіб. Позначимо через S таку множину многочленів:

$S = \{a(x)f(x) + b(x)g(x) \mid a(x), b(x) \in F[x]\}, S \subseteq F[x]$. Визначимо деякі властивості множини S :

1) Якщо $s_1(x)$ і $s_2(x) \in S \implies s_1(x) \pm s_2(x) \in S$. Дійсно, $s_1(x) = a_1(x)f(x) + b_1(x)g(x)$, $s_2(x) = a_2(x)f(x) + b_2(x)g(x) \implies s_1(x) \pm s_2(x) = (a_1(x) \pm a_2(x))f(x) + (b_1(x) \pm b_2(x))g(x)$.

2) Якщо $s(x) \in S$, а $p(x) \in F[x]$ многочлен (що не обов'язково є многочленом з S), то $p(x)s(x) \in S$. Дійсно, $s(x) = a(x)f(x) + b(x)g(x)$, тоді $p(x)s(x) = p(x)a(x)f(x) + p(x)b(x)g(x)$.

3) Якщо деякий многочлен $p(x) \mid f(x)$ і $p(x) \mid g(x)$ то $\forall s(x) \in S : p(x) \mid s(x)$.

4) $f(x) \in S, g(x) \in S$, оскільки $f(x) = 1 \cdot f(x) + 0 \cdot g(x)$, $g(x) = 0 \cdot f(x) + 1 \cdot g(x)$.

В множині S вибираємо ненульовий многочлен найменшого степеня і позначимо його через $k(x)$. За властивістю 3): якщо $d(x) = \text{НСД}(f(x), g(x)) \implies d(x) \mid k(x)$. Покажемо, що \forall многочлен з множини S ділиться на $k(x)$. Припустимо супротивне: деякий многочлен $s(x) \in S$ не ділиться на $k(x)$. Тоді поділимо його на $k(x)$ із залишком: $s(x) = k(x)q(x) + r(x)$, ст. $r(x) <$ ст. $k(x)$, $r(x) \neq 0$. Враховуючи 1) і 2) одержимо ($s(x) \in S, k(x) \in S \implies k(x)q(x) \in S \implies r(x) = s(x) - k(x)q(x) \in S$). Таким чином, в множині S ми знайшли ненульовий многочлен $r(x)$, степінь якого є меншим, ніж степінь $k(x)$, що суперечить вибору цього многочлена. Отже, $k(x) \mid s(x)$. Тоді, враховуючи 4), $k(x) \mid f(x), k(x) \mid g(x)$. Тому за означенням НСД $\implies k(x) \mid d(x)$. Раніше ми одержали $d(x) \mid k(x)$. Таким чином, многочлени $k(x)$ і $g(x)$ відрізняються лише числовим множником, тобто вони асоційовані. Тому $\exists \alpha \in F, \alpha \neq 0 : d(x) = \alpha k(x)$ і за 2) $d(x) \in S$. За означенням множини $S \exists f_1(x), g_1(x) \in F[x] : d(x) = f_1(x)f(x) + g_1(x)g(x)$.

2 спосіб доведення конструктивний. Він дає можливість знайти многочлени $f_1(x)$ і $g_1(x)$.

Нехай знову $d(x) = \text{НСД}(f(x), g(x))$, для визначеності вважаємо ст. $f(x) \geq$ ст. $g(x)$. Будемо знаходити НСД за допомогою алгоритма Евкліда.

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x), r_1(x) \neq 0; \\ g(x) &= r_1(x)q_2(x) + r_2(x), r_2(x) \neq 0; \\ r_1(x) &= r_2(x)q_3(x) + r_3(x), r_3(x) \neq 0; \\ r_2(x) &= r_3(x)q_4(x) \implies d(x) = r_3(x). \end{aligned}$$

Тоді з передостанньої рівності одержуємо:

$$\begin{aligned} d(x) &= r_3(x) = r_1(x) - r_2(x)q_3(x) = r_1(x) + (-q_3(x))r_2(x); \\ r_2(x) &= g(x) - r_1(x)q_2(x) \implies d(x) = r_1(x) + (-q_3(x))(g(x) - r_1(x)q_2(x)) = \\ &= (-q_3(x))g(x) + (1 + q_3(x)q_2(x))r_1(x); \\ r_1(x) &= f(x) - g(x)q_1(x) \implies \\ \implies d(x) &= (-q_3(x))g(x) + (1 + q_3(x)q_2(x))(f(x) - g(x)q_1(x)) = \\ &= (1 + q_3(x)q_2(x))f(x) + (-q_3(x) + (1 + q_3(x)q_2(x))q_1(x))g(x); \\ f_1(x) &= 1 + q_3(x)q_2(x); \\ g_1(x) &= -q_3(x) + (1 + q_3(x)q_2(x))q_1(x). \end{aligned}$$

Одержали шукані многочлени. Залишається довести остатню частину теореми. Припустимо ми вже знайшли многочлени $f_1(x)$ та $g_1(x)$, такі що $d(x) = f_1(x)f(x) + g_1(x)g(x)$ але, наприклад ст. $f_1(x) \geq$ ст. $g(x)$. Ділимо $f_1(x)$ на $g(x)$ із залишком. Тобто отримаємо $f_1(x) = g(x)q(x) + r(x)$, де ст. $r(x) <$ ст. $g(x)$, тоді $d(x) = (g(x)q(x) + r(x))f(x) + g_1(x)g(x) = r(x)f(x) + (g_1(x) + q(x)f(x))g(x)$. ст. $r(x) <$ ст. $g(x)$, треба показати, що ст. $(g_1(x) + q(x)f(x)) <$ ст. $f(x)$. Припустимо, це невірно: ст. $(g_1(x) + q(x)f(x)) \geq$ ст. $f(x)$, тоді ст. $(g_1(x) + q(x)f(x))g(x) \geq$ ст. $f(x) +$ ст. $g(x)$. Оскільки ст. $(r(x)f(x)) <$ ст. $f(x) +$ ст. $g(x)$, то ст. $d(x) \geq$ ст. $f(x) +$ ст. $g(x)$, що неможливо, а тому ст. $(g_1(x) + q(x)f(x)) <$ ст. $f(x)$. \square

Наслідок 1. *Нехай многочлени $f(x)$ і $g(x)$ взаємно прості, тоді існують многочлени $f_1(x)$ і $g_1(x)$, такі що $f_1(x)f(x) + g_1(x)g(x) = 1$, причому, якщо ст. $f(x) > 0$, ст. $g(x) > 0$, то многочлени $f_1(x)$ і $g_1(x)$*

можна вибрати так, що ст. $f_1(x) < \text{ст. } g(x)$, ст. $g_1(x) < \text{ст. } f(x)$.

6. Теорема Безу

Розглянемо кільце $F[x]$ всіх многочленів над числовим полем F , $f(x) \in F[x]$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $n \geq 1$, $\alpha \in F$.

Теорема 2. Значення многочлена $f(x)$ при $x = \alpha$, $\alpha \in F$ дорівнює залишку від ділення многочлена $f(x)$ на двочлен $(x - \alpha)$.

Доведення. Поділимо многочлен $f(x)$ на $(x - \alpha)$ з залишком $f(x) = (x - \alpha)g(x) + r$, $r = \text{const}$. Підставимо $x = \alpha \implies f(\alpha) = r$. \square

Наслідок 2. Число $\alpha \in F$ є коренем многочлена $f(x) \in F[x] \iff f(x)$ ділиться на $(x - \alpha)$, тоді $f(x) = (x - \alpha)g(x)$.

7. Схема Горнера та її застосування

Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$ і поділимо цей многочлен з залишком на $\alpha \in F$. $f(x) = (x - \alpha)g(x) + r$, $r = f(\alpha)$. Зрозуміло, що ст. многочлена $g(x) = n - 1$, тобто $g(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_1 x + b_0$, тоді $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = (x - \alpha)(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_1 x + b_0) + r$. Звідси $a_n = b_{n-1}$, $a_{n-1} = b_{n-2} - \alpha b_{n-1}$, $a_{n-2} = b_{n-3} - \alpha b_{n-2}$, ..., $a_2 = b_1 - \alpha b_2$, $a_1 = b_0 - \alpha b_1$, $a_0 = r - \alpha b_0 \implies b_{n-1} = a_n$, $b_{n-2} = a_{n-1} + \alpha b_{n-1}$, $b_{n-3} = a_{n-2} + \alpha b_{n-2}$, ..., $b_1 = a_2 + \alpha b_2$, $b_0 = a_1 + \alpha b_1$, $r = a_0 + \alpha b_0$. Таким чином коефіцієнт частки $g(x)$ і залишок r можна одержати, користуючись схемою Горнера.

	a_n	a_{n-1}	a_{n-2}	...	a_1	a_0
α	$b_{n-1} = a_n$	$b_{n-2} =$ $= a_{n-1} +$ $+\alpha b_{n-1}$	$b_{n-3} =$ $= a_{n-2} +$ $+\alpha b_{n-2}$...	$b_0 = a_1 +$ $+\alpha b_1$	$r = a_0 +$ $+\alpha b_0$

Приклад 2 (застосування схеми Горнера). Розкласти многочлен $f(x) = x^5 - 6x^4 - x^3 + x^2 + x + 1$ по степенях $(x - 1)$. Ділимо $f(x)$ на $(x - 1)$ з залишком $f(x) = (x - 1)g(x) + c_0$, $c_0 = f(1)$. Ділимо $g(x)$ на $(x - 1)$ з

залишком $g(x) = (x-1)h(x) + c_1$, тоді $f(x) = c_0 + c_1(x-1) + (x-1)^2h(x)$
і т. д.

	1	-6	-1	1	1	1
1	1	-5	-6	-5	-4	-3
1	1	-4	-10	-15	-19	
1	1	-3	-13	-28		
1	1	-2	-15			
1	1	-1				
1	1					

$$d(x) = -3 - 19(x-1) - 28(x-1)^2 - 15(x-1)^3 - (x-1)^4 + (x-1)^5.$$

8. Незвідні многочлени та основна теорема про подільність многочлена

Як відомо, простим числом називається число n таке, що $n \neq 1$ і його дільниками є лише саме число і 1. Аналогом простих чисел в кільці многочленів є незвідні многочлени.

Означення 6. Многочлен $f(x) \in F[x]$ ненульового степеня називається незвідним над полем F , якщо з того, що $f(x) = f_1(x) \cdot f_2(x)$, де $f_1(x) \in F[x]$, $f_2(x) \in F[x]$ випливає, що або ст. $f_1(x) = 0$, або ст. $f_2(x) = 0$, тобто, що принаймні один з них є константою.

Якщо многочлен $f(x)$ не є незвідним, то він називається звідним.

Основна теорема арифметики каже, що $\forall n \in N, n \neq 1$ можна розкласти у добуток простих. Аналогом цієї теореми для многочленів є основна теорема про подільність многочленів.

Нехай $p_1(x), p_2(x)$ незвідні многочлени і $p_1(x) | p_2(x)$, причому ст. $p_1(x) > 0$ і ст. $p_2(x) > 0$, $p_2(x) = p_1(x)f(x)$, $f(x) \in F[x]$, тоді за означенням незвідного многочлена ст. $f(x) = 0$, тобто $f(x) = \alpha = const$, $p_2(x) = \alpha p_1(x)$, тобто многочлен $p_1(x)$ і $p_2(x)$ асоційовані.

Лема 2 (про незвідні многочлени). *Нехай $p(x)$ — незвідний многочлен і $p(x)|f(x)g(x)$, $f(x), g(x) \in F[x]$. Тоді або $p(x)|f(x)$ або $p(x)|g(x)$.*

Доведення. Припустимо $g(x)$ не ділиться на $p(x)$ і покажемо, що $p(x)|f(x)$, а для цього доведемо, що $p(x)$ і $g(x)$ взаємно прості. Припустимо супротивне: $\exists k(x) \in F[x] : \text{ст. } k(x) > 0$, і $k(x)|p(x), k(x)|g(x)$. Тоді, оскільки $p(x)$ незвідний многочлен, то $k(x) = \alpha p(x)$, $\alpha \in F, \alpha \neq 0$. Тобто многочлени $p(x)$ і $k(x)$ асоційовані. Оскільки $k(x)|g(x)$, то і для асоційованого $p(x)|g(x)$, що суперечить припущенню. Таким чином, $p(x)$ і $g(x)$ взаємно прості многочлени і за наслідком з теореми про НСД $\exists p_1(x)$ і $g_1(x)$ такі, що $1 = p_1(x)p(x) + g_1(x)g(x)$. Домножимо цю рівність на $f(x)$: $f(x) = f(x)p_1(x)p(x) + g_1(x)f(x)g(x)$. Зрозуміло, що $p(x)|f(x)p_1(x)p(x)$. За умовою теореми: $p(x)|g_1(x)f(x)g(x)$. Звідси $p(x)|f(x)$. \square

Зауваження 1. Індуктивно по числу многочленів можна довести таке твердження: нехай $p(x)$ — незвідний многочлен і $p(x)|f_1(x)f_2(x)\dots f_k(x)$, де $f_1(x), f_2(x), \dots, f_k(x) \in F[x]$. Тоді принаймні для одного номера j : $p(x)|f_j(x)$.

Зауваження 2. Ця лема виконується тільки якщо $p(x)$ — незвідний многочлен. Дійсно, нехай $p(x)$ — звідний, тоді існують такі многочлени $p_1(x), p_2(x)$, що $p(x) = p_1(x)p_2(x)$, ст. $p_1(x) > 0$, ст. $p_2(x) > 0$. Тому ст. $p(x) = \text{ст. } p_1(x) + \text{ст. } p_2(x) \implies \text{ст. } p(x) > \text{ст. } p_1(x)$, ст. $p(x) > \text{ст. } p_2(x)$, а тому жоден з множників $p_1(x), p_2(x)$ не ділиться на $p(x)$.

Теорема 3 (Основна теорема про подільність многочлена). *Будь-який многочлен $f(x) \in F[x]$, такий що ст. $f(x) \geq 1$, можна розкласти в добуток незвідних многочленів над полем F . Причому цей розклад єдиний з точністю до порядку множників і констант.*

Доведення. 1) доведемо можливість розкладу.

Якщо многочлен $f(x)$ незвідний, то це виконується.

Якщо $f(x)$ звідний, то $\exists f_1(x), f_2(x) : \text{ст. } f_1(x) > 0$, ст. $f_2(x) > 0$, і $f(x) = f_1(x)f_2(x)$. Якщо многочлени $f_1(x), f_2(x)$ незвідні, то все викону-

ється, інакше їх також можна розкласти в добутки множників ненульового степеня. Оскільки на кожному кроці ст. многочлена зменшується, то через скінченне число кроків ми прийдемо до шуканого розкладу.

Інакше цей факт можна довести індукцією.

Зрозуміло, що для многочлена степеня 1 твердження виконується. Припустимо, що це виконується для всіх многочленів степеней $\leq n - 1$. Беремо деякий многочлен $f(x)$ степеня n . Якщо він незвідний, то все виконується. Якщо він звідний, то його можна розкласти в добуток двох многочленів меншого степеня, кожен з яких розкладається в добуток незвідних многочленів за припущенням індукції.

2) доведемо, що цей розклад єдиний.

Припустимо існує два розклади: $f(x) = p_1(x)p_2(x)\dots p_k(x)$, $f(x) = q_1(x)q_2(x)\dots q_s(x)$, при чому многочлени $p_1(x), \dots, p_k(x), q_1(x), \dots, q_s(x)$ незвідні над полем F і мають ненульовий степінь. Треба довести, що $k = s$ і розклади відрізняються лише порядком.

Припустимо, для визначеності, $k \leq s$, тоді $p_1(x)p_2(x)\dots p_k(x) = q_1(x)q_2(x)\dots q_s(x)$. Звідси $p_1(x)|q_1(x)q_2(x)\dots q_s(x)$ і, оскільки $p_1(x)$ незвідний многочлен, то з леми про незвідні многочлени випливає, що принаймні один з многочленів $q_1(x), q_2(x), \dots, q_s(x)$ ділиться на $p_1(x)$. Оскільки в добутку можна переставляти елементи, то можна вважати, що $p_1(x)|q_1(x)$, але многочлени $p_1(x)$ і $q_1(x)$ незвідні, тому вони асоційовані, тобто існує $\alpha_1 \in F, \alpha_1 \neq 0$ такий, що $q_1(x) = \alpha_1 p_1(x) \implies p_1(x)p_2(x)\dots p_k(x) = \alpha_1 p_1(x)q_2(x)\dots q_s(x)$. Скорочуємо цю рівність на $p_1(x)$ і отримаємо $p_2(x)p_3(x)\dots p_k(x) = \alpha_1 q_2(x)q_3(x)\dots q_s(x)$. Аналогічно доводимо, що $p_2(x)|q_2(x)$ і $\exists \alpha_2 \in F, \alpha_2 \neq 0 : q_2(x) = \alpha_2 p_2(x)$. Тоді після скорочення: $p_3(x)\dots p_k(x) = \alpha_1 \alpha_2 q_3(x)\dots q_s(x)$. Після k кроків такого процесу одержуємо рівність $1 = \alpha_1 \alpha_2 \dots \alpha_k q_{k+1}(x)\dots q_s(x)$. В лівій частині многочлен нульового степеня, тому ст. $(q_{k+1}(x)\dots q_s(x)) = 0$. І при $s > k$ приходимо до протиріччя. Таким чином $s = k$ і $q_i(x) = \alpha_i p_i(x), i = 1, \dots, k, \alpha_i \in F, \alpha_i \neq 0$, що доводить теорему. \square

Нехай n — непросте число ($n \neq 1$). Як відомо, це число можна розкласти в добуток простих чисел $n = p_1 p_2 \dots p_k$. Прості числа в цьому добутку можуть повторюватися, а тому можна зібрати разом однакові прості числа і одержати розклад $n = q_1^{n_1} q_2^{n_2} \dots q_s^{n_s}$, де всі числа q_1, q_2, \dots, q_s прості і різні. Аналогічну операцію можна зробити і для многочленів. Нехай многочлен $f(x)$ розкладається в добуток незвідних множників $f(x) = p_1(x)p_2(x)\dots p_k(x)$. Збираємо разом всі множники, які відрізняються лише числовими множниками і одержимо: $f(x) = q_1^{n_1}(x)q_2^{n_2}(x)\dots q_s^{n_s}(x)$, де всі многочлени $q_1(x), \dots, q_s(x)$ незвідні і різні. Цей розклад називається канонічним розкладом многочлена $f(x)$ в добуток незвідних множників.

9. Лема про похідну

Означення 7. Многочлен $g(x)$ входить множником в многочлен $f(x)$ з кратністю k , якщо $f(x)$ ділиться на $g^k(x)$ і не ділиться на $g^{k+1}(x)$.

Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ є многочленом з довільними комплексними коефіцієнтами, причому ст. $f(x) \geq 1$.

Означення 8. Похідною від многочлена $f(x)$ називають многочлен $f'(x) = a_n n x^{n-1} + a_{n-1} (n-1) x^{n-2} + \dots + a_1$. Похідною від многочлена нульового степеня вважається нульовий многочлен.

Зрозуміло, що це означення похідної від многочлена співпадає з функціональним. Безпосередньо перевіряється, що похідна задовольняє властивостям:

- 1) $(f(x) + g(x))' = f'(x) + g'(x)$;
- 2) $(\alpha f(x))' = \alpha f'(x), \quad \alpha \in F$;
- 3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$;
- 4) $(f^k(x))' = k f^{k-1}(x) f'(x)$.

Лема 3 (про похідну). *Якщо незвідний многочлен $p(x)$ входить мно-
жником до многочлена $f(x)$ з кратністю k , то $p(x)$ входить до $f'(x)$
з кратністю $k - 1$.*

Доведення. За умовою $f(x) = p^k(x)g(x)$, де многочлен $g(x)$ не діли-
ться на многочлен $p(x)$, тоді $f'(x) = kp^{k-1}(x)p'(x)g(x) + p^k(x)g'(x) =$
 $p^{k-1}(x)(kp'(x)g(x) + p(x)g'(x))$. Зрозуміло, що $p^{k-1}(x)|f'(x)$. Залишає-
ться показати, що $f'(x)$ не ділиться на $p^k(x)$. Припустимо супротивне:
 $p^k(x)|f'(x)$, тоді $p(x)|(kp'(x)g(x) + p(x)g'(x))$, оскільки $p(x)|p(x)g'(x)$, то
 $p(x)|kp'(x)g(x)$, але $p(x)$ — незвідний многочлен і $g(x)$ не ділиться на
 $p(x)$ за умовою леми. Це означає, що $p(x)|kp'(x)$ але степінь $p'(x)$ мен-
ший степені $p(x)$. Приходимо до протиріччя. \square

Наслідок 3. *Якщо незвідний многочлен $p(x)$ входить до многочлена
 $f(x)$ з кратністю 1, то $f'(x)$ не ділиться на $p(x)$.*

Наслідок 4. *Якщо $\alpha p_1^{n_1}(x)p_2^{n_2}(x)\dots p_k^{n_k}(x)$ — канонічний розклад мно-
гочлена $f(x)$ в добуток незвідних множників, то $\text{НСД}(f(x), f'(x)) =$
 $p_1^{n_1-1}(x)p_2^{n_2-1}(x)\dots p_k^{n_k-1}(x)$.*

Наслідок 5. *Всі незвідні множники входять до канонічного розкладу
многочлена $f(x)$ з кратністю 1 тоді і тільки тоді, коли многочлени
 $f(x)$ і $f'(x)$ взаємнопрості.*

10. Відокремлення кратних множників

Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ — деякий многочлен
над полем F , причому степінь $f(x) \geq 1$.

Як відомо, цей многочлен можна розкласти в добуток незвідних мно-
жників над полем F . Нехай $f(x) = \alpha p_1^{n_1}(x)p_2^{n_2}(x)\dots p_k^{n_k}(x)$ — канонічний
розклад цього многочлена. Позначимо $s = \max(n_1, \dots, n_k)$, тобто s — це
максимальна кратність незвідного множника. Далі позначимо $X_1(x)$ —
добуток всіх незвідних множників кратності 1. Якщо таких немає, по-
кладемо $X_1(x) = 1$. Аналогічно $X_2(x)$ — добуток всіх незвідних множи-
ків кратності 2, причому кожен множник входить в цей добуток 1 раз.

Якщо таких множників немає, покладемо $X_2(x) = 1$, і так далі. $X_s(x)$ — добуток всіх незвідних множників кратності s , взятих по одному. Тоді зрозуміло, що $f(x) = \alpha X_1(x)X_2^2(x)\dots X_s^s(x)$. Множники $X_i(x)$, $i = \overline{1, s}$ називаються кратними множниками многочлена $f(x)$.

Наприклад, $f(x) = (x - 1)^3(x - 2)(x^2 + 3)^5(x - 4)^3(x + 3)$. Тоді $X_1(x) = (x-2)(x+3)$, $X_2(x) = 1$, $X_3(x) = (x-1)(x-4)$, $X_4(x) = 1$, $X_5(x) = (x^2+3)$. Задача відокремлення полягає в тому, щоб для даного многочлена $f(x)$ визначити множники $X_1(x), X_2(x), \dots, X_s(x)$, при цьому спочатку розклад многочлена $f(x)$ в добуток незвідних множників ми не знаємо. Основою методу є лема про похідну та її наслідки. З леми, зокрема, випливає таке твердження: якщо $f(x) = \alpha X_1(x)X_2^2(x)\dots X_s^s(x)$, то $\text{НСД}(f(x), f'(x)) = X_2(x)X_3^2(x)\dots X_s^{s-1}$.

Алгоритм відокремлення кратних множників

Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$, ст. $f(x) \geq 1$,
 $f(x) = \alpha X_1(x)X_2^2(x)\dots X_s^s(x)$.

- 1) Зрозуміло, що $d_1(x) = \text{НСД}(f(x), f'(x)) = \alpha_1 X_2(x)X_3^2(x)\dots X_s^{s-1}(x)$,
аналогічно $d_2(x) = \text{НСД}(d_1(x), d_1'(x)) = \alpha_2 X_3(x)X_4^2(x)\dots X_s^{s-2}(x)$,
...
 $d_{s-1}(x) = \text{НСД}(d_{s-2}(x), d_{s-2}'(x)) = \alpha_{s-1} X_s(x)$,
 $d_s = \text{НСД}(d_{s-1}(x), d_{s-1}'(x)) = d_s = \text{const.}$

- 2) $E_1(x) = \frac{f(x)}{d_1(x)} = \gamma_1 X_1(x)X_2(x)\dots X_s(x)$,
 $E_2(x) = \frac{d_1(x)}{d_2(x)} = \gamma_2 X_2(x)X_3(x)\dots X_s(x)$,
 $E_3(x) = \frac{d_2(x)}{d_3(x)} = \gamma_3 X_3(x)X_4(x)\dots X_s(x)$,
...
 $E_{s-1}(x) = \frac{d_{s-2}(x)}{d_{s-1}(x)} = \gamma_{s-1} X_{s-1}(x)X_s(x)$,
 $E_s(x) = \frac{d_{s-1}(x)}{d_s(x)} = \gamma_s X_s(x)$.

$$3) X_1(x) = \beta_1 \frac{E_1(x)}{E_2(x)}, \quad X_2(x) = \beta_2 \frac{E_2(x)}{E_3(x)}, \quad X_3(x) = \beta_3 \frac{E_3(x)}{E_4(x)}, \dots, \quad X_{s-1}(x) = \beta_{s-1} \frac{E_{s-1}(x)}{E_s(x)}, \quad X_s(x) = \beta_s E_s(x).$$

11. Кратність коренів многочлена

Нехай $f(x) \in F[x]$, якщо число $\alpha \in F$ є коренем цього многочлена, то за теоремою Безу $(x - \alpha) | f(x)$.

Означення 9. Корінь α ненульового многочлена $f(x)$ називають коренем кратності k , якщо $f(x)$ ділиться на $(x - \alpha)^k$ і не ділиться на $(x - \alpha)^{k+1}$. Корінь кратності 1 називають простим коренем, а корінь, кратність якого більша 1, часто називають кратним коренем.

Лема 4. Число коренів даного ненульового многочлена з урахуванням їх кратності не перевищує степені даного многочлена.

Доведення. Припустимо $\alpha_1, \alpha_2, \dots, \alpha_k$ — корені многочлена $f(x)$ кратності, відповідно, n_1, n_2, \dots, n_k . Многочлен $f(x)$ ділиться на многочлени $(x - \alpha_1)^{n_1}, (x - \alpha_2)^{n_2}, \dots, (x - \alpha_k)^{n_k}$, але всі многочлени $(x - \alpha_i)$ незвідні, тобто взаємнопрости. Тому $f(x)$ ділиться на добуток многочленів $(x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \dots (x - \alpha_k)^{n_k}$. Тобто $f(x) = (x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \dots (x - \alpha_k)^{n_k} g(x)$, а тому степінь $f(x) \geq n_1 + n_2 + \dots + n_k$. \square

12. Рівність многочленів

Означення 10. Два многочлена $f(x)$ і $g(x)$ називаються рівними в алгебраїчному розумінні, якщо рівні їх степені і відповідні коефіцієнти.

Нехай $f(x)$ — многочлен над полем F , тоді $\forall \alpha \in F : f(\alpha) \in F$, тобто многочлен є відображенням $f : F \rightarrow F$.

Означення 11. Два многочлена $f(x)$ і $g(x)$ вважають рівними аналітично, якщо вони рівні як відображення, тобто $\forall \alpha \in F : f(\alpha) = g(\alpha)$.

Теорема 4. Два многочлена $f(x)$ і $g(x)$ на полі F рівні алгебраїчно тоді і тільки тоді, коли вони рівні аналітично.

Доведення. Зрозуміло, якщо многочлени $f(x)$ і $g(x)$ рівні алгебраїчно то вони рівні аналітично.

Припустимо $f(x)$ і $g(x)$ рівні аналітично. Позначимо $n = \max(\text{ст.}f(x), \text{ст.}g(x))$. Оскільки числове поле F нескінченне, вибираємо в ньому $n + 1$ різних елементів $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$. Виконується $f(\alpha_i) = g(\alpha_i)$ $i = \overline{1, n+1}$. Позначимо $t(x) = f(x) - g(x)$. Степінь многочлена $t(x)$ не перевищує n і при цьому $t(\alpha_i) = 0$, $i = \overline{1, n+1}$. Тобто $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ — корені многочлена $t(x)$. Але за доведеним, ненульовий многочлен степені $\leq n$ має не більше ніж n коренів, тому $t(x)$ — нульовий многочлен і многочлени $f(x)$ і $g(x)$ рівні в алгебраїчному розумінні. \square

13. Незвідні многочлени над полем комплексних чисел

Нехай спочатку F довільне і $f(x) \in F[x]$. Припустимо, ст. $f(x) = 1$, $f(x) = ax + b$, $a \neq 0$, зрозуміло, що многочлен $f(x)$ незвідний над полем F . Многочлен 1-го степеня ще називають лінійним многочленом.

Нехай ст. $f(x) > 1$ і многочлен $f(x)$ в полі F має корінь α . Тоді за теоремою Безу, $f(x)$ ділиться на $(x - \alpha)$ і $f(x) = (x - \alpha)g(x)$, $g(x) \in F[x]$, ст. $g(x) \geq 1$, тобто многочлен $f(x)$ звідний в полі F . Припустимо, ст. $f(x) \geq 2$, але многочлен $f(x)$ не має коренів в полі F . Чи буде $f(x)$ незвідним над полем F ? Візьмемо наприклад $f(x) = (x^2 + 1)^2 = (x^2 + 1)(x^2 + 1)$. Многочлен $f(x)$ не має дійсних коренів, але є звідним над полем \mathbb{R} . З іншого боку, многочлен $x^2 + 1$ незвідний над полем \mathbb{R} . Таким чином, можна зробити такі висновки: многочлени першого степеня незвідні над будь-яким числовим полем. Якщо степінь $f(x) \geq 1$ і многочлен $f(x)$ має в полі F корінь, то $f(x)$ звідний над полем F . Якщо ст. $f(x) \geq 2$, але $f(x)$ не має коренів в полі F , то $f(x)$ може бути як звідним так і незвідним многочленом над полем F .

Теорема 5 (Гаусса, основна теорема алгебри). *Будь-який многочлен*

ненульового степеня з комплексними коефіцієнтами має комплексний корінь.

Наслідок 6. Будь-який многочлен ненульового степеня з комплексними коефіцієнтами можна розкласти в добуток лінійних множників, тобто многочленів першого степеня.

Доведення. Нехай $f(x) \in \mathbb{C}[x]$, ст. $f(x) \geq 1$. За умовою теореми $f(x)$ має комплексний корінь α_1 , а тому за теоремою Безу $f(x) = (x - \alpha_1)g(x)$. Якщо степінь $g(x) = 0$, все доведено, інакше проведемо аналогічні міркування для $g(x)$ і т.д. Оскільки на кожному кроці степінь $g(x)$ зменшується, то за скінченну кількість кроків ми приходимо до розв'язку. З цього, зокрема, випливає, що число всіх коренів $f(x)$ з урахуванням їх кратності рівне ст. $f(x)$. \square

Теорема 6. Незвідними над полем \mathbb{C} є всі многочлени 1-го степеня і лише вони.

Доведення. Нехай $f(x) \in \mathbb{C}[x]$. Якщо ст. $f(x) = 1$, то цей многочлен незвідний. Якщо ст. $f(x) > 1$, то цей многочлен можна розкласти в добуток многочленів поршого степеня, тобто многочлен $f(x)$ звідний. \square

14. Незвідні многочлени над полем дійсних чисел

Визначимо деякі типи незвідних многочленів над полем \mathbb{R} . Припустимо $f(x) \in \mathbb{R}[x]$, ст $f(x) = 1$. Такий многочлен $f(x)$ незвідний. Припустимо ст $f(x) = 2$, але многочлен $f(x)$ не має дійсних коренів. Такий многочлен також є незвідним над \mathbb{R} . Наша задача показати, що інших незвідних многочленів не буде.

Лема 5. Нехай $f(x)$ многочлен з дійсними коефіцієнтами ст. $f(x) > 1$ і α — комплексний корінь многочлена $f(x)$. Тоді число $\bar{\alpha}$ (спряжене) також є комплексним коренем многочлена $f(x)$.

Доведення. Спочатку випишемо деякі властивості комплексного спряження:

1) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.

Дійсно, нехай $z_1 = x_1 + y_1i$, $z_2 = x_2 + y_2i$, тоді $z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i$, $\overline{z_1} = x_1 - y_1i$, $\overline{z_2} = x_2 - y_2i$, $\overline{z_1 + z_2} = (x_1 + x_2) - (y_1 + y_2)i = \overline{z_1} + \overline{z_2}$.

2) $\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}$ аналогічно.

3) $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.

Нехай $z_1 = x_1 + y_1i$, $z_2 = x_2 + y_2i$, тоді $z_1 \cdot z_2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i$, $\overline{z_1} = x_1 - y_1i$, $\overline{z_2} = x_2 - y_2i$, $\overline{z_1} \cdot \overline{z_2} = (x_1 x_2 - y_1 y_2) - (x_1 y_2 + x_2 y_1)i = \overline{z_1 z_2}$.

4) $z_2 \neq 0 : \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}$ аналогічно.

Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{R}$. За умовою $f(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$. Звідси $0 = \overline{0} = \overline{(a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0)} = \overline{a_n \alpha^n} + \overline{a_{n-1} \alpha^{n-1}} + \dots + \overline{a_1 \alpha} + \overline{a_0} = a_n \overline{\alpha^n} + a_{n-1} \overline{\alpha^{n-1}} + \dots + a_1 \overline{\alpha} + a_0 = f(\overline{\alpha}) = 0$. \square

Теорема 7. *Незвідними над полем \mathbb{R} є многочлени першого степеня і многочлени 2-го степеня, які не мають дійсних коренів. Інших незвідних многочленів немає.*

Доведення. 1) Нехай ст. $f(x) = 1$, $f(x) \in \mathbb{R}[x]$. Тоді $f(x)$ — незвідний многочлен.

2) Нехай ст. $f(x) = 2$ і $f(x) \in \mathbb{R}[x]$ не має дійсних коренів. Тоді $f(x)$ — незвідний многочлен.

3) Нехай $f(x) \in \mathbb{R}[x]$, ст. $f(x) \geq 2$, $f(x)$ має дійсний корінь $\alpha \in \mathbb{R}$. Тоді за теоремою Безу $f(x) = (x - \alpha)g(x)$, $g(x) \in \mathbb{R}[x]$, ст $g(x) \geq 1$, тому $f(x)$ звідний многочлен.

4) Нехай $f(x) \in \mathbb{R}[x]$, ст. $f(x) > 2$ і $f(x)$ не має дійсних коренів. За основною теоремою алгебри многочлен $f(x)$ має комплексний корінь $\alpha \in \mathbb{C}$, $\alpha \notin \mathbb{R}$. За лемою $\bar{\alpha}$ також є коренем $f(x)$ і при цьому $\alpha \neq \bar{\alpha}$. Тоді многочлен $f(x)$ ділиться на $(x - \alpha)$ і $(x - \bar{\alpha})$. Оскільки $\alpha \neq \bar{\alpha}$, то $(x - \alpha)$ і на $(x - \bar{\alpha})$ незвідні над полем \mathbb{C} і взаємнопрости. А тому $f(x)$ ділиться на $g(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$, але числа $\alpha + \bar{\alpha}$ і $\alpha\bar{\alpha}$ дійсні, тобто $g(x)$ — многочлен з дійсними коефіцієнтами. Тому $f(x) = g(x)h(x)$, $h(x) \in \mathbb{R}[x]$ і ст. $h(x) \geq 1$, тобто многочлен $f(x)$ звідний над полем \mathbb{R} .

□

Зауваження 3. З цієї теореми, зокрема, випливає, що будь-який многочлен з дійсними коефіцієнтами можна розкласти в добуток лінійних многочленів і многочленів 2-го степеня, які є незвідними над полем \mathbb{R} .

Наслідок 7. *Нехай $f(x)$ многочлен з дійсними коефіцієнтами ст. $f(x) \geq 2$, α — комплексний корінь многочлена $f(x)$. Тоді число $\bar{\alpha}$ також є комплексним коренем $f(x)$ і кратності коренів α і $\bar{\alpha}$ співпадають.*

Доведення. З леми 5 випливає: якщо α — комплексний корінь $f(x)$, то $\bar{\alpha}$ — також комплексний корінь $f(x)$. Залишається довести, що їх кратності співпадають. Припустимо кратність $\alpha = k_1$, кратність $\bar{\alpha} = k_2$ і для визначеності припустимо $k_1 \geq k_2$. Нам треба показати, що $k_1 = k_2$. Припустимо супротивне: $k_1 > k_2$. Тоді многочлен $f(x)$ ділиться на $(x - \alpha)^{k_1}$ і на $(x - \bar{\alpha})^{k_2}$. Оскільки многочлени $(x - \alpha)$ і $(x - \bar{\alpha})$ є взаємнопростими, то $f(x)$ ділиться на добуток $(x - \alpha)^{k_1}(x - \bar{\alpha})^{k_2}$. Тобто $f(x) = (x - \alpha)^{k_1}(x - \bar{\alpha})^{k_2}f_1(x)$, де $f_1(x)$ не ділиться на $(x - \alpha)$ і на $(x - \bar{\alpha})$. Позначимо $g(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$. Многочлен $g(x)$ з дійсними коефіцієнтами і $f(x) = g^{k_2}(x)(x - \alpha)^{k_1 - k_2}f_1(x) = g^{k_2}(x)h(x)$, де $h(x) = (x - \alpha)^{k_1 - k_2}f_1(x)$ — многочлен з дійсними коефіцієнтами. При $k_1 > k_2$ число α є коренем $h(x)$. Але $h(x)$ не ділиться на $(x - \bar{\alpha})$, тобто $\bar{\alpha}$ не є коренем $h(x)$, що суперечить лемі 5. Отже $k_1 = k_2$.

□

Наслідок 8. *Будь-який многочлен з дійсними коефіцієнтами непарного степеня має принаймні 1 дійсний корінь.*

Доведення. Нехай ст. $f(x) = n$, n — непарне число. Тоді число всіх дійсних і комплексних коренів $f(x)$ з урахуванням їх кратності дорівнює n . З попереднього наслідку випливає, що число всіх комплексних коренів з урахуванням їх кратності парне, а тому є принаймні 1 дійсний корінь. \square

14.1. Розклад многочлена з дійсними коефіцієнтами в добуток незвідних множників

Припустимо $f(x)$ — деякий многочлен з дійсними коефіцієнтами, ст. $f(x) \geq 1$. Знаходимо корені $f(x)$. Припустимо дійсні корені $\alpha_1, \alpha_2, \dots, \alpha_m$ з відповідними кратностями k_1, k_2, \dots, k_m і комплексні корені $\beta_1, \overline{\beta_1}, \beta_2, \overline{\beta_2}, \dots, \beta_s, \overline{\beta_s}$ з відпоідними кратностями l_1, l_2, \dots, l_s .

Тоді над полем \mathbb{C} многочлен $f(x)$ можна розкласти у добуток $f(x) = a \prod_{i=1}^m (x - \alpha_i)^{k_i} \prod_{j=1}^s (x - \beta_j)^{l_j} (x - \overline{\beta_j})^{l_j}$. Позначимо через $g_j(x) = (x - \beta_j)(x - \overline{\beta_j})$, $j = \overline{1, s}$. Тоді многочлени $g_j(x)$ — це многочлени степеня 2, які незвідні над полем \mathbb{R} . А тому $f(x) = \alpha \prod_{i=1}^m (x - \alpha_i)^{k_i} \prod_{j=1}^s g_j^{l_j}(x)$ — шуканий розклад.

15. Звідні многочлени над полем \mathbb{Q} раціональних чисел

Будемо розв'язувати задачу пошуку раціональних коренів многочлена з раціональними коефіцієнтами

$$f(x) = q_n x^n + q_{n-1} x^{n-1} + \dots + q_1 x + q_0, \quad q_n, q_{n-1}, \dots, q_1, q_0 \in \mathbb{Q}.$$

Позначимо через q найменше спільне кратне знаменників чисел q_n, \dots, q_0 і домножимо многочлен $f(x)$ на число q . При цьому корені многочлена не змінюються, але ми одержали многочлен з цілими коефіцієнтами.

Таким чином, задача пошуку раціональних коренів многочлена з раціональними коефіцієнтами зводиться до пошуку раціональних коренів многочлена з цілими коефіцієнтами.

Теорема 8. *Нехай нескоротний дріб $\frac{p}{q}$ є коренем многочлена з цілими коефіцієнтами $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{Z}$. Тоді*

- 1) $p \mid a_0$;
- 2) $q \mid a_n$;
- 3) $(p - tq) \mid f(m)$, $\forall m \in \mathbb{Z}$.

Доведення. 1) За умовою $\frac{p}{q}$ є коренем $f(x)$, тобто

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \left(\frac{p}{q}\right) + a_0 = 0.$$

Домножимо цю рівність на q^n :

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \dots + a_1 p q^{n-1} + a_0 q^n = 0. \quad (15.1)$$

Звідси $a_0 q^n = -a_n p^n - a_{n-1} p^{n-1} q - a_{n-2} p^{n-2} q^2 - \dots - a_1 p q^{n-1}$.

Всі доданки в правій частині діляться на число p , а тому $p \mid a_0 q^n$.

Але дріб $\frac{p}{q}$ за умовою нескоротний, а тому p і q — взаємно прості числа. Звідси $p \mid a_0$.

- 2) Аналогічно з рівності (15.1) одержуємо:

$$a_n p^n = -a_{n-1} p^{n-1} q - \dots - a_1 p q^{n-1} - a_0 q^n.$$

Знову всі доданки в правій частині діляться на q , тому $q \mid a_n p^n$, і, оскільки, p і q взаємно прості, то $q \mid a_n$.

- 3) Перепишемо рівність (15.1) у вигляді:

$$a_n p^n + (a_{n-1} q) p^{n-1} + (a_{n-2} q^2) p^{n-2} + \dots + (a_1 q^{n-1}) p + a_0 q^n = 0.$$

Нехай $g(y)$ такий многочлен, що $g(y) = b_n y^n + b_{n-1} y^{n-1} + \dots + b_1 y + b_0$, де $b_n = a_n, b_{n-1} = a_{n-1} q, \dots, b_1 = a_1 q^{n-1}, b_0 = a_0 q^n$. Тоді многочлен

$g(y)$ з цілими коефіцієнтами. Із рівності (15.1) випливає, що p є коренем цього многочлена. Тоді за теоремою Безу $g(y) = (y - p)h(y)$, де $h(y)$ — многочлен з цілими коефіцієнтами. Коефіцієнти многочлена $h(y)$ можна знайти за допомогою, наприклад, схеми Горнера.

Тоді $\forall k \in \mathbb{Z} : g(k)$ і $h(k)$ — цілі числа. А тому $\forall k \in \mathbb{Z}, k \neq p : (k - p) \mid g(k)$. Припустимо, що $m \in \mathbb{Z}$. Оскільки p і q взаємно прості, то $mq \neq p$, а тому $(mq - p) \mid g(mq) \implies (p - mq) \mid g(mq)$. Якщо $q=1$, вибираємо $m \neq p$. Тоді

$$\begin{aligned} g(mq) &= b_n(mq)^n + b_{n-1}(mq)^{n-1} + b_{n-2}(mq)^{n-2} + \dots + b_1mq + b_0 = \\ &= a_n(mq)^n + a_{n-1}q(mq)^{n-1} + a_{n-2}q^2(mq)^{n-2} + \dots + a_1q^{n-1}mq + a_0q^n = \\ &= a_nm^nq^n + a_{n-1}m^{n-1}q^n + a_{n-2}m^{n-2}q^n + \dots + a_1mq^n + a_0q^n = \\ &= q^n(a_nm^n + a_{n-1}m^{n-1} + a_{n-2}m^{n-2} + \dots + a_1m + a_0) = q^n f(m) \implies \end{aligned}$$

$(p - mq) \mid q^n f(m)$. Покажемо, що числа $p - mq$ і q взаємно прості.

Припустимо, d — спільний дільник цих чисел: $d \mid q, d \mid mq$, оскільки $d \mid (p - mq) \implies d \mid p$, але числа p і q взаємно прості, тому $d=1$.

Тому з $(p - mq) \mid q^n f(m) \implies (p - mq) \mid f(m)$.

□

З останньої теореми випливає метод знаходження всіх раціональних коренів многочлена з цілими коефіцієнтами. Припустимо дано многочлен $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, \quad a_n, a_{n-1}, \dots, a_0 \in \mathbb{Z}$.

- 1) Знаходимо всі натуральні дільники числа $a_0 : p_1, p_2, \dots, p_k$.
- 2) Знаходимо всі натуральні дільники числа $a_n : q_1, q_2, \dots, q_s$.
- 3) Складемо всі можливі нескоротні дроби вигляду $\pm \frac{p_i}{q_j}$. Тоді всі раціональні корені многочлена $f(x)$ знаходяться серед цих дробів, тобто всі ці дроби є можливими раціональними коренями.
- 4) Якщо цих можливих коренів дуже багато, можна скоротити їх число перевіркою виконання умов $(p - mq) \mid f(m), \forall m \in \mathbb{Z}$. Наприклад, спочатку для $m = 1, m = -1 \implies p - q \mid f(1), p + q \mid f(-1)$. Всі дроби, які не задовільняють хоча б одній з цих умов, можна викреслити.

- 5) Якщо і після цього залишаться багато можливих коренів, можна перевірити ці випадки для $m = 2, m = -2, \dots$
- 6) Всі можливі корені, які залишаються, підставляємо у $f(x)$ і перевіряємо, наприклад, за схемою Горнера. Якщо деяке $x = \alpha \in \mathbb{C}$ є коренем, то $f(x) = (x - \alpha)g(x)$, де степінь $g(x) = \text{степені } f(x) - 1$. Користуючись схемою Горнера, ми одержимо $g(x)$, а тому наступні корені можна підставляти вже у $g(x)$.

16. Примітивні многочлени

Означення 12. Многочлен з цілими коефіцієнтами $f(x)$ називається примітивним, якщо НСД всіх його коефіцієнтів $= 1$.

Лема 6 (Гаусса). Добуток двох примітивних многочленів є примітивним многочленом.

Доведення. Нехай $f(x)$ і $g(x)$ — примітивні многочлени: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, де $a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{Z}$, НСД(a_n, a_{n-1}, \dots, a_0) = 1, $a_n \neq 0$; $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$, де $b_m, b_{m-1}, \dots, b_1, b_0 \in \mathbb{Z}$, НСД(b_m, b_{m-1}, \dots, b_0) = 1, $b_m \neq 0$.

Припустимо, $h(x) = f(x)g(x)$. $h(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{m+n} x^{m+n}$. Припустимо d — спільний дільник чисел c_0, \dots, c_{m+n} . Оскільки многочлени $f(x)$ і $g(x)$ — примітивні, то існують такі числа i та j , $0 \leq i \leq n, 0 \leq j \leq m$, що $d \mid a_0, d \mid a_1, \dots, d \mid a_{i-1}$ і a_i не ділиться на d ; $d \mid b_0, d \mid b_1, \dots, d \mid b_{j-1}$ і b_j не ділиться на d . Тоді $c_{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \dots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \dots + a_{i+j} b_0$. За припущенням, $d \mid c_{i+j}, d \mid a_0 b_{i+j}, d \mid a_1 b_{i+j-1}, \dots, d \mid a_{i-1} b_{j+1}, d \mid a_{i+1} b_{j-1}, d \mid a_{i+j} b_0$, а тому $d \mid a_i b_j$. Припустимо, d — просте число, тоді або $d \mid a_i$ або $d \mid b_j$, що суперечить припущенню. Таким чином $d = 1$ і многочлен $h(x)$ — примітивний. \square

17. Ознака Ейзенштейна

Лема 7. *Нехай многочлен $f(x)$ з цілими коефіцієнтами звідний над полем раціональних чисел. Тоді многочлен $f(x)$ можна розкласти в добуток 2-х многочленів ненульового степеня з цілими коефіцієнтами.*

Доведення. За умовою многочлен $f(x)$ звідний над полем \mathbb{Q} , тоді існують $g(x), h(x) \in \mathbb{Q}[x]$, такі що $f(x) = g(x)h(x)$, степінь $g(x) > 0$, степінь $h(x) > 0$. Позначимо через k найменше спільне кратне знаменників всіх коефіцієнтів многочлена $g(x)$, а l — найменше спільне кратне знаменників всіх коефіцієнтів многочлена $h(x)$. Тоді $f(x) = \frac{1}{kl}(kg(x))(lh(x)) = \frac{1}{m}g_1(x)h_1(x)$, де $g_1(x) = kg(x), h_1(x) = lh(x)$ — многочлени з цілими коефіцієнтами, $m = kl \in \mathbb{Z}$. Далі позначимо через c НСД всіх коефіцієнтів многочлена $g_1(x)$, а через q НСД всіх коефіцієнтів $h_1(x)$. Тоді $f(x) = \frac{cq}{m} \left(\frac{1}{c}g_1(x) \right) \left(\frac{1}{q}h_1(x) \right) = \frac{cq}{m}g_2(x)h_2(x) = \frac{r}{s}g_2(x)h_2(x)$, де $g_2(x) = \frac{1}{c}g_1(x), h_2(x) = \frac{1}{q}h_1(x)$ — многочлени з цілими коефіцієнтами і примітивні, $\frac{r}{s}$ — нескоротний дріб.

Покажемо, що $s = 1$. Оскільки многочлени $g_2(x), h_2(x)$ — примітивні, то за лемою Гаусса їх добуток $g_2(x)h_2(x)$ теж примітивний. Нехай $g_2(x)h_2(x) = \beta_n x^n + \beta_{n-1}x^{n-1} + \dots + \beta_1 x + \beta_0$, де $\beta_n, \dots, \beta_0 \in \mathbb{Z}$, НСД(β_n, \dots, β_0) = 1. Оскільки $f(x) = \frac{r}{s}g_2(x)h_2(x)$, то $f(x) = \frac{\beta_n r}{s}x^n + \frac{\beta_{n-1}r}{s}x^{n-1} + \dots + \frac{\beta_1 r}{s}x + \frac{\beta_0 r}{s}$. Але всі коефіцієнти многочлена $f(x)$ цілі, тому $s \mid \beta_n r, s \mid \beta_{n-1}r, \dots, s \mid \beta_1 r, s \mid \beta_0 r$. За припущенням дріб $\frac{r}{s}$ нескоротний, тому числа r і s — взаємно прості $\implies s \mid \beta_n, s \mid \beta_{n-1}, \dots, s \mid \beta_1, s \mid \beta_0$. Але многочлен $g_2(x)h_2(x)$ — примітивний, тому $s = 1$. Одержуємо $f(x) = rg_2(x)h_2(x), r \in \mathbb{Z}$, степінь $g_2(x)$ = степені $g(x) > 0$, степінь $h_2(x)$ = степені $h(x) > 0$. \square

Якщо деякий многочлен з цілими коефіцієнтами можна розкласти в добуток двох многочленів ненульового степеня з раціональними коефі-

ціентами, то його можна розкласти в добуток двох многочленів ненульового степеня з цілими коефіцієнтами.

Теорема 9 (ознака Ейзенштейна). *Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ — многочлен з цілими коефіцієнтами. Нехай для нього існує раціональне число p таке, що виконуються умови:*

1) $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}$ і a_n не ділиться на p ;

2) a_0 не ділиться на p^2 .

Тоді многочлен $f(x)$ незвідний над полем раціональних чисел.

Доведення. Згідно з останньою лемою достатньо показати, що многочлен $f(x)$ не можна розкласти в добуток двох многочленів ненульового степеня з цілими коефіцієнтами. Припустимо супротивне: $f(x) = g(x)h(x)$, $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$, $b_m, \dots, b_0 \in \mathbb{Z}, b_m \neq 0, 0 < m < n$; $h(x) = c_k x^k + c_{k-1} x^{k-1} + \dots + c_1 x + c_0$, $c_k, \dots, c_0 \in \mathbb{Z}, c_k \neq 0, 0 < k < n, m + k = n$.

Тоді виконується $a_0 = b_0 c_0, a_1 = b_0 c_1 + b_1 c_0, a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0, \dots, a_i = b_0 c_i + b_1 c_{i-1} + \dots + b_i c_0, \dots, a_n = b_m c_k$. За умовою $p \mid a_0 \implies p \mid b_0 c_0$, але p — просте число. Тому принаймі один з коефіцієнтів $b_0 c_0$ ділиться на p . Але a_0 не ділиться на p^2 , тому якщо $p \mid b_0$, то c_0 не ділиться на p і навпаки, якщо $p \mid c_0$, то b_0 не ділиться на p . Припустимо для визначеності, що $p \mid b_0$ і c_0 на p не ділиться. Тоді $p \mid a_1, p \mid b_0 c_1, p \mid b_1 c_0$ і, оскільки c_0 на p не ділиться, то $p \mid b_1$. Аналогічно отримуємо $p \mid b_2$ і т.д. За умовою $a_n = b_m c_k$ не ділиться на p , тобто b_m не ділиться на p . Тому існує такий номер i , що $p \mid b_0, p \mid b_1, \dots, p \mid b_{i-1}$, але b_i не ділиться на p .

$a_i = b_0 c_i + b_1 c_{i-1} + \dots + b_{i-1} c_1 + b_i c_0$. За умовою $p \mid a_i$, за припущенням $p \mid b_0, p \mid b_1, \dots, p \mid b_{i-1} \implies p \mid b_i c_0$, але c_0 не ділиться на p , тому $p \mid b_i$, що суперечить припущенню. Таким чином, многочлен $f(x)$ незвідний над полем \mathbb{Q} . \square

Зауваження 4. Ця ознака є тільки достатньою умовою того, що многочлен є незвідним над полем \mathbb{Q} .

Приклад 3. $f(x) = x^5 - 12x^3 + 36x - 12, p = 3$ — незвідний за ознакою Ейзенштейна.

Приклад 4. $f(x) = x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$ — виконується 1), але не виконується 2).

18. Границі дійсних коренів дійсних многочленів

Лема 8 (про старший член). *Нехай дано $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ — многочлен з дійсними коефіцієнтами. Тоді для $\forall k > 0$ існує $C > 0$, таке що, при $|x| \geq C$ виконується нерівність*

$$|a_n x^n| > k |a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0|. \quad (18.1)$$

Доведення. Позначимо $A = \max(|a_{n-1}|, |a_{n-2}|, \dots, |a_1|, |a_0|)$ та будемо вважати, що $|x| > 1$. Тоді виконується:

$$\begin{aligned} |a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0| &\leq |a_{n-1} x^{n-1}| + |a_{n-2} x^{n-2}| + \dots + |a_1 x| + |a_0| \\ &= |a_{n-1}| |x^{n-1}| + |a_{n-2}| |x^{n-2}| + \dots + |a_1| |x| + |a_0| \leq A (|x|^{n-1} + |x|^{n-2} + \dots + |x| + 1) \\ &= A \frac{|x|^n - 1}{|x| - 1}. \end{aligned}$$

Оскільки $|x| > 1$, то $\frac{|x|^n - 1}{|x| - 1} < \frac{|x|^n}{|x| - 1} \implies$

$$|a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0| < A \frac{|x|^n}{|x| - 1}.$$

Зафіксуємо число $k > 0$ і для доведення достатньо показати, що $\exists C > 0$, що при $|x| \geq C$ виконується $|a_n x^n| \geq \frac{kA|x|^n}{|x| - 1}$. $|a_n||x^n| \geq \frac{kA|x|^n}{|x| - 1}$ при

$$|a_n| \geq \frac{kA}{|x| - 1}. \text{ Враховуючи, що } |x| > 1, \text{ одержимо } (|x| - 1)|a_n| \geq kA \implies$$

$$|x| \geq 1 + \frac{kA}{|a_n|}. \text{ Зрозуміло, якщо виконується ця нерівність, то } |x| > 1, \text{ а}$$

тому беремо $C = 1 + \frac{kA}{|a_n|}$ і при $|x| \geq C$ виконується (18.1). \square

Наслідок 9. *Для \forall многочлена $f(x)$ з дійсними коефіцієнтами існує таке число $C > 0$, що при $|x| \geq C$ знак многочлена $f(x)$ визначається знаком його старшого члена.*

Лема про старший член дає можливість довести таку важливу теорему.

Теорема 10. Нехай β — дійсний корінь многочлена з дійсними коефіцієнтами $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$.

Якщо $A = \max(|a_{n-1}|, |a_{n-2}|, \dots, |a_1|, |a_0|)$, то виконується нерівність

$$|\beta| \leq 1 + \frac{A}{|a_n|}$$

Доведення. Припустимо, значення x таке, що $|x| \geq 1 + \frac{A}{|a_n|}$. Покладемо в умові леми про старший член $k = 1$. Тому, при такому значенні змінної x , модуль старшого члена $>$ модуля суми всіх інших членів, тобто x не може бути коренем многочлена, а тому $|\beta| \leq 1 + \frac{A}{|a_n|}$. \square

19. Число дійсних коренів дійсного многочлена на дійсному проміжку (теорема Штурма)

Зауваження 5. Теорема Штурма виконується лише для таких многочленів $f(x)$ з дійсними коефіцієнтами, які не мають кратних коренів, як дійсних, так і комплексних.

Припустимо, що $f(x)$ може мати кратні корені. Тоді неважко знайти такий многочлен $g(x)$ з дійсними коефіцієнтами, всі корені якого кратності 1 і співпадають з усіма коренями $f(x)$. Щоб позбавитись від кратних коренів у $f(x)$, достатньо його поділити на $d(x) = \text{НСД}(f(x), f'(x))$. Припустимо $\alpha_1, \alpha_2, \dots, \alpha_s$ — всі корені многочлена $f(x)$, як дійсні, так і комплексні, і k_1, k_2, \dots, k_s — кратності цих коренів. Тоді для $\forall i = \overline{1, s}$, $(x - \alpha_i)^{k_i} \mid f(x)$ і $f(x)$ не ділиться на $(x - \alpha_i)^{k_i+1}$.

Над полем комплексних чисел многочлен $f(x)$ можна розкласти в добуток $f(x) = \alpha(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \dots (x - \alpha_s)^{k_s}$. Тоді за лемою про похідну: $f'(x) = \beta(x - \alpha_1)^{k_1-1}(x - \alpha_2)^{k_2-1} \dots (x - \alpha_s)^{k_s-1} u(x)$, де $u(x)$ — взаємно простий з усіма $(x - \alpha_1), (x - \alpha_2), \dots, (x - \alpha_s)$.

Тоді $d(x) = \text{НСД}(f(x), f'(x)) = (x - \alpha_1)^{k_1-1}(x - \alpha_2)^{k_2-1} \dots (x - \alpha_s)^{k_s-1}$.

Звідси $g(x) = \frac{f(x)}{d(x)} = \alpha(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_s)$. Таким чином многочлен $g(x)$ має тільки прості корені і вони співпадають з усіма коренями $f(x)$.

Оскільки $f(x) \in R[x]$, то і $f'(x) \in R[x] \implies d(x) = \text{НСД}(f(x), f'(x)) \in$

$R[x]$, $g(x) = \frac{f(x)}{d(x)} \in R[x]$, тобто многочлен $g(x)$ з дійсними коефіцієнтами.

19.1. Поняття знакозміни в системі дійсних чисел

Нехай дано скінченну послідовність дійсних чисел: $-5, 3, 0, 10, -4, 2, -7, 0, 8$. Викреслюємо з цієї послідовності всі нулі і кожному числу ставимо у відповідність його знак: $- + + - + - +$. Будемо казати, що два числа в послідовності утворюють знакозміну, якщо вони стоять поруч і мають різні знаки, наприклад -5 і 3 . Число всіх таких пар будемо називати числом знакозмін в даній послідовності чисел (для нашої 5). Зрозуміло, що число знакозмін можна знайти для \forall скінченної впорядкованої послідовності дійсних чисел.

19.2. Система функцій Штурма

Нехай $f(x)$ — многочлен з дійсними коефіцієнтами, який не має кратних коренів, тобто $\text{НСД}(f(x), f'(x)) = 1$.

Означення 13. Упорядкована система дійсних многочленів $f_0(x), f_1(x), \dots, f_s(x)$ називається системою функцій Штурма многочлена $f(x)$, якщо виконуються умови:

- 1) $f_0(x) = f(x)$;
- 2) останній многочлен $f_s(x)$ не має дійсних коренів;
- 3) \forall пара суміжних многочленів в цій послідовності не має спільних коренів;
- 4) якщо $x = \alpha$ — дійсний корінь деякого проміжного многочлена $f_i(x)$, $0 < i < s$, то числа $f_{i-1}(\alpha), f_{i+1}(\alpha)$ різних знаків;
- 5) Якщо $x = \alpha$ — дійсний корінь многочлена $f_0(x)$ і ми рухаємось вздовж дійсної числової прямої зліва направо і проходимо точку $x = \alpha$, то при цьому добуток $f_0(x)f_1(x)$ змінює знак з мінуса на

плюс. Це означає, що в деякому околі $O_\varepsilon(\alpha)$ $f_0(x)$ має лише один корінь α і добуток $f_0(x)f_1(x)$ має знаки “–” при $x = \alpha - \varepsilon$, “+” при $x = \alpha + \varepsilon$.

19.3. Існування системи функцій Штурма

Припустимо $f(x)$ — многочлен з дійсними коефіцієнтами, який не має кратних коренів, тобто $\text{НСД}(f(x), f'(x)) = 1$. Для знаходження системи функцій Штурма будемо шукати НСД многочленів $f(x)$ та $f'(x)$ за допомогою алгоритма Евкліда. При цьому на кожному кроці залишок будемо брати з протилежним знаком.

1) За означенням покладемо $f_0(x) = f(x)$. Візьмемо $f_1(x) = f'(x)$ та виконаємо алгоритм Евкліда для $f_0(x)$, $f_1(x)$, тобто $f_0(x) = g_1(x)f_1(x) + r_1(x)$. Покладемо $f_2(x) = -r_1(x)$, а тому $f_0(x) = g_1(x)f_1(x) - f_2(x)$.

2) $f_1(x) = g_2(x)f_2(x) + r_2(x)$, $f_3(x) = -r_2(x)$,
 $f_1(x) = g_2(x)f_2(x) - f_3(x)$.

3) $f_2(x) = g_3(x)f_3(x) + r_3(x)$, $f_4(x) = -r_3(x)$,
 $f_2(x) = g_3(x)f_3(x) - f_4(x)$.

4) $f_3(x) = g_4(x)f_4(x) + r_4(x)$, $f_5(x) = -r_4(x)$,
 $f_3(x) = g_4(x)f_4(x) - f_5(x)$.

5) $f_4(x) = g_5(x)f_5(x) + r_5(x)$. Припустимо, $r_5(x) = \text{const} \neq 0$.

Тоді $f_6(x) = -r_5(x)$, $f_4(x) = g_5(x)f_5(x) - f_6(x)$.

Таким чином одержимо упорядковану систему многочленів:

$f_0(x), f_1(x), f_2(x), f_3(x), f_4(x), f_5(x), f_6(x)$. Покажемо, що ця система задовольняє умовам системи функцій Штурма.

1) Виконується $f_0(x) = f(x)$.

2) $f_6(x) = \text{const} = A \neq 0$, тобто останній многочлен не має дійсних коренів.

3) Припустимо для визначеності, що α — спільний корінь многочленів $f_2(x), f_3(x)$. Оскільки $f_1(x) = g_2(x)f_2(x) - f_3(x)$, то $f_1(\alpha) = 0$. Тобто α — спільний корінь многочленів $f_1(x), f_2(x)$, але $f_0(x) = g_1(x)f_1(x) - f_2(x)$, тому $f_0(\alpha) = 0$. Таким чином α — спільний корінь многочленів $f_0(x) = f(x), f_1(x) = f'(x)$. Тоді $(x - \alpha) \mid f(x), (x - \alpha) \mid f'(x)$, що суперечить умові НСД $(f(x), f'(x)) = 1$. Тобто умова 3) виконується.

4) Припустимо $x = \alpha$ — дійсний корінь многочлена $f_4(x)$. Тоді за властивістю 3) $f_3(\alpha) \neq 0, f_5(\alpha) \neq 0$. Треба показати, що числа $f_3(\alpha), f_5(\alpha)$ мають різні знаки.

$$f_3(x) = g_4(x)f_4(x) - f_5(x), f_3(\alpha) = g_4(\alpha)f_4(\alpha) - f_5(\alpha), f_3(\alpha) = -f_5(\alpha).$$

5) Припустимо $x = \alpha$ — дійсний корінь многочлена $f_0(x) = f(x)$. За властивістю 3) $f_1(\alpha) \neq 0$, а тому існує ε -окіл числа $\alpha O_\varepsilon(\alpha)$, можливо дуже маленький, в якому многочлен $f(x)$ має єдиний корінь α , а многочлен $f_1(x) = f'(x)$ зберігає свій знак. Припустимо для визначеності $f'(x) < 0 \forall x \in (\alpha - \varepsilon, \alpha + \varepsilon)$. Це означає, що функція $f(x)$ спадає на цьому проміжку і, оскільки, $f(\alpha) = 0$, то $f(\alpha - \varepsilon) > 0, f(\alpha + \varepsilon) < 0$. А тому при $x = \alpha - \varepsilon: f(x)f'(x) < 0$, а при $x = \alpha + \varepsilon: f(x)f'(x) > 0$. Аналогічно у випадку $f'(x) > 0, \forall x \in (\alpha - \varepsilon, \alpha + \varepsilon)$. Тобто ця умова виконується.

Таким чином, ми побудували систему функцій Штурма. Для даного многочлена існують й інші системи функцій Штурма.

19.4. Теорема Штурма

Припустимо $f_0(x), f_1(x), \dots, f_s(x)$ система функцій Штурма $f(x)$. Зафіксуємо дійсне число $x = \alpha$. Тоді одержимо послідовність дійсних чисел $f_0(\alpha), f_1(\alpha), \dots, f_s(\alpha)$. Число знакозмін в цій послідовності будемо позначати $W(\alpha)$.

Теорема 11 (Штурма). *Нехай $f(x)$ — многочлен з дійсними коефіцієнтами, який не має кратних коренів; a, b — дійсні числа, які не є*

коренями многочлена $f(x)$, i $a < b$; $f_0(x), f_1(x), \dots, f_s(x)$ — система функцій Штурма многочлена $f(x)$. Тоді $W(a) \geq W(b)$, і число дійсних коренів многочлена $f(x)$ на проміжку (a, b) дорівнює $W(a) - W(b)$.

Доведення. Для доведення достатньо визначити, як змінюється величина $W(x)$ при зростанні x . Якщо x зростає, але при цьому ми не проходимо через корінь якогось з многочленів системи функцій Штурма, то всі многочлени зберігають свої знаки, і величина $W(x)$ не змінюється. Тому достатньо розглянути 2 випадки:

1) Ми проходимо через дійсний корінь $x = \alpha$ деякого проміжного многочлена $f_i(x)$, $0 < i < s$.

2) Ми проходимо через деякий дійсний корінь $x = \alpha$ многочлена $f_0(x)$.

1) Розглянемо перший випадок $f_i(\alpha) = 0$. Тоді за властивістю системи функцій Штурма $f_{i-1}(\alpha) \neq 0$, $f_{i+1}(\alpha) \neq 0$ і $f_{i-1}(\alpha), f_{i+1}(\alpha)$ різних знаків. Тому існує деякий $O_\varepsilon(\alpha)$, в якому многочлен $f_i(x)$ має єдиний корінь α , а многочлени $f_{i-1}(x), f_{i+1}(x)$ зберігають свої знаки. Припустимо для $\forall x \in (\alpha - \varepsilon, \alpha + \varepsilon) : f_{i-1}(x) < 0, f_{i+1}(x) > 0$. Тоді, якщо, наприклад, $f_i(\alpha - \varepsilon) > 0$, то $f_i(\alpha + \varepsilon) < 0$. Отже знаки послідовності $f_{i-1}(\alpha - \varepsilon), f_i(\alpha - \varepsilon), f_{i+1}(\alpha - \varepsilon)$ такі: $- + +$, тобто в цій послідовності одна знакозмінна. В послідовності $f_{i-1}(\alpha + \varepsilon), f_i(\alpha + \varepsilon), f_{i+1}(\alpha + \varepsilon)$: $- - +$, також одна знакозмінна.

Аналогічно, якщо навпаки $f_i(\alpha - \varepsilon) < 0, f_i(\alpha + \varepsilon) > 0$, то знаки $f_{i-1}(\alpha - \varepsilon), f_i(\alpha - \varepsilon), f_{i+1}(\alpha - \varepsilon)$ такі: $- - +$, а знаки $f_{i-1}(\alpha + \varepsilon), f_i(\alpha + \varepsilon), f_{i+1}(\alpha + \varepsilon)$: $- + +$. Число знакозмін не змінюється. Тому якщо ми проходимо через деякий корінь многочлена $f_i(x)$, $0 < i < s$, то величина $W(x)$ не змінюється.

2) Припустимо, ми проходимо через корінь $x = \alpha$ многочлена $f_0(x) = f(x)$. Тоді, згідно з властивістю 3), $f_1(\alpha) \neq 0$, а тому існує інтервал $(\alpha - \varepsilon, \alpha + \varepsilon)$ на якому многочлен $f_0(x)$ має єдиний корінь α , а многочлен $f_1(x)$ зберігає свій знак.

Припустимо $\forall x \in (\alpha - \varepsilon, \alpha + \varepsilon) : f_1(x) > 0$, тоді за властивістю 5) $f_0(\alpha - \varepsilon) < 0$, $f_0(\alpha + \varepsilon) > 0$. Тому парі чисел $f_0(\alpha - \varepsilon)$, $f_1(\alpha - \varepsilon)$ відповідають знаки $-+$, а парі чисел $f_0(\alpha + \varepsilon)$, $f_1(\alpha + \varepsilon)$: $++$. Тобто в системі функцій Штурма при переході від $\alpha - \varepsilon$ до $\alpha + \varepsilon$ втрачається одна знакозміна. Аналогічно, якщо припустити, що $f_1(x) < 0 \forall x \in (\alpha - \varepsilon, \alpha + \varepsilon)$, то $f_0(\alpha - \varepsilon) > 0$, $f_0(\alpha + \varepsilon) < 0$. Числам $f_0(\alpha - \varepsilon)$, $f_1(\alpha - \varepsilon)$ відповідають знаки $+-$, а числам $f_0(\alpha + \varepsilon)$, $f_1(\alpha + \varepsilon)$: $--$. Тобто також втрачається одна знакозміна.

□

За допомогою теореми Штурма можна визначити число всіх дійсних коренів многочлена. Як відомо, можна знайти такий скінченний інтервал, на якому знаходяться всі корені даного многочлена, а тому можна використати теорему Штурма для цього інтервалу. Можна також це зробити по іншому.

Нехай $f(x)$ — многочлен з дійсними коефіцієнтами. З наслідку з леми про старший член випливає, що $\exists c > 0$, що при $|x| \geq c$ знаки всіх многочленів системи функцій Штурма визначаються їх старшими членами, а тому можна скористатися теоремою Штурма для інтервалу $(-c, c)$. Число c можна і не знаходити, формально припустивши, що $c = +\infty$. Тоді число всіх дійсних коренів дорівнює $W(-\infty) - W(+\infty)$, а знаки всіх многочленів на нескінченності визначаються їх старшими членами. Якщо визначити число $W(0)$, то число всіх від'ємних коренів дорівнюватиме $W(-\infty) - W(0)$, додатніх: $W(0) - W(+\infty)$.

Теорема Штурма дає можливість розв'язати задачу локалізації коренів, тобто визначити такі скінченні інтервали (α, β) , на кожному з яких знаходиться по одному і тільки одному кореню $f(x)$. За термінологією теореми Штурма це означає, що $W(\alpha) - W(\beta) = 1$, тобто на інтервалі (α, β) втрачається одна знакозміна.

20. Інтерполяційні многочлени

Нехай значення деякої функції $f(x)$ відомі в точках $x_0, x_1, x_2, \dots, x_n$, тобто $f(x_0) = y_0, f(x_1) = y_1, \dots, f(x_n) = y_n$. Стоїть задача наблизити функцію $f(x)$ многочленом $g(x)$, значення якого в точках $x_0, x_1, x_2, \dots, x_n$ співпало би з $y_0, y_1, y_2, \dots, y_n$. Ця задача носить назву задачі інтерполяції, а многочлен $g(x)$ називається інтерполяційним многочленом для $f(x)$. Неважко показати, що існує єдиний многочлен степеня $\leq n$, який задовольняє цим умовам.

Запишемо многочлен степеня n в загальному вигляді: $g(x) = a_0 + a_1x + \dots + a_nx^n$, і підберемо коефіцієнти a_0, a_1, \dots, a_n так, щоб виконувались умови задачі, тобто підставляємо

$$g(x_0) = a_0 + a_1x_0 + \dots + a_nx_0^n = y_0,$$

$$g(x_1) = a_0 + a_1x_1 + \dots + a_nx_1^n = y_1,$$

.....

$$g(x_n) = a_0 + a_1x_n + \dots + a_nx_n^n = y_n.$$

Одержали систему лінійних рівнянь відносно невідомих a_0, a_1, \dots, a_n . Ця система квадратна, тому випишемо визначник цієї системи. Одержимо визначник Вандермонда:

$$\Delta = \begin{vmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ & & \dots & & \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{vmatrix} = \prod_{i>j} (x_i - x_j)$$

та при різних значеннях x_i : $\Delta \neq 0$. Тобто система має єдиний розв'язок, а тому многочлен $g(x)$ визначений однозначно.

Інтерполяційний многочлен можна записувати в різних формах.

$$g_1(x) = C_0 + C_1(x-x_0) + C_2(x-x_0)(x-x_1) + \dots + C_n(x-x_0)(x-x_1) \dots (x-x_{n-1}). \quad (20.1)$$

Вважатимемо, що цей многочлен є інтерполяційним для функції $f(x)$ і визначимо його коефіцієнти. Оскільки $g_1(x_0) = y_0 \implies c_0 = y_0, g_1(x_1) = y_1 \implies y_1 = c_0 + c_1(x_1 - x_0) = y_0 + c_1(x_1 - x_0) \implies c_1 = \frac{y_1 - y_0}{x_1 - x_0}$ і т.д.

Многочлен (20.1) називається інтерполяційним многочленом Ньютона.

Випишемо такий многочлен:

$$g_2(x) = \sum_{i=0}^n y_i \frac{(x - x_0) \dots (x - x_{i-1})(x - x_{i+1}) \dots (x - x_n)}{(x_i - x_1) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x_i - x_n)}. \quad (20.2)$$

Зрозуміло, що виконується $g_2(x_i) = y_i$, $i = \overline{0, n}$. Многочлен (20.2) називається інтерполяційним многочленом Лагранжа.

Література

- [1] Чарін В.С. Лінійна алгебра. – К.: Техніка, 2004. – 416 с.
- [2] Курош А.Г. Курс высшей алгебры. – М.: Наука, 1965. – 360 с.
- [3] Фаддеев Д.К. Лекции по алгебре. – М.: Наука, 1984. – 416 с.
- [4] Винберг Э.Б. Курс алгебры. – М: Факториал Пресс, 2002. – 544 с.
- [5] Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. – М.: Наука, 1977. – 302 с.