Міністерство освіти і науки України

Прикарпатський національний університет

імені Василя Стефаника

Пилипів В.М., Заторський Р.А.,
Ліщинський І.І.

КІЛЬЦЕ ПОЛІНОМІВ

Івано-Франківськ — ЛІК

2023

УДК 512.622
ББК 22.144
П 32

Пилипів В.М., Заторський Р.А., Ліщинський І.І. Кільце поліномів: навчальний посібник (видання друге, доповнене). — Івано-Франківськ: ЛІК. — 2023. — 120 с.

В посібнику розглянуто алгебраїчні та функціональні аспекти теорії поліномів, описано структуру кільця поліномів над полем та його властивості. Матеріал насичений багатьма прикладами та вправами для самостійної роботи.

Посібник розроблено для користування студентами класичних, технічних та економічних університетів при вивченні алгебри та алгебраїчної частини вищої математики.

Рекомендовано Вченою радою факультету математики та інформатики Прикарпатського національного університету імені Василя Стефаника як навчальний посібник для студентів математичних спеціальностей закладів вищої освіти (протокол № 2 від 21 лютого 2023 р.).

Рецензенти: проф,, д.ф.-м.н. М.І. Дмитришин, завідувач кафедри диференціальних рівнянь та прикладної математики Прикарпатського національного університету імені Василя Стефаника;
проф., д.ф.-м.н. С.В. Шарин, професор кафедри математичного і функціонального аналізу Прикарпатського національного університету імені Василя Стефаника.

© Пилипів В.М., Заторський Р.А., Ліщинський І.І., 2023.

Зміст

КІЛЬЦЕ ПОЛІНОМІВ

Вступ

Посібник присвячено розгляду як алгебраїчного, так і функціонального аспектів теорії поліномів. Так, тут описано структуру кільця поліномів над полем та деякі його властивості (цілісність, ділення з остачею, існування коренів полінома тощо). З другого боку, детально розглянуто властивості похідної полінома та знаходження меж дійсних коренів полінома з дійсними коефіцієнтами. Крім того, в посібнику висвітлено деякі питання теорії поліномів від багатьох змінних та об'єкти, які з ними пов'язані (дискримінант та результант). Посібник завершується поверхневим розглядом поліномів розбиттів, що часто виникають у багатьох розділах математики.

Посібник розроблено для студентів класичних університетів, які навчаються за спеціальностями Математика, Статистика, Прикладна математика. Буде також корисним для студентів технічних та економічних напрямів при вивченні алгебраїчної частини вищої математики.

1 Кільце поліномів від однієї змінної

Поняття про поліноми (поліс - багато, номе - член (гр.)) та їх застосування зустрічаються на ранніх етапах розвитку алгебраїчної науки.

Початковий погляд на поліном від однієї змінної, як на функцію вигляду $f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$, задану на множині дійсних чисел, де коефіцієнти a_k $(k = 0, 1, \dots, n)$ - довільно вибрані дійсні числа (**функціональне** тлумачення полінома), є дещо вузьким, оскільки насправді коефіцієнтами полінома можуть бути елементи довільного кільця, зокрема, і нечислового (наприклад, кільця квадратних матриць, класів лишків за певним модулем тощо). У зв'язку з цим, загальна теорія поліномів ґрунтується на основі їх **алгебраїчного** тлумачення, яке зараз і буде розглянуте.

1.1 Побудова кільця поліномів

Нехай R - довільне комутативне кільце з одиницею.

Утворимо множину $\overline{R}$, елементами якої є нескінченні впорядковані послідовності $f = (f_0, f_1, f_2, ...)$, де $f_i \in R$, в яких всі члени, починаючи з деякого, дорівнюють нулю, і визначимо на ній операції додавання і множення. Позначивши дві довільні послідовності із множини $\overline{R}$ через $f = (f_0, f_1, f_2, ...)$, де $f_i \in R$, та $g = (g_0, g_1, g_2, ...)$, де $g_i \in R$, вважатимемо, що

$$f+g = (f_0, f_1, f_2, ...)+(g_0, g_1, g_2, ...) = (f_0+g_0, f_1+g_1, f_2+g_2, ...), \tag{1.1}$$

$f \cdot g = (f_0, f_1, f_2, ...) \cdot (g_0, g_1, g_2, ...) = u = (u_0, u_1, u_2, ...)$, де

$$u_k = \sum_{i+j=k} f_i g_j,\ k = 0, 1, 2, \dots \tag{1.2}$$

Із означення операцій додавання і множення елементів з $\overline{R}$, тобто деяких послідовностей, випливає, що результати цих операцій теж є послідовностями зі скінченною кількістю відмінних від нуля елементів з R, і, значить, формулами (1.1) і (1.2) на множині $\overline{R}$ визначаються бінарні операції додавання і множення.

Покажемо тепер, що *множина* $\overline{R}$ *із заданими на ній операціями додавання і множення утворює комутативне кільце з одиницею.*

Операція додавання елементів множини $\overline{R}$ є асоціативною і комутативною, оскільки зводиться до додавання відповідних елементів кільця R. Очевидним є існування в $\overline{R}$ нульового (нейтрального) елемента $(0, 0, 0, \dots)$ та протилежного (оберненого) до довільного елемента $f = (f_0, f_1, f_2, \dots)$ елемента $-f = (-f_0, -f_1, -f_2, \dots)$. Це дає підстави стверджувати, що $\overline{R}$ є абелевою адитивною групою.

Для доведення асоціативності операції множення виберемо три довільні елементи множини $\overline{R}$: $f = (f_0, f_1, f_2, \dots)$, де $f_i \in R$, $g = (g_0, g_1, g_2, \dots)$, де $g_j \in R$, $h = (h_0, h_1, h_2, \dots)$, де $h_k \in R$. Нехай $f \cdot g = u = (u_0, u_1, u_2, \dots)$, де $u_k = \sum\limits_{i+j=l} f_i g_j, l = 0, 1, 2, \dots$ Тоді $(f \cdot g)h = uh = q = (q_0, q_1, q_2, \dots)$, де $q_s = \sum\limits_{l+k=s} u_l h_k = \sum\limits_{l+k=s} (\sum\limits_{i+j=l} f_i g_j) h_k = \sum\limits_{i+j+k=s} f_i g_j h_k$. Аналогічний вираз отримаємо при обчисленні $f(g \cdot h)$. Отже, $\overline{R}$ є мультиплікативною півгрупою. Дистрибутивний закон $(f + g)h = fh + gh$ випливає із очевидної рівності:

$$\sum_{i+j=k} (a_i + b_i)c_j = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j,$$

звідки робимо висновок, що $\overline{R}$ є кільцем.

Комутативність операції множення елементів множини $\overline{R}$ випливає із симетричності виразу елементів u_k через f_i та g_j і комутативності операції множення в кільці R. Отже, $\overline{R}$ - кільце комутативне.

Роль одиничного елемента в множині $\overline{R}$ відіграє послідовність $e = (1, 0, 0, \dots)$, оскільки для довільного $f = (f_0, f_1, f_2, \dots)$ отримаємо, що $fe = ef = f$. Таким чином, $\overline{R}$ є комутативним кільцем з одиницею.

Те, що послідовності $(a, 0, 0, \dots) \in \overline{R}$ додаються і перемножуються так само, як елементи $a \in R$, дає можливість ототожнити такі послідовності з $\overline{R}$ із відповідними елементами з R, тобто для всіх $a \in R$ покласти $a = (a, 0, 0, \dots)$. Це означає, що кільце R ізоморфне деякій підмножині $\{(a, 0, 0, \dots), a \in R, +, \cdot\}$ кільця $\overline{R}$ (яка, значить, теж утворює кільце) і є підкільцем кільця $\overline{R}$.

Позначимо тепер елемент $(0, 1, 0, 0, \dots)$ кільця $\overline{R}$ символом x і назвемо його **змінною** (або **невідомою**) над R. Користуючись означенням операції множення на $\overline{R}$, отримаємо:

$$x = (0, 1, 0, 0, \dots),$$

$$x^2 = (0, 0, 1, 0, 0, \dots),$$

$$x^3 = (0, 0, 0, 1, 0, 0, \dots),$$

$$\dots$$

$$x^n = (0, 0, \dots, 0, 1, 0, 0, \dots)(\text{тут перед одиницею знаходяться n нулів}). \tag{1.3}$$

Із означення операції множення елементів з $\overline{R}$ і формул (1.3) матимемо:

$$(0, 0, \dots, 0, a, 0, 0, \dots) = (a, 0, 0, \dots)\cdot(0, 0, \dots, 0, 1, 0, 0, \dots) = ax^n.$$

Тоді для довільного елемента $f = (f_0, f_1, f_2, \ldots, f_n, 0, 0, \ldots)$ кільця $\overline{R}$ отримаємо:

$$\begin{aligned} f &= (f_0, f_1, f_2, \ldots, f_n, 0, 0, \ldots) = \\ &= (f_0, f_1, f_2, \ldots, f_{n-1}, 0, 0, \ldots) + f_n x^n = \\ &= (f_0, f_1, f_2, \ldots, f_{n-2}, 0, 0, \ldots) + f_{n-1}x^{n-1} + f_n x^n = \ldots \\ &= f_0 + f_1 x + f_2 x^2 + \cdots + f_{n-1}x^{n-1} + f_n x^n. \end{aligned} \tag{1.4}$$

Подання (1.4) елемента f є однозначним, оскільки $f_0, f_1, \ldots, f_n$ є членами послідовності $f = (f_0, f_1, \ldots, f_n, 0, 0, \ldots)$, а рівність двох послідовностей рівносильна рівності їх відповідних членів.

Таким чином, кільце $\overline{R}$ складається з елементів вигляду:

$$f = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n,$$

де $f_0, f_1, \ldots, f_n \in R$, n - ціле невід'ємне число, і при $n > 0$ $f_n \neq 0$.

Побудоване вище кільце $\overline{R}$ позначається символом $R[x]$ і називається **кільцем поліномів** *від змінної* x *над кільцем* R. Елементи кільця $R[x]$ називаються **поліномами (многочленами)** *від змінної* x *над кільцем* R і позначаються символами $f(x),\ g(x),\ h(x)$ тощо.

Елемент $x = (0, 1, 0, 0, \ldots)$ кільця $\overline{R}$ при викладеному вище алгебраїчному тлумаченні полінома називають "змінною x" за аналогією до його функціонального тлумачення, де поліном $f(x)$ розглядається як функція від змінної x.

Елементи $f_0, f_1, \ldots, f_n$ називають **коефіцієнтами** полінома $f(x)$. Поліном, всі коефіцієнти якого дорівнюють нулю, називають **нуль-поліномом** (позначається $\theta(x)$). Коефіцієнт f_0 при x в нульовому степені, називають **вільним** (сталим) **членом** (або **поліномом нульового степеня**). Коефіцієнт $f_n \neq 0$ називають **старшим коефіцієнтом**, $n = \deg f$ - **степенем** (*degree* – степінь (англ.)), а член $f_n x^n$

– **старшим членом** полінома. Поліном $f(x)$ називається **нормованим** (зведеним, унітарним), якщо його старший коефіцієнт дорівнює одиничному елементу кільця R.

Якщо позначити коефіцієнти $f_0, f_1, \dots, f_n$ через $a_0, a_1, \dots, a_n$, то запис полінома $f(x)$ набуде відомого вигляду:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n. \tag{1.5}$$

Звичним також є запис полінома $f(x)$ за спаданням степеня x, тобто у вигляді:

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n. \tag{1.6}$$

Форма запису полінома, в якому його члени упорядковані за спаданням (зростанням) степеня змінної x, називається **канонічною**. Вибір форми запису (1.5) чи (1.6) полінома $f(x)$ в подальшому розгляді залежатиме від зручності використання.

1.2 Дії над поліномами

Для розгляду операцій над елементами $R[x]$ в нових символах запишемо поліноми $f(x)$ та $g(x)$ за зростанням степеня змінної x:

$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n, a_n \neq 0,$$

$$g(x) = b_0 + b_1x + \dots + b_{m-1}x^{m-1} + b_mx^m, b_m \neq 0.$$

Поліноми $f(x)$ і $g(x)$ називаються **рівними** між собою ($f(x) = g(x)$), якщо рівні їх коефіцієнти при однакових степенях змінної x.

Відношення рівності поліномів є відношенням еквівалентності на множині $R[x]$ (має властивості рефлексивності, симетричності і транзитивності).

Запишемо тепер для множини $R[x]$ поліномів змінної x формули суми і добутку. Нехай $\deg f \geq \deg g \geq 0$.

Сумою поліномів $f(x)$ і $g(x)$ називається поліном

$$f(x) + g(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_{n-1} x^{n-1} + d_n x^n, \quad (1.7)$$

де $d_k = a_k + b_k,\ k = 0, 1, 2, \ldots, n,\ b_k = 0$ при $k > m$. Із означення суми двох поліномів $f(x)$ та $g(x)$ випливає:

$$\forall f(x), g(x) \in R[x] \Rightarrow \deg(f + g) \leq \max\{\deg f, \deg g\}.$$

Випадок $\deg(f + g) < \max\{\deg f, \deg g\}$ може статись при додаванні двох поліномів однакового степеня ($\deg f = \deg g$), коли їх старші коефіцієнти є протилежними елементами кільця R.

Добутком поліномів $f(x)$ і $g(x)$ називається поліном

$$f(x)g(x) = c_0 + c_1 x + \cdots + c_{n+m-1} x^{n+m-1} + c_{n+m} x^{n+m}, \quad (1.8)$$

де

$$c_k = \sum_{i+j=k} a_i b_j = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k,$$

$k = 0, 1, 2, \ldots, n + m$, тут $a_i = 0$ при $i > n, b_j = 0$ при $j > m$.

Зокрема,

$$\begin{aligned}
c_0 &= a_0 b_0, \\
c_1 &= a_1 b_0 + a_0 b_1, \\
&\ \ldots \\
c_{n+m-1} &= a_{n+m-1} b_0 + a_{n+m-2} b_1 + \cdots + a_{n+1} b_{m-2} + a_n b_{m-1} + \\
&\quad + a_{n-1} b_m + a_{n-2} b_{m+1} + \cdots + a_0 b_{m+n-1} = a_n b_{m-1} + a_{n-1} b_m, \\
c_{n+m} &= a_{n+m} b_0 + a_{n+m-1} b_1 + \cdots + a_{n+1} b_{m-1} + a_n b_m + \\
&\quad + a_{n-1} b_{m+1} + \cdots + a_0 b_{m+n} = a_n b_m.
\end{aligned}$$

Із означення добутку двох поліномів $f(x)$ та $g(x)$ випливає:

$$\forall f(x) \neq \theta(x), g(x) \neq \theta(x) \Rightarrow [\deg(fg) \leq \deg f + \deg g].$$

Дійсно, якщо старші коефіцієнти a_n та b_m є дільниками нуля в кільці R, то $c_{n+m} = a_n b_m = 0$, і, значить,

$$\deg(fg) < \deg f + \deg g.$$

Якщо ж старші коефіцієнти a_n та b_m не є дільниками нуля в кільці R (кільце R - цілісне), то $c_{n+m} = a_n b_m \neq 0$, і, значить,

$$\deg(fg) = \deg f + \deg g.$$

Із останнього висновку випливає наступне твердження: якщо R - цілісне кільце, то і кільце $R[x]$ поліномів від змінної x *є цілісним*.

1.3 Кільце поліномів

Перед розглядом будови (конструкції) кільця поліномів введемо деякі додаткові поняття.

В довільному комутативному кільці з одиницею A, що містить деяке ненульове підкільце (з одиницею) R, виберемо елемент t, який не належить R. Позначимо символом B перетин всіх таких підкілець кільця A, які містять підкільце R і елемент t (ясно, що B теж є підкільцем A). При такому виборі кільце B є мінімальним підкільцем кільця A, яке містить R і t. Вважають, що кільце B утворене приєднанням до кільця R елемента t і позначають $B = R[t]$.

Елемент t кільця A називається **алгебраїчним** відносно кільця R, якщо в кільці R існують елементи $a_0, a_1, a_2, \ldots, a_n$ (не всі з яких дорівнюють нулю), такі, що

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n = 0. \qquad (1.9)$$

Якщо ж рівність (1.9) виконується тільки при умові, що $a_0 = a_1 = a_2 = \cdots = a_n = 0$, то елемент t кільця A називається **трансцендентним** відносно кільця R.

Теорема 1.1. *Елемент* $x = (0, 1, 0, 0, \dots)$ *кільця* $R[x]$ *є трансцендентним відносно кільця* R.

Доведення. Дійсно, згідно формул (1.1) та (1.3) отримаємо:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = (a_0, 0, 0, \dots) + (0, a_1, 0, 0, \dots) + \cdots +$$

$$+ (0, 0, \dots, 0, a_n, 0, 0) = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots),$$

звідки випливає, що рівність

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

є рівносильною рівності

$$(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) = (0, 0, 0, \dots),$$

а, значить, виконується тільки при $a_0 = a_1 = a_2 = \cdots = a_n = 0$. Це й доводить трансцендентність елемента $x = (0, 1, 0, 0, \dots)$ відносно кільця R. □

Теорема 1.2. *Кільце поліномів* $R[x]$ *утворюється приєднанням до кільця* R *трансцендентного відносно* R *елемента* x.

Доведення. Для доведення досить показати, що в кільці $R[x]$ немає іншого підкільця, яке б містило R та x. Позначимо через B - підкільце кільця $R[x]$, в якому містяться кільце R і трансцендентний відносно R елемент x, а через $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ - довільно вибраний елемент кільця $R[x]$. Із того, що елементи $a_0, a_1, a_2, \ldots, a_n$, як елементи кільця R, містяться в підкільці B і $x \in B$, випливає, що й елемент $f(x)$ міститься в підкільці B. Отже, кожний елемент кільця $R[x]$ міститься в підкільці B і, значить, підкільце B співпадає із кільцем $R[x]$, що й вимагалось довести. $\square$

Вправи 1.3. *Виконати наступні дії над поліномами* $f(x) = 2x^5 - 3x^4 + x^2$ *та* $g(x) = -x^4 + x^3 + x - 1$*:*

(а) $f(x) + g(x)$;

(б) $f(x) - g(x)$;

(в) $f(x) + 2x \cdot g(x)$;

(г) $f(x) \cdot g(x)$.

2 Подільність в кільці поліномів

2.1 Подільність в цілісному кільці

При вивченні питання подільності поліномів вважатимемо, що комутативне кільце з одиницею R, над яким ми означили кільце поліномів, є полем, тобто що кожен елемент із R є оборотним. Кільце поліномів над полем F позначають $F[x]$. Перед викладом теорії подільності в кільці поліномів $F[x]$ розглянемо деякі загальні відомості теорії подільності в довільному цілісному кільці A.

Означення 2.1. *Елемент* $a \in A$ *ділиться на елемент* $b \in A$ *(або елемент* $b \in A$ *ділить елемент* $a \in A$*, або елемент* $a \in A$ *кратний* *елементу $b \in A$), якщо в цілісному кільці A існує такий елемент c, для якого $a = bc$. Позначається так: $a \vdots b$.*

Лема 2.2. *Якщо в комутативному кільці для елементів a, b, q, r виконується рівність $a = bq + r$, тоді $(a,b) = (b,r)$, (де (a,b) – найбільший спільний дільник елементів a і b).*

Доведення. Нехай $d = (a,b)$, $d_1 = (b,r)$. Оскільки $a \vdots d$ і $b \vdots d$, то із умови $a = bq + r$ випливає $r \vdots d$. Так як d – спільний дільник b і r, а d_1 - найбільший спільний дільник b і r, то $d_1 \vdots d$. Аналогічно і навпаки: $d \vdots d_1$. Звідси, $d = d_1$. □

Розглянемо випадок ділення поліномів націло (без остачі). Наведемо основні властивості такої подільності, доведення яких випливає з означення.

1. $\forall f(x),\ g(x),\ h(x) \in F[x] \left[f(x) \vdots g(x) \wedge g(x) \vdots h(x) \Rightarrow f(x) \vdots h(x) \right]$.

2. $\forall f(x),\ g(x),\ h(x) \in F[x]$
   $\left[f(x) \vdots h(x) \wedge g(x) \vdots h(x) \Rightarrow (f(x) \pm g(x)) \vdots h(x) \right]$.

3. $\forall f(x),\ h(x) \in F[x] \left[f(x) \vdots h(x) \Rightarrow \forall g(x) \in F[x]\ f(x)g(x) \vdots h(x) \right]$.

4. $\forall h(x),\ f_1(x), \dots, f_m(x) \in F[x]$
   $\left[f_1(x) \vdots h(x) \wedge f_2(x) \vdots h(x) \wedge \dots \wedge f_m(x) \vdots h(x) \Rightarrow \forall g_1(x), \dots, g_m(x) \in F[x]\ [f_1(x)g_1(x) + \dots + f_m(x)g_m(x)] \vdots h(x) \right]$.

5. $\forall f(x) \in F[x],\ c_{\neq 0} \in F \left[f(x) \vdots c \right]$.

6. $\forall f(x),\ g(x) \in F[x],\ c_{\neq 0} \in F \left[f(x) \vdots g(x) \Rightarrow f(x) \vdots cg(x) \right]$.

2.2 Ділення з остачею поліномів над полем

В загальному випадку два різні поліноми з $F[x]$ один на одного не діляться, тому для побудови теорії подільності в кільці $F[x]$ операцію ділення поліномів замінимо операцією ділення поліномів з остачею.

Теорема 2.3. *(Про ділення з остачею). Для довільних поліномів $f(x)$ та $g(x) \neq \theta(x)$ з кільця $F[x]$ в цьому кільці існує єдина пара поліномів $s(x)$ та $r(x)$, для яких*

$$f(x) = g(x)s(x) + r(x),$$

де $\deg r(x) < \deg g(x)$ *або* $r(x) = \theta(x)$.

Доведення. а) Можливість. Нехай

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m.$$

1. Якщо $f(x) = \theta(x)$, то $s(x) = \theta(x)$, $r(x) = \theta(x)$.
2. Якщо $\deg f(x) < \deg g(x)$, то $s(x) = \theta(x)$, $r(x) = f(x)$.
3. Нехай $\deg f(x) \geq \deg g(x)$. Скористаємося методом індукції за степенем полінома. При $n = 0$ матимемо $m = 0$, тому $f(x) = a_n$, $g(x) = b_m (\neq 0)$, звідки $s(x) = \frac{a_n}{b_m}$, $r(x) = \theta(x)$, де $s(x) \in F[x]$, оскільки $\frac{a_n}{b_m} \in F$ (саме тут врахована умова, що кільце, над яким ми розглядаємо кільце поліномів, є полем).

Припустимо, що теорема справедлива для всіх поліномів таких, що $\deg f(x) < n$, і доведемо її для поліномів степеня n. Утворимо поліном

$$f_1(x) = f(x) - \frac{a_0}{b_0}x^{n-m}g(x) \qquad (a_0, b_0 \neq 0).$$

Оскільки старший член полінома $\frac{a_0}{b_0}x^{n-m}g(x)$ дорівнює a_0x^n, тобто старшому члену полінома $f(x)$, то $\deg f_1(x) < n$ і, за припущенням індукції, $f_1(x)$ можна поділити з остачею на $g(x)$:

$$f_1(x) = f(x) - \frac{a_0}{b_0}x^{n-m}g(x) = g(x)s_1(x) + r_1(x),$$

де $s_1(x), r_1(x) \in F[x]$, причому $r_1(x) = \theta(x)$ або $\deg r_1(x) < \deg g(x)$, звідки

$$f(x) = g(x)s(x) + r(x),$$

де $r(x) = r_1(x) \in F[x], s(x) = s_1(x) + \frac{a_0}{b_0}x^{n-m} \in F[x]$ і $r(x) = \theta(x)$ або $\deg r(x) < \deg g(x)$. Можливість ділення $f(x)$ на $g(x)$ доведена.

б) Єдиність. Доведемо від супротивного. Допустимо можливість двох розкладів:

$$f(x) = g(x)s(x) + r(x), \deg r(x) < \deg g(x),$$

$$f(x) = g(x)s'(x) + r'(x), \deg r'(x) < \deg g(x).$$

Віднімемо їх:

$$g(x)[s(x) - s'(x)] = r'(x) - r(x).$$

Припустивши, що $r'(x) \neq r(x)$, отримаємо, що $s'(x) \neq s(x)$ (оскільки за умовою $g(x) \neq \theta(x)$ і кільце $F[x]$ не містить дільників нуля). Але тоді права частина останньої рівності буде поліномом степеня, меншого від $\deg g(x)$, і тому меншого від степеня лівої частини. Отримана суперечність заперечує припущення, тому $r'(x) = r(x)$, звідки і $s'(x) = s(x)$, що й доводить єдиність розкладу. Теорема доведена. □

Цілісне кільце, в якому має місце ділення з остачею, називають **евклідовим**.

Таким чином, на підставі поданого вище твердження про цілісність кільця поліномів та теореми про ділення з остачею поліномів над полем можна сформулювати висновок, що кільце поліномів $F[x]$ над полем F є евклідовим.

Викладений при доведенні теореми метод відшукання поліномів $s(x)$ та $r(x)$ для заданих поліномів $f(x)$ та $g(x)$ називається *алгоритмом ділення з остачею* і лежить в основі практичних способів ділення поліномів з остачею, які подамо нижче.

1. Алгоритм ділення з остачею лежить в основі відомого зі шкільної програми методу ділення поліномів "кутом суть якого зводиться до того, що спочатку від $f(x)$ віднімають $\frac{a_0}{b_0}x^{n-m}g(x)$, потім так само, як з $f(x)$, діють із поліномом-різницею $f_1(x)$ і так далі. Процес триває доти, поки не буде отримано поліном, степінь якого менший від $\deg g(x)$, який і буде остачею $r(x)$, а часткою $s(x)$ буде сума множників при $g(x)$, які виникали в процесі цього віднімання, тобто $\frac{a_0}{b_0}x^{n-m}, \ldots$.

Приклад 2.4. *1.* $f(x) = x^4 - x^3 + 3x^2 - 2$, $g(x) = x^2 + 1$.

$p_1(x) = f(x) - \frac{a_n}{b_m}x^{n-m}g(x)$.

$p_1(x) = (x^4 - x^3 + 3x^2 - 2) - x^2(x^2 + 1) = -x^3 + 2x^2 - 2$. *Далі так само.*

$p_2(x) = (-x^3 + 2x^2 - 2) - (-x)(x^2 + 1) = 2x^2 + x - 2$.

$p_3(x) = (2x^2 + x - 2) - 2(x^2 + 1) = x - 4$.

Степінь $p_3(x)$ *вже менший від степеня* $g(x)$. *Отже,*

$r(x) = p_3(x) = x - 4$. $s(x) = x^2 - x + 2$.

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

2. Суть методу невизначених коефіцієнтів, який теж використовується при діленні поліномів з остачею, полягає в тому, що, згідно

формули $f(x) = g(x)s(x) + r(x)$ про ділення з остачею, $s(x)$ записують у вигляді полінома з невизначеними коефіцієнтами степеня $n - m$, а $r(x)$ – степеня $m - 1$.

$x^4 - x^3 + 3x^2 - 2 = (x^2 + 1)s(x) + r(x)$, *де степінь* $s(x)$ *не може перевищувати* $n - m$ *(в цьому випадку 2), а степінь* $r(x)$ *менший від* $m = 2$*, тобто 1. Це означає, що* $s(x)$ *і* $r(x)$ *можна подати в канонічній формі так:* $s(x) = A_2x^2 + A_1x + A_0$*,* $r(x) = B_1(x) + B_0$*, де* $A_0,\ A_1,\ A_2,\ B_0,\ B_1$ *– невідомі коефіцієнти. Запишемо формулу ділення з остачею:*

$$x^4 - x^3 + 3x^2 - 2 = (x^2 + 1)(A_2x^2 + A_1x + A_0) + B_1(x) + B_0.$$

Згідно означення рівності поліномів коефіцієнти при однакових степенях рівні.

$A_2 = 1$, $A_1 = -1$, $A_2 + A_0 = 3$, $A_1 + B_1 = 0$, $A_0 + B_0 = -2$. *Звідси:* $A_1 = -1,\ A_2 = 1,\ A_0 = 2$, $B_0 = -4,\ B_1 = -1$. *Таким чином,* $s(x) = x^2 - x + 2$, $r(x) = x - 4$.

Вправи 2.5. *Поділити з остачею поліном* $f(x)$ *на* $g(x)$*, використовуючи:*

(а) *метод ділення "кутом";*

(б) *метод невизначених коефіцієнтів,*

якщо:

1) $f(x) = 2x^5 - x^4 + 3x^2 + 2x$, $g(x) = x^3 + 2x^2 - 3$.

2) $f(x) = x^5 - 2x^4 + x^3 + 2x^2 - x + 3$, $g(x) = 2x^2 + 3x - 5$.

3 Дільники полінома. Алгоритм Евкліда

3.1 НСД поліномів. Алгоритм Евкліда

Поліном $q(x)$, на який діляться поліноми $f(x)$ і $g(x)$, називається спільним дільником цих поліномів. Найбільшим спільним дільником (НСД) поліномів $f(x)$ і $g(x)$ називається спільний дільник $f(x)$ і $g(x)$, який ділиться на кожний інший їхній спільний дільник. Позначається $(f(x), g(x))$. НСД поліномів визначається неоднозначно, оскільки, якщо $d(x)$ - їх НСД, то і $c \cdot d(x)$ - їх НСД, тобто НСД поліномів визначається однозначно з точністю до сталого множника.

Розглянемо питання існування та знаходження найбільшого спільного дільника поліномів $f(x)$ і $g(x)$. Якщо обидва поліноми $f(x)$ і $g(x)$ є нуль-поліномами, то вважають, що їхній НСД дорівнює нулю або що НСД вони не мають. Якщо $f(x) = \theta(x)$, а $g(x) \neq \theta(x)$, то $(f(x), g(x)) = g(x)$. Надалі розглядатимемо випадок, коли $f(x)$ і $g(x)$ не є нуль-поліномами.

Доведемо тепер твердження, що в кільці $F[x]$ для довільних двох поліномів $f(x)$ і $g(x)$ існує їх найбільший спільний дільник, і вкажемо метод його практичного відшукання.

Нехай $\deg f(x) \geq \deg g(x)$. Виконаємо послідовне ділення з остачею.

$$f(x) = g(x) \cdot s_1(x) + r_1(x),$$

$$g(x) = r_1(x) \cdot s_2(x) + r_2(x),$$

$$r_1(x) = r_2(x) \cdot s_3(x) + r_3(x),$$

$$\dots,$$

$$r_{n-2}(x) = r_{n-1}(x) \cdot s_n(x) + r_n(x),$$

$$r_{n-1}(x) = r_n(x) \cdot s_{n+1}(x), \quad r_{n+1} = 0. \tag{3.1}$$

Процес триває до отримання нульової остачі. Послідовність степенів $\deg f, \deg g, \deg r_1, \deg r_2, \ldots$, як спадна послідовність натуральних чисел, мусить обірватися через скінченну кількість кроків. На основі леми 2.2: $(f, g) = (g, r_1) = (r_1, r_2) = \cdots = (r_n, 0) = r_n$. Таким чином, найбільший спільний дільник поліномів $f(x)$ і $g(x)$ є останньою ненульовою остачею в алгоритмі Евкліда (при діленні $f(x)$ на $g(x)$).

Приклад 3.1. *Обчислити НСД поліномів:*

$f(x) = x^3 - 2x^2 + x - 2$, $g(x) = x^3 - x^2 - 2x$.

Використаємо алгоритм Евкліда:

$$\begin{aligned}
&x^3 - 2x^2 + x - 2 = (x^3 - x^2 - 2x) \cdot 1 + (-x^2 + 3x - 2)\\
&x^3 - x^2 - 2x = (-x^2 + 3x - 2)(-x) + (2x^2 - 4x) =\\
&\qquad = (-x^2 + 3x - 2)(-x) + (-x^2 + 3x - 2)(-2) + 2x - 4 =\\
&\qquad = (-x^2 + 3x - 2)(-x - 2) + 2x - 4\\
&- x^2 + 3x - 2 = (2x - 4)(-\frac{x}{2} + \frac{1}{2}) + 0\\
&s_1(x) = 1,\ r_1(x) = -x^2 + 3x - 2\\
&s_2(x) = -x - 2,\ r_2(x) = 2x - 4\\
&s_3(x) = -\frac{x}{2} + \frac{1}{2},\ r_3(x) = 0
\end{aligned}$$

Отже, найбільший спільний дільник дорівнює $2x - 4$*, а з точністю до сталого множника* $x - 2$*.*

3.2 Наслідки з алгоритму Евкліда

Теорема 3.2. *Для будь-яких поліномів $f(x)$, $g(x)$ кільця $F[x]$ існує найбільший спільний дільник $d(x)$, причому $d(x)$ можна подати у вигляді*

$$d(x) = f(x) \cdot u(x) + g(x) \cdot v(x),$$

де $u(x)$,$v(x)$ - деякі поліноми з $F[x]$.

Доведення. Доведення випливає із запису (3.1) алгоритму Евкліда при безпосередньому вираженні $d(x) = r_n(x)$ через $r_{n-1}(x)$ і $r_{n-2}(x)$, потім через $r_{n-2}(x)$ і $r_{n-3}(x)$, і т.д., через $r_2(x)$ і $r_1(x)$, через $r_1(x)$ і $g(x)$, і, нарешті, через $f(x)$ і $g(x)$ (для цього в схемі (3.1) доведеться виконати $(n-1)$ послідовних підставлянь). Належність утворених поліномів $u(x)$ і $v(x)$ до кільця $F[x]$ випливає із їх побудови. □

Теорема 3.3. *НСД поліномів $f_1(x), f_2(x), f_3(x), \ldots, f_n(x)$ дорівнює НСД полінома $f_n(x)$ і НСД поліномів $f_1(x), f_2(x), \ldots, f_{n-1}(x)$. Скорочений запис має вигляд:*

$$(f_1, f_2, \ldots, f_n) = ((f_1, f_2, \ldots, f_{n-1}), f_n).$$

Доведення. При $n = 2$ твердження теореми очевидне. Припустимо його справедливість для $(n-1)$ (≥ 2) поліномів і доведемо, що воно справедливе і для n поліномів. Нехай $d^*(x)$ є НСД поліномів $f_1(x),\ f_2(x), \ldots,\ f_{n-1}(x)$ (який, згідно припущення, існує). Позначимо через $d(x)$ НСД поліномів $d^*(x)$ і $f_n(x)$ і покажемо, що $d(x)$ і є НСД поліномів $f_1(x), f_2(x), \ldots, f_n(x)$. Дійсно, оскільки $d^*(x)$ ділиться на $d(x)$, то, за відомою властивістю подільності в довільному кільці, кожний із поліномів $f_1(x),\ f_2(x), \ldots,\ f_{n-1}(x)$ теж ділиться на $d(x)$, звідки випливає, що $d(x)$ є спільним дільником поліномів $f_1(x),\ f_2(x), \ldots,\ f_{n-1}(x),\ f_n(x)$. Крім того, довільний інший спільний дільник поліномів $f_1(x),\ f_2(x), \ldots,\ f_{n-1}(x),\ f_n(x)$ теж буде спільним дільником поліномів $d^*(x)$ і $f_n(x)$, а, значить, і їх найбільшого спільного дільника $d(x)$, тобто, $d(x)$ є найбільшим із спільних дільників поліномів $f_1(x),\ f_2(x), \ldots,\ f_{n-1}(x),\ f_n(x)$, що й вимагалось довести. □

Практично найбільший спільний дільник великої кількості поліномів $f_1(x), f_2(x), \ldots, f_n(x)$ знаходять так: $d_1(x) = (f_1, f_2), d_2(x) = (d_1, f_3), d_3(x) = (d_2, f_4), \ldots, d_{n-1}(x) = (d_{n-2}, f_n)$. $d_{n-1}(x)$ і є найбільшим спільним дільником всіх цих поліномів.

Означення 3.4. *Поліноми $f(x)$ та $g(x)$ кільця $F[x]$ називаються взаємно простими, якщо кожний їхній спільний дільник є поліномом нульового степеня (відмінним від нуля елементом поля F). Позначається: $(f, g) = c$ або $(f, g) = 1$.*

Якщо які-небудь два з поліномів $f_1(x), f_2(x), \ldots, f_n(x)$ є взаємно простими, то найбільший спільний дільник цих поліномів дорівнює одиниці.

Теорема 3.5. *Поліноми $f(x)$ і $g(x)$ кільця $F[x]$ є взаємно простими тоді і тільки тоді, коли в цьому кільці існують поліноми $u(x)$ і $v(x)$, такі, що*

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1.$$

Доведення. Необхідність. Із того, що поліноми $f(x)$ і $g(x)$ кільця $F[x]$ є взаємно простими, випливає, що їх НСД $(f, g) = d(x) = 1$, звідки із врахуванням твердження теореми 3.2 отримаємо, що $f(x) \cdot u(x) + g(x) \cdot v(x) = d(x) = 1$.

Достатність. Із того, що в кільці $F[x]$ існують поліноми $u(x)$ та $v(x)$, для яких виконується рівність $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$, випливає, що поліноми $f(x)$ і $g(x)$ є взаємно простими, тобто не мають спільних дільників, відмінних від поліномів нульового степеня, оскільки якщо б вони мали деякий спільний дільник $q(x)$ ненульового степеня, то ліва частина рівності $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$, а, значить, і права її частина (елемент 1), мали б ділитися на $q(x)$, що неможливо. $\square$

Властивості взаємно простих поліномів

1. $\forall f(x), g(x), h(x) \in F[x] \ \big[(f, g) = 1 \wedge (f, h) = 1 \Rightarrow (f, gh) = 1\big]$.

Помноживши рівність $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$ на $h(x)$, отримаємо $f(x)[u(x) \cdot h(x)] + [g(x) \cdot h(x)]v(x) = h(x)$, звідки видно, що кожний спільний дільник $q(x)$ полінома $f(x)$ і добутку $g(x) \cdot h(x)$ був би також дільником і для полінома $h(x)$. Оскільки за умовою $f(x)$ і $h(x)$ не мають спільних дільників, відмінних від полінома нульового степеня, то $f(x)$ і $g(x) \cdot h(x)$ також спільних дільників, відмінних від полінома нульового степеня, не мають, тобто, поліноми $f(x)$ і $g(x) \cdot h(x)$ є взаємно простими.

2. $\forall f(x), g(x), h(x) \in F[x] \ [f(x) \cdot g(x) \vdots h(x) \wedge (f, h) = 1 \Rightarrow g(x) \vdots h(x)]$.

Згідно умови $(f, h) = 1$ в кільці $F[x]$ існують поліноми $u(x)$ та $v(x)$, для яких $f(x) \cdot u(x) + h(x) \cdot v(x) = 1$. Помноживши цю рівність на $g(x)$, отримаємо $[f(x) \cdot g(x)]u(x) + h(x)[v(x) \cdot g(x)] = g(x)$. Із того, що обидва доданки лівої частини рівності діляться на $h(x)$, випливає, що й права її частина $g(x)$ ділиться на $h(x)$.

3. $\forall f(x), g(x), h(x) \in F[x]$ $[f(x) \vdots g(x) \wedge f(x) \vdots h(x) \wedge (g,h) = 1 \Rightarrow f(x) \vdots g(x)h(x)]$.

Із умови $f(x) \vdots g(x)$ випливає існування в кільці $F[x]$ такого полінома $t(x)$, що $f(x) = g(x) \cdot t(x)$. Умову $f(x) \vdots h(x)$ подамо тепер у вигляді: $g(x) \cdot t(x) \vdots h(x)$. Оскільки $(g,h) = 1$, то, згідно попередньої властивості, $t(x) \vdots h(x)$, тобто $t(x) = h(x) \cdot t^*(x)$, де $t^*(x) \in F[x]$. Звідси, $f(x) = [g(x) \cdot h(x)]t^*(x)$, тобто $f(x) \vdots g(x)h(x)$.

Властивості 1-3 поширюються на довільну скінченну систему поліномів.

3.3 НСК поліномів

Означення 3.6. *Поліном $s(x)$, який ділиться на поліноми $f(x)$ і $g(x)$, називається* **спільним кратним** *цих поліномів.* **Найменшим спільним кратним** *поліномів $f(x)$ і $g(x)$ називається спільне кратне цих поліномів, на яке ділиться будь-яке їх спільне кратне.*

Доведемо тепер твердження про існування в кільці $F[x]$ для довільних двох відмінних від нуля поліномів $f(x)$ і $g(x)$ найменшого спільного кратного, і вкажемо метод його обчислення.

Теорема 3.7. *Для будь-яких відмінних від нуля поліномів $f(x)$ і $g(x)$ з кільця $F[x]$ найменше спільне кратне існує і визначається однозначно з точністю до сталого множника.*

Доведення. Розглянемо поліном $s(x) = \frac{f(x) \cdot g(x)}{(f,g)}$. Із рівності $s(x) = \frac{f(x)}{(f,g)} g(x) = \frac{g(x)}{(f,g)} f(x)$ випливає, що $s(x)$ - спільне кратне $f(x)$ і $g(x)$. Доведемо, що $s(x)$ - найменше спільне кратне. Якщо $h(x)$ - довільне інше спільне кратне поліномів $f(x)$ і $g(x)$, то $h(x) \vdots f(x)$ і

$h(x) \vdots g(x)$, тому $h(x) = h_1(x) \cdot f(x)$, причому $h_1(x) \cdot f(x) \vdots g(x)$, тобто $\frac{h_1(x) \cdot f(x)}{g(x)} = p(x)$ - поліном з $F[x]$.

Подамо тепер $f(x)$ і $g(x)$ у вигляді:

$$f(x) = (f, g) \cdot f_1(x), \; g(x) = (f, g) \cdot g_1(x),$$

де $f_1(x), g_1(x)$ - поліноми з $F[x]$, причому $(f_1, g_1) = 1$. Тоді $p(x) = \frac{h_1(x) f_1(x)(f,g)}{g_1(x)(f,g)} = \frac{h_1(x) f_1(x)}{g_1(x)}$. Оскільки $(f_1, g_1) = 1$, то $h_1(x) \vdots g_1(x)$. Введемо означення $\frac{h_1(x)}{g_1(x)} = t(x) \in F[x]$, одержимо $h_1(x) = g_1(x) \cdot t(x)$, звідки $h(x) = h_1(x) \cdot f(x) = f(x) \cdot g_1(x) \cdot t(x) = \frac{f(x)g(x)}{(f,g)} t(x) = s(x) \cdot t(x)$, тобто $h(x) \vdots s(x)$.

Отже, довільне спільне кратне $h(x)$ ділиться на спільне кратне $s(x)$. Тому $s(x) = [f(x), g(x)] = \frac{f(x)g(x)}{(f,g)}$ і є найменшим спільним кратним поліномів $f(x)$ і $g(x)$. $\square$

Вправи 3.8. *Для поліномів* $f(x) = 2x^4 - 3x^3 + x^2 - 2x + 2$ *та* $g(x) = x^3 - 4x^2 + 3x$ *знайти:*

(а) найбільший спільний дільник $d(x)$*;*

(б) такі поліноми $u(x)$ *та* $v(x)$*, щоб виконувалась рівність* $f(x)u(x) + g(x)v(x) = d(x)$*;*

(в) найменше спільне кратне.

4 Незвідні поліноми над полем

4.1 Незвідні поліноми та їх властивості

Означення 4.1. *Поліном ненульового степеня* $f(x)$ *з кільця* $F[x]$ *називається* **незвідним** *у кільці* $F[x]$ *(або незвідним над полем* F*),* *якщо він не ділиться на жодний поліном* $g(x) \in F[x]$, *у якого* $0 < \deg g(x) < \deg f(x)$.

Поліном $f(x) \in F[x]$ *називається* **звідним** *у кільці* $F[x]$ *(над полем* F*), якщо він ділиться на деякий поліном* $g(x) \in F[x]$, *у якого* $0 < \deg\ g(x) < \deg f(x)$, *тобто якщо його можна подати у вигляді добутку двох поліномів додатного степеня із* $F[x]$.

Таким чином, будь-який поліном додатного степеня є або звідним, або незвідним у даному полі, тобто, звідність і незвідність полінома є відносними поняттями, які залежать від самого поля F, над яким цей поліном розглядається.

На відміну від властивості звідності, величина найбільшого спільного дільника поліномів не залежить від того, над яким полем ці поліноми розглядаються.

Приклади 4.2. *1. Поліном* $x^2 - 2$ *незвідний в полі* $\mathbb{Q}$ *- раціональних чисел, але звідний в полях* $\mathbb{R}$ *і* $\mathbb{C}$ *- дійсних і комплексних чисел.*

2. Поліном $x^2 + 2$ *незвідний в полях* $\mathbb{Q}$, $\mathbb{R}$, *проте звідний в полі* $\mathbb{C}$.

Нуль-поліном і поліноми нульового степеня не відносяться ні до звідних, ні до незвідних поліномів. Поліном першого степеня над довільним полем F є над цим полем незвідним, оскільки не може мати дільників, степінь яких більший за 0 і менший за 1.

Властивості незвідних поліномів

1. Якщо поліном $p(x)$ *є незвідним над полем* F, *то і* $c \cdot p(x)$ *є над цим полем незвідним (*c *- довільний ненульовий елемент поля* F*).*

Дійсно, із припущення, що поліном $c \cdot p(x)$ є звідним над полем F, тобто має в кільці $F[x]$ дільники, степінь яких більший нуля і менший від степеня $c \cdot p(x)$, випливає, що ці ж дільники є також дільниками полінома $p(x)$, що суперечить умові його незвідності і підтверджує неправильність припущення.

2. Якщо $p(x)$ - незвідний у полі F поліном, а $f(x)$ - довільний поліном над цим полем, то або $f(x)$ ділиться на $p(x)$, або $f(x)$ і $p(x)$ є взаємно простими.

$(f(x), p(x)) = d(x)$ є дільником незвідного полінома $p(x)$, тобто $\deg d(x) = 0$ або $\deg d(x) = \deg p(x)$, звідки $d(x) = c$ або $d(x) = c \cdot p(x)$, де $c \neq 0$, а це означає, що або $f(x)$ і $p(x)$ - взаємно прості, або $f(x)$ ділиться на $p(x)$.

3. Якщо незвідний в полі F поліном $p(x)$ ділиться на інший, незвідний в полі F, поліном $q(x)$, то ці поліноми збігаються з точністю до сталого множника.

Із того, що $p(x)$ ділиться на $q(x)$, тобто $p(x)$ і $q(x)$ мають спільний дільник $q(x)$, випливає, що $p(x)$ і $q(x)$ не є взаємно простими, а оскільки $p(x)$ - незвідний, то $q(x)$ (за попередньою властивістю) має на нього ділитися, тому з того, що $p(x)$ ділиться на $q(x)$, матимемо, що $q(x)$ ділиться на $p(x)$, звідси поліноми $p(x)$ і $q(x)$ - збігаються з точністю до сталого множника.

4. Якщо добуток поліномів $f_1(x)$ і $f_2(x)$ з кільця $F[x]$ ділиться на незвідний поліном $p(x)$, то хоча б один із цих поліномів ділиться на $p(x)$.

Якщо $f_1(x)$ не ділиться на незвідний поліном $p(x)$, то (за властивістю 2) $f_1(x)$ і $p(x)$ є взаємно простими і, значить, на $p(x)$ ділиться $f_2(x)$.

Властивість 4 поширюється на добуток довільної кількості поліномів.

4.2 Розклад полінома в добуток незвідних множників

Теорема 4.3. *Довільний поліном $f(x)$ ненульового степеня з кільця $F[x]$ розкладається на незвідні множники над полем F однозначно з точністю до сталого множника.*

Доведення. Необхідно довести можливість і єдиність існування (з точністю до сталого множника) розкладу

$$f(x) = p_1(x) \cdot p_2(x) \cdots p_k(x), \tag{4.1}$$

де $p_1(x), p_2(x), \dots, p_k(x)$ - незвідні поліноми над полем F.

Скористаємось методом математичної індукції за степенем полінома. Для незвідного над полем F полінома $f(x)$ твердження теореми справедливе, оскільки шуканий добуток складається з єдиного множника $f(x)$. Це означає, що теорема справедлива для всіх поліномів першого степеня, які є незвідними над довільним полем.

Припустимо справедливість теореми для довільного полінома, степінь якого більший за 1 і менший за n, і доведемо її справедливість для довільного полінома степеня n. Якщо поліном $f(x)$ степеня n з кільця $F[x]$ є незвідним над полем F, то теорема справедлива. Якщо поліном $f(x)$ звідний над полем F, то $f(x) = f_1(x) \cdot f_2(x)$, де $f_1(x)$ і $f_2(x)$ - поліноми з кільця $F[x]$, степені яких більші від нуля і менші від n. Поліноми $f_1(x)$ і $f_2(x)$, за припущенням, розкладаються в добуток деяких поліномів, незвідних над полем F, тобто

$$f_1(x) = p_1(x) \cdot p_2(x) \cdots p_r(x), \quad f_2(x) = p_{r+1}(x) \cdot p_{r+2}(x) \cdots p_s(x),$$

звідки $f(x) = p_1(x) \cdot p_2(x) \cdots p_r(x) \cdot p_{r+1}(x) \cdot p_{r+2}(x) \cdots p_s(x)$. Отже, теорема справедлива і для випадку полінома степеня n.

Для доведення другої частини теореми припустимо, що існує два розклади полінома $f(x)$ на незвідні множники:

$$f(x) = p_1(x)p_2(x)\dots p_k(x),\;\; f(x) = q_1(x)q_2(x)\dots q_s(x),\;\; (k \le s).$$

За властивістю 4 незвідних поліномів хоча б один з поліномів $p_i(x)$ ділиться на $q_1(x)$. Не зменшуючи загальності, нехай це буде $p_1(x)$. Але тоді за властивістю 3 маємо, що $q_1(x) = c_1 p_1(x)$ де $c_1 \in F$. Отже, рівність $p_1(x)p_2(x)\dots p_k(x) = q_1(x)q_2(x)\dots q_s(x)$ можна скоротити на $p_1(x)$ і отримаємо $p_2(x)\dots p_k(x) = c_1 q_2(x)\dots q_s(x)$. Проводячи дальше аналогічні міркування, приходимо до висновку, що $k = s$ (бо в супротивному випадку $k < s$, і можна прийти до рівності $1 = c_1 \dots c_k q_{k+1}(x)\dots q_s(x)$, яка не має змісту), тому поліноми $p_i(x)$ відрізняються від поліномів $q_i(x)$ хіба що сталими множниками. □

У зв'язку з можливою повторюваністю незвідних множників $p_i(x)$, де $i = 1, 2, \dots, k$, в розкладі $f(x) = p_1(x)\cdot p_2(x)\cdots p_k(x)$, останній можна записати у вигляді

$$f(x) = [p_1(x)]^{k_1}\cdot[p_2(x)]^{k_2}\cdots[p_m(x)]^{k_m}, \tag{4.2}$$

де $p_i(x)$ - попарно різні поліноми (неасоційовані), незвідні в полі F. Це зображення єдине з точністю до сталого множника.

Зображення (4.2) називається **канонічним розкладом** полінома $f(x)$ у полі F. Поліном $p_i(x)$, який входить до канонічного розкладу в степені з показником k_i, називають **множником кратності** k_i полінома $f(x)$. Множники, кратність яких більша за одиницю, називають *кратними множниками* полінома. Інакше: незвідний множник $p_i(x)$ називається множником *кратності* k_i полінома $f(x)$, якщо $f(x)$ ділиться на $[p_i(x)]^{k_i}$, але не ділиться на $[p_i(x)]^{k_i+1}$.

5 Корені поліномів

5.1 Корені та лінійні множники полінома. Теорема Безу

Якщо $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ - довільний поліном над полем F , а c - деякий елемент поля F, то вираз

$$f(c) = a_0c^n + a_1c^{n-1} + \cdots + a_{n-1}c + a_n$$

називається значенням полінома $f(x)$ при $x = c$.

Означення 5.1. *Коренем полінома $f(x) \in F[x]$ називається елемент α поля F (або деякого його розширення) такий, що $f(\alpha) = 0$.*

Поняття кореня полінома тісно пов'язане з подільністю полінома на лінійний біном (двочлен).

Теорема 5.2. *(Безу) Для будь-якого елемента c із поля F остача при діленні полінома $f(x) \in F[x]$ на $(x - c)$ дорівнює $f(c)$.*

Доведення. Згідно теореми про ділення поліномів з остачею, $f(x) = g(x) \cdot s(x) + r(x)$. В нашому випадку $f(x) = (x - c)s(x) + r(x)$, де $\deg r(x) < \deg(x - c) = 1$, тобто $r = const$. Тоді $f(c) = (c - c) \cdot s(c) + r = r$. □

Наслідок 5.3. *Елемент $\alpha \in F$ є коренем полінома $f(x) \in F[x]$ тоді і тільки тоді, коли $f(x)$ ділиться на $(x - \alpha)$.*

Доведення. Дійсно, якщо α є коренем полінома $f(x)$, тобто $f(\alpha) = 0$, то, згідно теореми Безу, $r = f(\alpha) = 0$ і, значить, $f(x)$ ділиться на $(x - \alpha)$. І навпаки, якщо $f(x)$ ділиться на $(x - \alpha)$, то $r = f(\alpha) = 0$, тобто α є коренем $f(x)$. □

Згідно останнього твердження можна дати ще одне означення кореня полінома.

Означення 5.4. *Коренем полінома* $f(x) \in F[x]$ *називається елемент* α *, якщо* $f(x) \vdots (x-\alpha)$.

Перше означення пов'язане із *функціональною* сутністю полінома $f(x)$, а друге - з *алгебраїчною.* Таким чином, якщо α є коренем полінома, то $(x-\alpha)$ є дільником цього полінома, тобто задача знаходження коренів полінома рівносильна задачі знаходження лінійних дільників цього полінома. У зв'язку з цим розглянемо простий спосіб ділення полінома $f(x)$ на лінійний біном $(x-c)$.

5.2 Схема Горнера

При розгляді важливого випадку ділення полінома на лінійний біном $(x-c)$ використаємо метод невизначених коефіцієнтів:

$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = (x-c)(A_0x^{n-1} + A_1x^{n-2} + \dots + A_{n-2}x + A_{n-1}) + r$, де r - константа. Прирівнявши коефіцієнти при однакових степенях змінної

$$\begin{array}{rcl} a_0 = A_0 & & A_0 = a_0 \\ a_1 = A_1 - cA_0 & & A_1 = a_1 + cA_0 \\ \dots & \Rightarrow & \dots \\ a_{n-1} = A_{n-1} - cA_{n-2} & & A_{n-1} = a_{n-1} + cA_{n-2} \\ a_n = r - cA_{n-1} & & r = a_n + cA_{n-1}, \end{array} \tag{5.1}$$

отримаємо просту схему ділення полінома на лінійний біном $(x-c)$ (**схему Горнера**), суть якої така: кожний наступний коефіцієнт A_k частки і остача r отримуються множенням c на обчислений раніше коефіцієнт A_{k-1} і додаванням до знайденого добутку відповідного коефіцієнта a_k полінома.

	a_0	a_1	a_2	a_3	$\cdots$	a_{n-1}	a_n
c	A_0	cA_0+a_1	cA_1+a_2	cA_2+a_3	$\cdots$	$cA_{n-2}+a_{n-1}$	$cA_{n-1}+a_n$
	A_0	A_1	A_2	A_3	$\cdots$	A_{n-1}	r

Приклад 5.5. *Поділити* $f(x) = 2x^4 + x^3 - 3x^2 - 2$ *на* $g(x) = x + 2$.

	2	1	-3	0	-2
-2	2	$-2 \cdot 2+1$	-2·(-3)+(-3)	-2·3+0	-2·(-6)+(-2)
	2	-3	3	-6	10

Отже, частка $s(x) = 2x^3 - 3x^2 + 3x - 6$, *остача* $r = 10$.

За допомогою багаторазового ділення полінома $f(x)$ на лінійний біном $(x - c)$ можна отримати розклад $f(x)$ за степенями $(x - c)$, який широко використовується в математиці та її прикладних розділах. Дійсно, $f(x) = (x - c) \cdot f_{n-1}(x) + r_n$, де $f_{n-1}(x)$ - поліном $(n - 1)$ степеня з $F[x]$, а r_n - елемент з поля F. Аналогічно

$$f_{n-1}(x) = (x - c)f_{n-2}(x) + r_{n-1},$$

$$f_{n-2}(x) = (x - c)f_{n-3}(x) + r_{n-2},$$

$$\cdots$$

$$f_1(x) = (x - c)f_0(x) + r_1,$$

$f_1(x)$ - поліном першого степеня, $f_0(x)$ - поліном нульового степеня (позначимо його $f_0(x) = r_0$). Після виключення $f_{n-1}(x)$, $f_{n-2}(x)$, $\ldots$, $f_2(x)$, $f_1(x)$, отримаємо:

$$f(x) = r_0(x - c)^n + r_1(x - c)^{n-1} + \ldots + r_{n-1}(x - c) + r_n. \quad (5.2)$$

Таким чином, щоб розкласти поліном за степенями $(x - c)$, треба знайти остачі r_i:

r_n – остача від ділення $f(x)$ на $(x-c)$,

r_{n-1} – остача від ділення першої частки $f_{n-1}(x)$ на $(x-c)$,

r_{n-2} – остача від ділення другої частки $f_{n-2}(x)$ на $(x-c)$, і так далі,

r_0 – остання частка в процесі ділення.

Приклад 5.6. *Розкласти поліном* $f(x) = 2x^4 + x^3 - 3x^2 - 2$ *за степенями лінійного двочлена* $x-1$.

	2	*1*	*-3*	*0*	*-2*
1	*2*	*3*	*0*	*0*	*-2*
1	*2*	*5*	*5*	*5*	
1	*2*	*7*	*12*		
1	*2*	*9*			
1	*2*				

У першому рядку таблиці – коефіцієнти полінома $f(x)$

У другому рядку – коефіцієнти першої частки і остача $r_0 = -2$.

У третьому – коефіцієнти ділення першої частки на $x-1$ *і остача* $r_1 = 5$*, і т.д.*

Отже, $f(x) = 2(x-1)^4 + 9(x-1)^3 + 12(x-1)^2 + 5(x-1) - 2$.

5.3 Кількість коренів полінома

Елемент α називається k **- кратним коренем** полінома $f(x) \in F[x]$, якщо $f(x)$ ділиться на $(x-\alpha)^k$, але не ділиться на $(x-\alpha)^{k+1}$.

Зрозуміло, що α є k - кратним коренем полінома $f(x) \in F[x]$ тоді і тільки тоді, коли $f(x) = (x-\alpha)^k \cdot g(x)$, де $g(x)$ - поліном над $F[x]$, для якого α не є коренем. Ясно, що $\deg g(x) = \deg f(x) - k$, звідки $k \leq \deg f(x)$.

Теорема 5.7. *Кількість всеможливих коренів полінома $f(x)$ над полем F не перевищує степеня полінома.*

Доведення. Для поліномів нульового степеня теорема справедлива, оскільки жоден з них не має коренів. Нехай в полі F довільний поліном $f(x)$ ненульового степеня має наступні корені: α_1 - кратності $k_1, \alpha_2 - k_2, \ldots, \alpha_m - k_m$, причому $\alpha_i \neq \alpha_j$ при $i \neq j$. Тоді, згідно означення кратного кореня, матимемо $f(x) = (x - \alpha_1)^{k_1} \cdot g_1(x)$, де $g_1(x)$ не ділиться на $(x-\alpha_1)$. Із того, що $f(x)$ ділиться на $(x-\alpha_2)^{k_2}$, а $(x - \alpha_1)^{k_1}$ взаємно простий з $(x - \alpha_2)^{k_2}$, випливає, що $g_1(x)$ ділиться на $(x-\alpha_2)^{k_2}$, тобто $g_1(x) = (x-\alpha_2)^{k_2} \cdot g_2(x)$, де поліном $g_2(x)$ не ділиться на $(x - \alpha_2)$. Звідси $f(x) = (x - \alpha_1)^{k_1} \cdot (x - \alpha_2)^{k_2} \cdot g_2(x)$. Продовжуючи і далі аналогічні міркування або ж застосовувавши метод математичної індукції, отримаємо $f(x) = (x - \alpha_1)^{k_1} \cdot (x - \alpha_2)^{k_2} \cdot \cdots \cdot (x - \alpha_m)^{k_m} \cdot g_m(x)$, де $g_m(x)$ - поліном, для якого жодне із α_i не є коренем. Із останньої рівності видно, що $\deg f = n = k_1 + k_2 + \cdots + k_m + \deg g_m$, тобто $k_1 + k_2 + \cdots + k_m \leq n$. □

Наслідок 5.8. *Якщо поліном $f(x) \in F[x]$ степеня, не вищого за n, має $(n+1)$ різних коренів, то $f(x)$ є нуль-поліномом.*

Цей же наслідок сформулюємо інакше: *якщо два поліноми $f(x)$ і $g(x) \in F[x]$ степеня, не вищого за n, приймають однакові значення при $(n+1)$ різних значеннях x з поля F, то вони рівні між собою.*

Доведення. Нехай $f(\alpha_i) = g(\alpha_i) = \beta_i$, де $i = 1, 2, \ldots, n+1$. Припустимо супротивне, тобто $f(x) \neq g(x)$. Тоді для полінома-різниці $h(x) = f(x) - g(x)$ виконуватимуться наступні рівності: $h(\alpha_i) = 0$ для всіх $i = 1, 2, \ldots, n+1$, тобто $h(x)$ є ненульовим поліномом, степінь якого не перевищує n, і який, за умовою, має в полі F більше ніж n коренів, що суперечить висновку теореми 5.7 і заперечує припущення. $\square$

Це означає, що серед поліномів степеня, не вищого за n, існує не більше одного полінома, який приймає наперед задані значення $\beta_i \in F$ при $n+1$ різних значеннях $\alpha_1, \ldots, \alpha_{n+1}$ змінної x з поля F.

5.4 Поліноміальні функції

Наслідок із теореми 5.7 дає можливість розв'язати питання про співвідношення функціональної і алгебраїчної точок зору на поліноми. Кожному поліному $f(x) \in F[x]$ ставиться у відповідність функція $f^* : a \to f(a), \forall a \in F$. Множина всіх таких функцій утворює кільце F^* *поліноміальних функцій.*

Теорема 5.9. *Якщо F - цілісне кільце з нескінченною кількістю елементів, то відображення $f \to f^*$ кільця поліномів $F[x]$ на кільце поліноміальних функцій F^* є ізоморфізмом.*

По суті, це твердження є переформулюванням наслідку теореми 5.7, оскільки мова йде тільки про те, що ненульовому поліному $f(x)$ ставиться у відповідність ненульова функція f^*, тобто $f(a) \neq 0$ хоча б для одного $a \in F$. Насправді $f(x)$ має не більше, ніж n коренів в F, якщо $\deg f(x) = n$.

Таким чином, кільце поліномів над нескінченним полем F ототожнюють із кільцем поліноміальних функцій, і залишається тільки встановити, як за f^* (а насправді за кількома значеннями полінома f) відновити в явному вигляді сам поліном.

Точна постановка задачі відновлення (інтерполяції) полягає у необхідності знаходження полінома $f(x)$ степеня, не вищого за n, який при $(n+1)$ різних значеннях $x = \alpha_i \in F$ приймає задані значення $\beta_i \in F$ $(i = 1, 2, \ldots, n+1)$. Наслідок із теореми 5.7 стверджує про єдиність такого полінома. Залишилось підтвердити існування такого полінома.

Розглянемо наступний поліном:

$$\begin{aligned} f(x) = {} & \frac{(x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_{n+1})}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_{n+1})}\beta_1 + \\ & + \frac{(x-\alpha_1)(x-\alpha_3)\ldots(x-\alpha_{n+1})}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_{n+1})}\beta_2 + \\ & + \frac{(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_{i-1})(x-\alpha_{i+1})\ldots(x-\alpha_{n+1})}{(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\ldots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\ldots(\alpha_i-\alpha_{n+1})}\beta_i + \\ & + \cdots + \frac{(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)}{(\alpha_{n+1}-\alpha_1)(\alpha_{n+1}-\alpha_2)\ldots(\alpha_{n+1}-\alpha_n)}\beta_{n+1} \end{aligned} \tag{5.3}$$

Усі члени побудованого полінома є поліномами n-го степеня. Із виразу полінома видно, що при $x = \alpha_i$ його i-ий член перетворюється в β_i, а всі інші - в 0. Таким чином, i-ий член приймає значення β_i тільки при одному значенні x, яке дорівнює α_i (оскільки при всіх інших значеннях x: $f(x) \neq \beta_i$). Отже, $f(x)$ і є шуканим поліномом.

Поліном (5.3) називається **інтерполяційним поліномом Лагранжа**. За $(n+1)$ значеннями полінома степеня, не вищого за n, можна знайти всі його значення.

Деякі переваги інколи має ще одна очевидна формула полінома - **інтерполяційний поліном Ньютона**:

$$\begin{aligned} f(x) = {} & c_0 + c_1(x-\alpha_1) + c_2(x-\alpha_1)(x-\alpha_2) + c_3(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) + \\ & + \cdots + c_n(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \end{aligned} \tag{5.4}$$

де коефіцієнти $c_0, c_1, \ldots, c_n$ визначаються шляхом послідовного підставляння значень $x = \alpha_i$, тобто

$f(\alpha_1) = c_0,$

$f(\alpha_2) = c_0 + c_1(\alpha_2 - \alpha_1),$

$f(\alpha_3) = c_0 + c_1(\alpha_3 - \alpha_1) + c_2(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$, і так далі.

Інтерполяційні методи є важливим практичним інструментом досліджень в багатьох розділах математики та інших наук.

Приклад 5.10. *Побудувати поліном $f(x)$ не вище 3 степеня над полем $\mathbb{Q}$, якщо $f(-1) = -7$, $f(0) = -1$, $f(1) = 1$, $f(2) = 5$.*

Формула Лагранжа:

$$f(x) = \frac{(x-0)(x-1)(x-2)}{(-1-0)(-1-1)(-1-2)} \cdot (-7) + \frac{(x+1)(x-1)(x-2)}{(0+1)(0-1)(0-2)} \cdot (-1) +$$

$$+ \frac{(x+1)(x-0)(x-2)}{(1+1)(1-0)(1-2)} \cdot 1 + \frac{(x+1)(x-0)(x-1)}{(2+1)(2-0)(2-1)} \cdot 5 = x^3 - 2x^2 + 3x - 1.$$

Формула Ньютона:

$-7 = f(-1) = c_0;\ \ c_0 = -7.$

$-1 = f(0) = c_0 + c_1(0 - (-1)) = -7 + c_1;\ \ c_1 = 6.$

$1 = f(1) = c_0 + c_1(1-(-1)) + c_2(1-(-1))(1-0) = 5 + 2c_2;\ \ c_2 = -2.$

$5 = f(2) = c_0 + c_1(2-(-1)) + c_2(2-(-1))(2-0) + c_3(2-(-1))(2-0)(2-1) =$

$-1 + 6c_3;\ c_3 = 1.$

$f(x) = -7 + 6(x-(-1)) - 2(x-(-1))(x-0) + (x-(-1))(x-0)(x-1) =$

$x^3 - 2x^2 + 3x - 1.$

5.5 Існування кореня полінома

Розглянемо питання, чи кожний поліном ненульового степеня має хоча б один корінь.

Довільний поліном першого степеня $f(x) = ax + b$ з кільця $F[x]$ має в полі F корінь $x = -\frac{b}{a}$. Поліном $f(x)$ степеня $n > 1$ з кільця $F[x]$ може не мати в полі F жодного кореня. Це стосується, зокрема, полінома $f(x)$ степеня $n > 1$, незвідного в полі F, оскільки при існуванні в полі F кореня цього полінома випливала б наявність у нього лінійного множника, тобто його звідність над полем F.

Приклад 5.11. *Поліном $f(x) = x^2 - 3 \in \mathbb{Q}[x]$ над полем $\mathbb{Q}$ не має раціональних коренів, а $g(x) = x^2 + 2 \in \mathbb{R}[x]$ над полем $\mathbb{R}$ не має дійсних коренів. Але кожний із цих поліномів у деякому розширенні відповідного поля буде мати корені: $f(x)$ має корені $\pm\sqrt{3}$ в полі $\mathbb{R}$, а $g(x)$ - корені $\pm i\sqrt{2}$ в полі $\mathbb{C}$.*

З'ясуємо питання, чи для кожного полінома $f(x)$ степеня $n > 1$ з кільця $F[x]$, який не має коренів в полі F, існує розширення F_1 поля F, в якому поліном матиме корені.

Теорема 5.12. *(Кронекера) Для довільного полінома $f(x)$ ненульового степеня над полем F існує розширення F_1 поля F, в якому цей поліном має корінь.*

Доведення. Для доведення теореми необхідні деякі відомості з теорії кілець. Нехай $p(x)$ – один із незвідних множників полінома $f(x)$ у полі F (якщо сам $f(x)$ – незвідний, то $p(x) = f(x)$). Можна записати, що $f(x) = p(x) \cdot s(x)$ і далі продовжувати доведення теореми для полінома $p(x)$. Розглянемо головний ідеал (p) кільця $F[x]$, породжений елементом $p(x)$, і фактор-кільце $F_1 = F[x]/(p)$. Оскільки $F[x]$ – кільце головних ідеалів, а (p) – ідеал, породжений простим елементом $p(x)$, то F_1 є полем (згідно відповідної теореми теорії кілець).

Поле F_1 складається з класів лишків за модулем (p), представниками яких є всі можливі остачі від ділення будь-якого полінома $h(x) \in F[x]$ на $p(x)$, тобто усі можливі поліноми не вище певного степеня з $F[x]$. Це поле містить усі константи $\overline{c}$, де $c \in F$, тобто є розширенням поля F. Саме у цьому розширенні існує корінь полінома $p(x)$, таким коренем є елемент $\overline{x} \in F_1$. Дійсно, якщо $g(x)$ – довільний поліном з $F_1[x]$, то для знаходження $g(\bar{x})$ треба взяти остачу від ділення $g(x)$ на $p(x)$. Тому $p(\overline{x}) = 0$ (бо остача від ділення $p(x)$ на $p(x)$ дорівнює нулю).

Отже, в F_1 дійсно існує корінь полінома $p(x)$, а, значить, і $f(x)$. Теорему доведено. $\square$

Наслідком з теореми Кронекера є наступне твердження:

Теорема 5.13. *Для будь-якого полінома $f(x) \in F[x]$ ненульового степеня над полем F існує таке розширення $\bar{F}$ поля F, в якому знаходяться всі корені $f(x)$ (тобто поліном $f(x)$ розкладається на лінійні множники).*

Доведення. Нехай $\deg f = n$. Згідно теореми Кронекера існує розширення F_1 поля F, в якому $f(x)$ має корінь α_1 , і тому $f(x) = (x - \alpha_1) \cdot f_1(x)$, де $f_1(x) \in F_1[x], \deg f_1 = n - 1$.

Застосуємо теорему Кронекера для F_1 і полінома $f_1(x)$, отримаємо розширення F_2 поля F_1, в якому існує корінь α_2 полінома $f_1(x)$. Ясно, що α_2 є також коренем $f(x)$, а F_2 - розширенням поля F, в якому можливий розклад $f(x) = (x - \alpha_1)(x - \alpha_2) f_2(x)$, де $f_2(x) \in F_2[x]$, $\deg f_2 = n - 2$.

Продовжуючи аналогічні міркування, отримаємо розширення F_3, $F_4, \ldots, F_n$ поля F, корені $\alpha_1, \alpha_2, \ldots, \alpha_n$, розклади $f_3(x)$, $f_4(x), \ldots,$

$f_n(x)$, і нарешті, дістанемо $\deg f_{n+1} = 0$, тобто $f_{n+1} = c \in F_n$. Поле F_n і є шуканим полем $\bar{F}$, бо воно є розширенням поля F, в якому

$$f(x) = c \cdot (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

$\square$

Поле $\bar{F}$, в якому поліном $f(x)$ розкладається на лінійні множники, називається **полем розкладу** цього полінома.

Звідси, останню теорему можна сформулювати інакше: *для будь-якого полінома $f(x) \in F[x]$ ненульового степеня існує поле розкладу $\bar{F}$, яке є розширенням поля F.*

Приклад 5.14. *Розкласти на лінійні множники $f(x) = x^4 - 5 \in \mathbb{Q}[x]$.*

У полі $\mathbb{Q}$ не можна розкласти на лінійні множники.

В кільці $\mathbb{R}[x]$ $f(x) = (x - \sqrt[4]{5})(x + \sqrt[4]{5})(x^2 + \sqrt{5})$.

В кільці $\mathbb{C}[x]$ $f(x) = (x - \sqrt[4]{5})(x + \sqrt[4]{5})(x - \sqrt[4]{5}i)(x + \sqrt[4]{5}i)$.

Означення 5.15. *Поле F називається* **алгебраїчно замкнутим**, *якщо воно є полем розкладу для будь-якого полінома $f(x) \in F[x]$ ненульового степеня.*

Інакше: *F є алгебраїчно замкнутим полем, якщо усі корені будь-якого полінома $f(x) \in F[x]$ належать цьому полю.*

Наслідок 5.16. *Поліном $f(x) \in F[x]$ n-го степеня має у полі розкладу n коренів.*

Наслідок 5.17. *У полі розкладу поліном $f(x) = a_0x^n + \dots + a_{n-1}x + a_n$ має канонічний розклад вигляду*

$$f(x) = a_0(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdot \dots \cdot (x - \alpha_m)^{k_m}, \tag{5.5}$$

де $k_1 + k_2 + \dots + k_m = n$, $\alpha_1, \alpha_2, \dots, \alpha_m$ *- різні корені полінома* $f(x)$.

Доведення. Степені $k_1, k_2, \dots, k_m$ появилися тому, що можуть зустрітися однакові корені. Константа $c = a_0$ випливає із прирівнювання коефіцієнтів у записах полінома $f(x) = c \cdot (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ і $f(x) = a_0 x^n + \dots + a_{n-1}x + a_n$. □

5.6 Формули Вієта

Нехай $f(x) = x^n + \dots + a_{n-1}x + a_n$ - довільний нормований ($a_0 = 1$) поліном з кільця $F[x], \alpha_1, \alpha_2, \dots, \alpha_n$ - його корені, звідки $f(x) = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$.

Виконавши множення у правій частині рівності

$$x^n + \dots + a_{n-1}x + a_n = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n),$$

звівши подібні члени і прирівнявши коефіцієнти при однакових степенях x, отримаємо формули, які пов'язують між собою корені і коефіцієнти полінома в будь-якому полі його розкладу.

$$a_1 = -(\alpha_1 + \alpha_2 + \dots + \alpha_n),$$

$$a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \dots + \alpha_2\alpha_n + \dots + \alpha_{n-1}\alpha_n,$$

$$\dots,$$

$$a_k = (-1)^k \sum_{i_1 < i_2 < \dots < i_k} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k},$$

$$\dots,$$

$$a_n = (-1)^n \alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_n. \tag{5.6}$$

Отримані співвідношення називають **формулами Вієта**. Якщо поліном $f(x)$ не є нормованим ($a_0 \neq 1$), то праві частини формул Вієта дорівнюватимуть відношенням $\frac{a_i}{a_0}$, $i = 1, 2, \dots, n$.

Вправи 5.18. *(1) Розкласти поліном* $f(x) = 3x^5 - 4x^4 + x^3 - 2x^2 - x + 3$ *за степенями лінійного двочлена:*

(а) $x + 1$*;*

(б) $x - 1$*;*

(в) $x + 2$.

(2) Побудувати поліном $f(x)$ *не вище четвертого степеня над полем* $\mathbb{Q}$*, якщо* $f(-1) = 2$*,* $f(0) = 3$*,* $f(1) = -1$*,* $f(2) = 0$*,* $f(3) = 4$*, використовуючи:*

(а) формулу Лагранжа;

(б) формулу Ньютона.

(3) Записати формули Вієта звязку між коефіцієнтами і коренями поліномів:

(а) $f(x) = 2x^4 - 5x^3 - 3x^2 + 4x - 1$*;*

(б) $f(x) = 3x^5 - 4x^3 + x^2 + 1$.

6 Кратні множники і кратні корені полінома

6.1 Похідна полінома

Відшукати корені полінома $f(x) \in F[x]$ було б набагато легше, якби був відомим канонічний розклад цього полінома над полем F, тобто вираз

$$f(x) = [p_1(x)]^{k_1} \cdot [p_2(x)]^{k_2} \cdot \dots \cdot [p_m(x)]^{k_m},$$

оскільки тоді досить було б шукати корені незвідних множників $p_1(x)$, $p_2(x), \dots, p_m(x)$, степені яких менші (переважно) за степінь самого

$f(x)$. Якісь загальні методи отримання канонічного розкладу полінома відсутні, однак є способи, з допомогою яких без розкладання цього полінома на незвідні множники можна встановити наявність чи відсутність у нього кратних множників, і, в разі їх наявності, розкласти його в добуток поліномів, які вже кратних множників не мають. Ці способи застосовні за умови нульової характеристики поля F і пов'язані з поняттям похідної від полінома.

Нехай $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ - поліном n-го степеня над полем F. Функціональне тлумачення полінома робить природним наступне означення.

Похідною полінома $f(x) \in F[x]$ називається поліном

$$f'(x) = n \cdot a_0x^{n-1} + (n-1) \cdot a_1x^{n-2} + \cdots + 2a_{n-2}x + a_{n-1}. \quad (6.1)$$

Якщо $F = \mathbb{R}$ (поле дійсних чисел), а f^* - зв'язана з f поліноміальна функція, то подане означення похідної співпадає зі звичайним її означенням як границі. У випадку ж довільного поля поняття границі не завжди застосовне, тому при означенні похідної полінома над полем користуються формальним записом (6.1).

Похідні полінома нульового степеня і нуль-полінома вважають рівними нулю.

Оскільки коефіцієнти похідної $f'(x)$ полінома $f(x) \in F[x]$ є добутками коефіцієнтів полінома та натуральних чисел, то похідна полінома над полем F теж є поліномом над полем F.

Твердження $\deg f' = \deg f - 1$ має місце тільки за умови, що поле F є полем характеристики 0, оскільки в цьому випадку із $a_0 \neq 0$ випливає $n \cdot a_0 \neq 0$. Якщо ж поле має деяку скінченну характеристику $p \geq 1$, то із $p \cdot a_0 = 0$ випливає, що похідна, наприклад, полінома $q(x) = a_0x^p$ дорівнює нуль-поліному, тобто $\deg q' \neq \deg q - 1$.

Загальні правила диференціювання залишаються справедливими і для поліномів над довільним полем:

1. $[f(x) + g(x)]' = f'(x) + g'(x)$,

2. $[f(x) \cdot g(x)]' = f'(x)g(x) + f(x)g'(x)$,

$2'$. $[cf(x)]' = cf'(x)$, $(c = const)$,

$2''$. $\{[f(x)]^k\}' = k[f(x)]^{k-1} \cdot f'(x)$, $(k \in \mathbb{N})$.

Доведення цих рівностей випливає із означення (6.1) похідної полінома. Для прикладу наведемо доведення першої з них (інші доводяться аналогічно). Якщо

$$f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n, \;\; g(x) = b_0+b_1x+b_2x^2+\cdots+b_mx^m,$$

то (при $n \geq m$) $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_m+b_m)x^m+a_{m+1}x^{m+1}+\cdots+a_nx^n$, і, за означенням похідної, $[f(x)+g(x)]' = (a_1+b_1)+2(a_2+b_2)x+\cdots+m(a_m+b_m)x^{m-1}+(m+1)a_{m+1}x^m+ +\cdots+n\cdot a_nx^{n-1} = (a_1+2a_2x+\cdots+m\cdot a_mx^{m-1}+(m+1)\cdot a_{m+1}x^m+\cdots+ +n\cdot a_nx^{n-1})+(b_1+2b_2x+\cdots+m\cdot b_mx^{m-1}) = f'(x)+g'(x)$.

Розглядають також другу, третю,..., k-у похідну полінома. Зокрема, $f^{(k)}(x)$ визначається як похідна від $f^{(k-1)}(x)$.

6.2 Кратні множники

Розглянемо простий спосіб встановлення наявності у полінома кратних множників.

Теорема 6.1. *Якщо незвідний у заданому полі F характеристики 0 поліном $q(x)$ є множником кратності $k \geq 1$ для полінома $f(x)$, то він є множником кратності $(k-1)$ для похідної $f'(x)$.*

Доведення. Очевидно, що будь-який множник кратності $k = 1$ полінома $f(x)$ в розклад похідної $f^{'}(x)$ на незвідні множники не входить.

Умова того, що поліном $q(x)$ є множником кратності k для полінома $f(x)$, може бути записана так:

$$f(x) = [q(x)]^k \cdot t(x),$$

де $t(x)$ - поліном, який не ділиться на $q(x)$ і тому є з ним взаємно простим.

Із виразу для похідної $f^{'}(x) = k[q(x)]^{k-1} \cdot q^{'}(x) \cdot t(x) + [q(x)]^k \cdot t^{'}(x) = [q(x)]^{k-1}\{k \cdot q^{'}(x)t(x) + q(x)t^{'}(x)\}$, випливає, що $f^{'}(x)$ ділиться на $[q(x)]^{k-1}$.

Залишилось показати, що $q(x)$ є для $f^{'}(x)$ множником кратності саме $(k-1)$, тобто довести, що поліном $r(x) = k \cdot q^{'}(x)t(x) + q(x)t^{'}(x)$ не ділиться на $q(x)$. Дійсно, якщо б $r(x)$ ділився на $q(x)$, то й $q^{'}(x)t(x) = \frac{1}{k}[r(x) - q(x)t^{'}(x)]$ ділився б на $q(x)$, але оскільки $t(x)$ і $q(x)$ взаємно прості, то це означало б, що на $q(x)$ ділиться $q^{'}(x)$, а це неможливо, бо степінь $q^{'}(x)$ нижчий за степінь $q(x)$. □

Наслідок 6.2. *Для того, щоб поліном $f(x)$ не мав кратних множників, необхідно і достатньо, щоб $f(x)$ був взаємно простий зі своєю похідною $f^{'}(x)$.*

Доведення. а) Якщо всі незвідні множники полінома $f(x)$ мають кратність 1, то в розкладі $f^{'}(x)$ на незвідні множники не буде жодного множника, спільного з множниками $f(x)$, тобто $(f, f^{'}) = 1$.

б) Якщо $f(x)$ має хоч один кратний множник $q(x)$, то $(f, f^{'})$ ділиться на $q(x)$ і тому не є константою, а, значить, f і $f^{'}$ не є взаємно простими. □

Таким чином, наявність чи відсутність кратних множників у полінома залежать виключно від його коефіцієнтів, і не залежать від поля, над яким цей поліном розглядають.

Приклад 6.3. *Чи має кратні множники поліном* $f(x) = x^3+2x^2-x-2$*?*

Обчислимо похідну: $f'(x) = 3x^2 + 4x - 1$. *Користуючись алгоритмом Евкліда, переконуємось, що* $(f, f') = 1$.

Отже, поліном $f(x)$ *кратних множників не має.*

6.3 Відокремлення кратних множників

Задача подання полінома у канонічному вигляді є непростою, тому, у зв'язку з відсутністю загальних методів отримання такого розкладу, розглянемо спосіб, з допомогою якого без розкладання цього полінома на незвідні множники можна встановити наявність чи відсутність у нього кратних множників, і, в разі їх наявності, отримати розклад його в добуток поліномів, які вже кратних множників не мають, хоча цей розклад і не буде таким повним, як канонічний.

Виберемо в канонічному розкладі

$$f(x) = [p_1(x)]^{k_1} \cdot [p_2(x)]^{k_2} \cdot \dots \cdot [p_m(x)]^{k_m}$$

ті незвідні множники $p_i(x)$, степінь яких $k_i = 1$, і позначимо добуток цих множників через $\varphi_1(x)$:

$$\varphi_1(x) = p_{i_1}(x)p_{i_2}(x)\dots p_{i_k}(x).$$

Утворимо далі добуток тих множників $p_j(x)$, кратність яких k_j дорівнює 2, тобто тих, які входять до канонічного розкладу у другому степені.

$$\varphi_2(x) = p_{j_1}(x)p_{j_2}(x)\dots p_{j_r}(x).$$

Оскільки $\varphi_2(x)$ - це добуток самих незвідних множників кратності 2, то до розкладу $f(x)$ входить $[\varphi_2(x)]^2$.

Аналогічно утворимо $\varphi_3(x)$ як добуток незвідних множників, що мають кратність 3, і так дальше. В кінцевому результаті канонічний розклад запишеться у вигляді:

$$f(x) = \varphi_1 \cdot \varphi_2^2 \cdot \varphi_3^3 \cdots \varphi_m^m. \tag{6.2}$$

Якщо множників k-тої кратності нема, то вважаємо, що $\varphi_k = 1$. Розклад (6.2) доцільний лише тоді, коли в канонічному розкладі існують *кратні* множники.

Приклад 6.4. *Подати канонічний запис полінома* $f(x) = (x-1)^4(x+1)^2(x^2+2)(x-2)^2$ *у вигляді (6.2).*

$\varphi_1(x) = x^2 + 2$, $\varphi_2(x) = (x+1)(x-2) = x^2 - x - 2$, $\varphi_3(x) = 1$, $\varphi_4(x) = x - 1$.

$f(x) = \varphi_1 \cdot \varphi_2^2 \cdot \varphi_3^3 \cdot \varphi_4^4 = (x^2+2)(x^2-x-2)^2(x-1)^4$.

Задача зображення полінома у вигляді (6.2) називається **відокремленням кратних множників.**

Для отримання розкладу $f(x) = \varphi_1 \cdot \varphi_2^2 \cdot \varphi_3^3 \cdot \dots \cdot \varphi_m^m$ потрібно за коефіцієнтами полінома $f(x)$ знайти поліноми $\varphi_1, \varphi_2, \varphi_3, \dots, \varphi_m$.

Оскільки $\varphi_1(x)$ - це добуток незвідних множників полінома $f(x)$, які мають кратність $k = 1$, то в $f'(x)$ жоден із цих множників не входить. Із того, що $\varphi_2(x)$ - добуток незвідних множників кратності 2, випливає, що в $f'(x)$ усі ці множники входять з кратністю 1, тобто $f'(x)$ має своїм множником добуток $\varphi_2(x)$ незвідних множників, але вже у першому степені. Аналогічно, якщо $f(x)$ має множником $[\varphi_k(x)]^k$, то $f'(x)$ матиме множник $[\varphi_k(x)]^{k-1}$. Таким чином,

$$f'(x) = \varphi_2 \cdot \varphi_3^2 \cdots \varphi_m^{m-1} \cdot \psi_1,$$

де ψ_1 не ділиться на $\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m$.

Тоді найбільший спільний дільник (f, f') є добутком усіх множників, які входять у розклади як $f(x)$, так і $f'(x)$.

$$d_1 = (f, f') = \varphi_2 \cdot \varphi_3^2 \cdot \cdots \cdot \varphi_m^{m-1}.$$

Знайдемо тепер d_1'.

$$d_1' = \varphi_3 \cdot \varphi_4^2 \cdots \varphi_m^{m-2} \cdot \psi_2,$$

де ψ_2 не ділиться на $\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m$.

$$d_2 = (d_1, d_1') = \varphi_3 \cdot \varphi_4^2 \cdots \varphi_m^{m-2}.$$

Аналогічно можна розрахувати:

$$d_2' = \varphi_4 \cdot \varphi_5^2 \cdots \varphi_m^{m-3} \cdot \psi_3,$$

$$d_3 = (d_2, d_2') = \varphi_4 \cdot \varphi_5^2 \cdots \varphi_m^{m-3},$$

$$\ldots$$

$$d_{m-2} = (d_{m-3}, d_{m-3}') = \varphi_{m-1} \cdot \varphi_m^2,$$

$$d_{m-1} = (d_{m-2}, d_{m-2}') = \varphi_m,$$

$$d_m = (d_{m-1}, d_{m-1}') = 1.$$

Поділивши f на d_1, d_1 на d_2 і так далі, отримаємо:

$$q_1 = \frac{f}{d_1} = \varphi_1 \cdot \varphi_2 \cdots \varphi_m,$$

$$q_2 = \frac{d_1}{d_2} = \varphi_2 \cdot \varphi_3 \cdots \varphi_m,$$

$$\ldots$$

$$q_{m-1} = \frac{d_{m-2}}{d_{m-1}} = \varphi_{m-1} \cdot \varphi_m,$$

$$q_m = \frac{d_{m-1}}{d_m} = \varphi_m.$$

І, нарешті, шукані множники φ_i дістанемо так:

$$\varphi_1 = \frac{q_1}{q_2},\ \varphi_2 = \frac{q_2}{q_3}, \dots, \varphi_{m-1} = \frac{q_{m-1}}{q_m},\ \varphi_m = q_m.$$

Таким чином: у довільного полінома над полем F можна *відокремити кратні множники* за допомогою скінченного кількості раціональних дій над деякими поліномами.

Оскільки похідні та найбільший спільний дільник не залежать від поля задання поліномів, то розклад (6.2), на відміну від канонічного розкладу (4.1), не залежить від того, до якого поля F належать коефіцієнти цього полінома.

Приклад 6.5. *Відокремити кратні множники полінома*
$f(x) = x^5 + x^4 - 5x^3 - x^2 + 8x - 4.$

Розв'язання. $f' = 5x^4 + 4x^3 - 15x^2 - 2x + 8$. *Знайдемо* d_i *за алгоритмом Евкліда:*

$$d_1 = (f, f') = x^3 - 3x + 2;\ \ d_1' = 3x^2 - 3.$$

$$d_2 = (d_1, d_1') = x - 1;\ \ d_2' = 1.\ \ d_3 = (d_2, d_2') = 1.$$

Обчислимо q_i. $q_1 = \frac{f}{d_1} = x^2 + x - 2$; $q_2 = \frac{d_1}{d_2} = x^2 + x - 2$; $q_3 = \frac{d_2}{d_3} = x - 1$.

Знаходимо φ_i. $\varphi_1 = \frac{q_1}{q_2} = 1$; $\varphi_2 = \frac{q_2}{q_3} = x + 2$; $\varphi_3 = q_3 = x - 1$.

В результаті маємо: $f(x) = \varphi_1 \cdot \varphi_2^2 \cdot \varphi_3^3 = (x+2)^2(x-1)^3$.

6.4 Встановлення кратності кореня полінома

Розглянемо способи визначення кратності кореня полінома.

1 спосіб. Згідно з означенням кратного кореня полінома для встановлення кратності кореня α полінома $f(x)$ досить послідовним діленням $f(x)$ на $(x-\alpha)$ знайти таке k, щоб $f(x)$ ділився на $(x-\alpha)^k$, але не ділився на $(x-\alpha)^{k+1}$. При цьому k і буде кратністю кореня α.

2 спосіб. Цей спосіб ґрунтується на твердженні наступної теореми:

Теорема 6.6. *Для того, щоб α був коренем кратності k полінома $f(x)$, необхідно і достатньо, щоб*

$$f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0, \ f^{(k)}(\alpha) \neq 0. \qquad (6.3)$$

Доведення. а) Нехай α - корінь $f(x)$ кратності k. Значить, $(x-\alpha)$ - незвідний множник $f(x)$ кратності k, тобто, згідно теореми 6.1, $(x-\alpha)$ - незвідний множник $f'(x)$ кратності $(k-1)$, звідки α - корінь $f'(x)$ кратності $(k-1)$. Аналогічно, α - корінь $f''(x)$ кратності $(k-2)$ і так далі. Нарешті, $f^{(k-1)}(x)$ має $(x-\alpha)$ своїм множником кратності 1, а $f^{(k)}(x)$ множника $(x-\alpha)$ не має. Тому, за наслідком з теореми Безу, $f^{(k)}(\alpha) \neq 0$.

б) Нехай умова (6.3) теореми справджується. Тоді α є коренем $f(x)$. Нехай кратність α дорівнює m. Згідно необхідності,

$$f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0, \ f^{(m)}(\alpha) \neq 0 \qquad (6.4)$$

При $m < k$ умова (6.3) свідчила б про те, що $f^{(m)}(\alpha) = 0$, а це суперечить (6.4). Аналогічно відкидаємо $m > k$. Отже, $m = k$. $\square$

Приклад 6.7. *Знайти кратність кореня -2 полінома $f(x) = x^5 + x^4 - 5x^3 - x^2 + 8x - 4$.*

1 спосіб. Скористаємось схемою Горнера:

	1	*1*	*-5*	*-1*	*8*	*-4*
-2	*1*	*-1*	*-3*	*5*	*-2*	*0*
-2	*1*	*-3*	*3*	*-1*	*0*	
-2	*1*	*-5*	*13*	**-27**$_{\neq 0}$		

$f(x)$ *ділиться на* $(x+2)^2$*, але не ділиться на* $(x+2)^3$*. Тому кратність кореня -2 дорівнює 2.*

2спосіб.

$f'(x) = 5x^4 + 4x^3 - 15x^2 - 2x + 8, \;\; f'(-2) = 0.$

$f''(x) = 20x^3 + 12x^2 - 30x - 2, \;\; f''(-2) = -54.$

Отже, кратність кореня -2 дорівнює 2.

Вправи 6.8. *(1) Відокремити кратні множники поліномів:*

(а) $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$*;*

(б) $f(x) = x^4 + 2x^2 + 1$*;*

(в) $f(x) = x^5 - 2x^4 + 2x^3 - 4x^2 + x - 2$*.*

(2) Знайти кратність кореня α *полінома* $f(x)$*:*

(а) $\alpha = 1,\; f(x) = x^4 - 2x^3 + 2x - 1$*;*

(б) $\alpha = 2,\; f(x) = 3x^3 - 4x^2 - x - 6$*;*

(в) $\alpha = -1,\; f(x) = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1$*.*

7 Поліноми від багатьох змінних

7.1 Кільце поліномів від багатьох змінних

Поняття полінома від багатьох змінних є узагальненням поняття полінома від однієї змінної. Для початку розглянемо випадок полінома від двох змінних. Нагадаємо, що $R[x]$ - кільце поліномів від однієї змінної x над кільцем R, де R і $R[x]$ - комутативні кільця з одиницею. Побудуємо тепер кільце поліномів від однієї змінної y над кільцем $R[x]$ (позначивши його, за аналогією, через $R[x][y]$), тобто множину всеможливих поліномів вигляду

$$a_0(x)y^n + a_1(x)y^{n-1} + \cdots + a_{n-1}(x)y + a_n(x), \qquad (7.1)$$

де $a_i(x) \in R[x], i = 0, 1, \ldots, n$, тобто є поліномами від змінної x над кільцем R і мають вигляд:

$$a_i(x) = a_{i0}x^{m_i} + a_{i1}x^{m_i-1} + \cdots + a_{i,m_i-1}x + a_{i,m_i} = \sum_{j=0}^{m_i} a_{ij}x^{m_i-j}.$$

Підставивши отримані вирази для $a_i(x), i = 0, 1, \ldots, n$ (елементів кільця $R[x]$) в (7.1), отримаємо вираз для елементів кільця $R[x][y]$, який матиме вигляд

$$\sum_{i=0}^{n}\sum_{j=0}^{m_i} a_{ij}x^{m_i-j}y^{n-i}, \qquad a_{ij} \in R.$$

Таким чином, довільний елемент кільця $R[x][y]$ рівний деякій скінченній сумі $\sum a_{ij}x^{k_i}y^{l_j}$, де k_i, l_j - невід'ємні цілі числа. Ясно, що й навпаки, довільна скінченна сума $\sum a_{ij}x^{k_i}y^{l_j}$, де $a_{ij} \in R$, а k_i, l_j - деякі невід'ємні цілі числа, є елементом кільця $R[x][y]$, так як кожний вираз $a_{ij}x^{k_i}y^{l_j}$ є поліномом від змінної y з коефіцієнтами $a_{ij}x^{k_i} \in R[x]$, тобто належить кільцю $R[x][y]$.

Оскільки x та y є елементами комутативного кільця $R[x][y]$, то $R[x][y] = R[y][x]$ (надалі позначатимемо $R[x, y]$ або $R[y, x]$). Кільце $R[x, y]$ називають *кільцем поліномів від двох змінних x, y над кільцем R*, а кожний його елемент - *поліномом від змінних x, y*

над кільцем R. Позначають поліноми від двох змінних так: $f(x, y)$, $g(x, y)$ і т.д.

Приклад 7.1. *Записати поліном від двох змінних* $f(x, y) = 3x^2y^2 + 5x^2y - 7xy^2 + 2x - 4y - 2$ *у вигляді полінома від змінної* y *над* $\mathbb{Q}[x]$.

Розв'язування. $f(x, y) = 3x^2y^2 + 5x^2y - 7xy^2 + 2x - 4y - 2 = (3x^2 - 7x)y^2 + (5x^2 - 4)y + (2x - 2)$.

Сформулюємо тепер означення кільця поліномів від багатьох змінних над кільцем.

Означення 7.2. *Кільцем поліномів* $R[x_1, x_2, \ldots, x_n]$ *від* n *змінних* $x_1, x_2, \ldots, x_n$ *над комутативним кільцем* R *з одиницею називається кільце поліномів від однієї змінної* x_n *над кільцем* $R[x_1, x_2, \ldots, x_{n-1}]$.

Тобто, $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$.

Користуючись методом математичної індукції за кількістю невідомих, можна довести твердження, аналогічне тому, що стосується кільця поліномів від однієї змінної.

Теорема 7.3. *Якщо кільце* R *є цілісним, то і кільце* $R[x_1, x_2, \ldots, x_n]$ *є цілісним.*

Доведення. При $n = 1$ отримаємо раніше доведений випадок поліномів від однієї змінної. Припустимо, що поліноми від $(n - 1)$ змінних з коефіцієнтами із кільця R утворюють цілісне кільце. Доведемо це твердження для n. Кожний поліном від змінних $x_1, x_2, \ldots, x_{n-1}, x_n$ можна однозначно подати як поліном від змінної x_n з коефіцієнтами, які є поліномами від $x_1, x_2, \ldots, x_{n-1}$. І навпаки, кожний поліном від змінної x_n з коефіцієнтами із кільця поліномів від $x_1, x_2, \ldots, x_{n-1}$ над кільцем R можна розглядати як поліном над цим же кільцем R

від всієї сукупності змінних $x_1, x_2, \ldots, x_n$. Очевидно, що отримана взаємно однозначна відповідність між поліномами від n змінних і поліномами від однієї змінної над кільцем поліномів від $(n-1)$ змінних є ізоморфізмом по відношенню операцій як додавання, так і множення.

Оскільки сукупність поліномів від однієї змінної над кільцем поліномів від $(n-1)$ змінних утворює цілісне кільце, то й ізоморфна їй сукупність поліномів від n змінних над кільцем R утворює цілісне кільце. $\square$

Вище було показано, як виглядає елемент кільця поліномів від двох змінних. Запишемо тепер загальний вигляд кожного елемента кільця $R[x_1, x_2, \ldots, x_n]$ поліномів від n змінних.

Довільний елемент f кільця $R[x_1, x_2, \ldots, x_n]$ поліномів від n змінних має вигляд

$$f = \sum_{i=1}^{N} a_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}, \tag{7.2}$$

де $a_i \in R, k_{ji}$ - цілі невід'ємні числа. І навпаки, *кожний вираз вигляду* (7.2) *є елементом кільця $R[x_1, x_2, \ldots, x_n]$ поліномів від n змінних.* Останнє твердження легко доводиться методом математичної індукції за кількістю змінних.

Елемент $f = \sum\limits_{i=1}^{N} a_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}$ кільця $R[x_1, x_2, \ldots, x_n]$ називають **поліномом від n змінних** $x_1, x_2, \ldots, x_n$ над R і позначають $f(x_1, x_2, \ldots, x_n)$. Тут кожний доданок $a_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}$ - *одночлен (або моном)*, елемент a_i - коефіцієнт цього одночлена (надалі за аналогією до попереднього називатимемо доданки $a_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}$ *членами* полінома $f(x_1, x_2, \ldots, x_n)$). Члени полінома називаються *подібними*, якщо усі змінні входять до них в попарно рівних степенях. Заміну кількох подібних членів одним називають зведенням подібних членів. Передбачається, що $f(x_1, x_2, \ldots, x_n)$ не містить подібних членів над кільцем і що розглядаються лише члени з ненульовими коефіцієнтами.

Два поліноми від n змінних називаються *рівними*, якщо рівні їх коефіцієнти при однакових членах.

Виконання операцій додавання і множення над поліномами кільця $R[x_1, x_2, \ldots, x_n]$ зводиться до виконання відповідних операцій над членами $a_k x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ цих поліномів (внаслідок дистрибутивного закону, який виконується в кільці). Зокрема, додавання зводиться до додавання елементів кільця R (коефіцієнтів при однакових членах), а множення виконується наступним чином:

$$a_k x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \cdot b_m x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n} = a_k b_m x_1^{k_1+m_1} x_2^{k_2+m_2} \ldots x_n^{k_n+m_n}.$$

Нагадаємо, що форму запису полінома, яка не містить подібних членів, називають канонічною або нормальною. Така форма запису є єдиною з точністю до порядку членів, тобто якщо два поліноми, записані в канонічній формі, є рівними між собою, то кожний член одного із цих поліномів є також членом іншого, і навпаки.

Степенем по відношенню до змінної $x_i (i = 1, \ldots, n)$ називається найвищий показник, з яким змінна x_i входить в члени цього полінома. Степенем члена $a_k x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ називається число $k_1 + k_2 + \cdots + k_n$, тобто сума показників при невідомих. Найвищий із степенів членів називається степенем полінома $f(x_1, x_2, \ldots, x_n)$, а член з найбільшим степенем - старшим членом полінома. В загальному випадку поліном може містити декілька членів найвищого степеня, тому поняття старшого члена застосовне не для кожного полінома.

Єдиним поліномом з $R[x_1, x_2, \ldots, x_n]$, до якого поняття степеня незастосовне, є **нуль-поліном**. Якщо всі члени полінома мають той самий степінь s, то поліном називається **однорідним** поліномом або **формою** степеня s. Ясно, що будь-який поліном можна подати як суму скінченної кількості однорідних поліномів різних степенів.

Теорема 7.4. *Степінь добутку двох відмінних від нуля поліномів від n змінних над цілісним кільцем дорівнює сумі степенів цих поліномів.*

Доведення. Нехай $\varphi(x_1, x_2, \ldots, x_n)$ – форма степеня s, а $\psi(x_1, x_2, \ldots, x_n)$ – форма степеня t. Добуток будь-якого члена форми φ на будь-який член форми ψ буде мати степінь $(s + t)$, а тому добуток $\varphi\psi$ буде формою степеня $(s + t)$, оскільки зведення подібних членів не може перетворити всі коефіцієнти цього добутку в нуль через відсутність в кільці $R[x_1, x_2, \ldots, x_n]$ дільників нуля.

Якщо тепер дано довільні поліноми $f(x_1, x_2, \ldots, x_n)$ і $g(x_1, x_2, \ldots, x_n)$ відповідно степенів s і t, то подаючи кожний з них у вигляді суми форм різних степенів, отримаємо:

$$f(x_1, x_2, \ldots, x_n) = \varphi(x_1, x_2, \ldots, x_n) + \ldots,$$

$$g(x_1, x_2, \ldots, x_n) = \psi(x_1, x_2, \ldots, x_n) + \ldots,$$

де φ і ψ будуть відповідно формами степенів s і t, а всі інші $(+\ldots)$ будуть формами нижчих степенів. Тоді $f \cdot g = \varphi \cdot \psi + \ldots$ Форма $\varphi\psi$ має степінь $(s+t)$, а всі інші $(+\ldots)$ мають менший степінь, тому $\deg fg = \deg f + \deg g$. $\square$

Означення подільності, дільника, загальні властивості відношення подільності, поняття і властивості незвідних поліномів без змін переносяться з кільця поліномів від однієї змінної на кільце поліномів від n змінних. Важливою особливістю теорії подільності в кільці $F[x_1, x_2, \ldots, x_n]$ порівняно з кільцем $F[x]$ є те, що $F[x_1, x_2, \ldots, x_n]$ при $n > 1$ не є евклідовим кільцем, тобто, що на випадок поліномів від n змінних не поширюються алгоритм Евкліда і його наслідки. Проте один з основних результатів теорії подільності в кільці $F[x]$, а саме можливість і однозначність розкладу полінома у добуток незвідних множників, залишається незмінним і в кільці $F[x_1, x_2, \ldots, x_n]$ при $n > 1$, однак, оскільки $F[x_1, x_2, \ldots, x_n]$ не є евклідовим кільцем, то доведення цього твердження не повинно опиратися на означення ділення поліномів з остачею, тому тут достатньо скористатися методом математичної індукції за степенем полінома $f(x_1, x_2, \ldots, x_n)$.

7.2 Лексикографічне розміщення членів полінома

Оскільки в загальному випадку поліном від багатьох змінних може містити декілька членів однакового степеня, то для таких поліномів поняття степеня члена є вже недостатнім для встановлення єдиного порядку розміщення його членів.У зв'язку з цим для таких поліномів був вибраний інший принцип упорядкування членів полінома – **лексикографічний** (лексикон (гр.) – словник).

Згідно алфавітного порядку розміщення букв, взаємне розташування слів у словнику визначається за першими буквами у цих словах, а в разі їх співпадання – за другими, і так далі.

Нехай $a_k x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ $(7.3')$ і $b_m x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ $(7.3'')$ - два різні члени полінома $f(x_1, x_2, \ldots, x_n)$ із кільця $F[x_1, x_2, \ldots, x_n]$, коефіцієнти яких є деякими відмінними від нуля елементами із F. Оскільки ці члени різні, то хоча б одна із різниць показників при змінних $k_i - m_i$ $(i = 1, 2, \ldots, n)$ відмінна від нуля. Член $(7.3')$ буде вважатися *вищим* члена $(7.3'')$, якщо перша із цих ненульових різниць є додатною, тобто якщо існує таке і $(1 \leq i \leq n)$, що $k_1 = m_1, k_2 = m_2, \ldots, k_{i-1} = m_{i-1}$, але $k_i > m_i$. Іншими словами, член $(7.3')$ буде вищим члена $(7.3'')$, якщо показник при x_1 в $(7.3')$ більший ніж в $(7.3'')$, або якщо ці показники рівні, але показник при x_2 в $(7.3')$ більший ніж в $(7.3'')$ і так далі.

Таке зображення полінома, в якому вищі члени випереджають нижчі, називається *лексикографічним.*

Приклад 7.5. *Поліном* $f(x_1, x_2, x_3, x_4) = x_1^4 + 3x_1^2x_2^2x_3 + x_1^2x_2^2x_4^2 - x_3^2x_4 - 7$ *розміщений лексикографічно.*

Те, що один член полінома є вищим за іншого, не означає, що його степінь більший степеня іншого. Перший за порядком член при лексикографічному розміщенні називається *вищим членом* полінома.

Лема 7.6. *Вищий член добутку двох поліномів від n змінних дорівнює добутку вищих членів цих поліномів.*

Доведення. Нехай $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ $(7.4')$ – вищий, $a'x_1^{s_1}x_2^{s_2}\ldots x_n^{s_n}$ $(7.4'')$ – будь-який інший член полінома $f(x_1, x_2, \ldots, x_n)$, тоді існує таке i $(1 \leq i \leq n)$, що $k_1 = s_1, \ldots, k_{i-1} = s_{i-1}$, але $k_i > s_i$. Нехай $bx_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}$ $(7.5')$ – вищий, $b'x_1^{t_1}x_2^{t_2}\ldots x_n^{t_n}$ $(7.5'')$ – будь-який інший член полінома $g(x_1, x_2, \ldots, x_n)$, тоді існує таке j $(1 \leq j \leq n)$, що $m_1 = t_1, \ldots, m_{j-1} = t_{j-1}$, але $m_j > t_j$.

При знаходженні добутку поліномів f і g знайдемо добутки $(7.4')$ і $(7.5')$, а також $(7.4'')$ і $(7.5'')$. Отримаємо: $abx_1^{k_1+m_1}x_2^{k_2+m_2}\ldots x_n^{k_n+m_n}$

(7.6$'$) і $a'b'x_1^{s_1+t_1}x_2^{s_2+t_2}\dots x_n^{s_n+t_n}$ (7.6$''$). Очевидно, що член (7.6$'$) вищий члена (7.6$''$). Дійсно, якщо $i \le j$, то $k_1+m_1 = s_1+t_1, \dots, k_{i-1}+m_{i-1} = s_{i-1}+t_{i-1}$, але $k_i+m_i > s_i+t_i$, бо $k_i > s_i$, $m_i \ge t_i$. Аналогічно для $j \le i$.

Так само перевіряється, що член (7.6$'$) буде вищим за добуток членів (7.4$'$) і (7.5$''$), а також за добуток членів (7.4$''$) і (7.5$'$). Таким чином, (7.6$'$) як добуток вищих членів двох поліномів, є вищим за всі інші члени, які отримуються в результаті почленного перемноження поліномів f і g, а тому цей член при зведенні подібних членів не знищується, а залишається вищим членом в добутку fg. □

Крім лексикографічного розміщення членів полінома часто користуються розміщенням членів за степенями однієї змінної.

Вправи 7.7. *Розмістити члени поліномів лексикографічно:*

(а) $f(x_1,x_2,x_3) = x_2^2x_3 - 3x_1x_2x_3^2 + 4x_1x_3 - 2x_1^3x_2$;

(б) $f(x_1,x_2) = x_1^2x_2^2 - 2x_1^3x_2 + 2x_1x_2^3 + x_1^4 - x_2^4$.

8 Симетричні поліноми

8.1 Означення, властивості

Якщо $f(x_1,x_2,\dots,x_n)$ - довільний поліном з кільця $F[x_1,x_2,\dots,x_n]$, а $\delta = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix}$ – деяка підстановка множини $\{x_1,x_2,\dots,x_n\}$, то, замінивши в поліномі змінні x_k на змінні x_{i_k}, де $k = 1,2,\dots,n$, отримаємо поліном $f(x_{i_1},x_{i_2},\dots,x_{i_n})$, тобто підстановка δ перетворює поліном $f(x_1,x_2,\dots,x_n)$ в $f(x_{i_1},x_{i_2},\dots,x_{i_n})$.

Означення 8.1. *Поліном $f(x_1, x_2, \ldots, x_n)$ із $F[x_1, x_2, \ldots, x_n]$ називають* **симетричним поліномом** *відносно $x_1, x_2, \ldots, x_n$, якщо довільна підстановка множини $\{x_1, x_2, \ldots, x_n\}$ перетворює його в самого себе.*

Приклади 8.2. *1. Поліном $f(x_1, x_2) = 7x_1^2 x_2 - 3x_1 x_2 + 2x_1 + 2x_2 + 7x_1 x_2^2 - 4$ є симетричним відносно x_1, x_2.*

2. З прикладами симетричних поліномів ми зустрічались у формулах Вієта:

$$x_1 + x_2 + \cdots + x_n = \sigma_1,$$

$$x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n = \sigma_2,$$

$$\cdots,$$

$$x_1 x_2 \ldots x_n = \sigma_n. \tag{8.1}$$

Поліноми $\sigma_1, \sigma_2, \ldots, \sigma_n$ називаються **елементарними симетричними поліномами**.

Із означення симетричних поліномів випливають їх основні **властивості.**

1. Якщо симетричний поліном $f(x_1, x_2, \ldots, x_n)$ містить деякий член $ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$, то він містить і член, утворений з попереднього довільною підстановкою множини $k_1, k_2, \ldots, k_n$.

Дійсно, якщо член $ax_{i_1}^{k_1} x_{i_2}^{k_2} \ldots x_{i_n}^{k_n}$ утворений з $ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ підстановкою $\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix}$, то він є членом деякого полінома $f(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$, утвореного із $f(x_1, x_2, \ldots, x_n)$ цією ж підстановкою, звідки із симетричності полінома $f(x_1, x_2, \ldots, x_n)$ отримаємо $f(x_1, x_2, \ldots, x_n) = f(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$, тобто поліном $f(x_1, x_2, \ldots, x_n)$ теж містить член $ax_{i_1}^{k_1} x_{i_2}^{k_2} \ldots x_{i_n}^{k_n}$.

2. Якщо $ax_1^{k_1}x_2^{k_2}\dots x_i^{k_i}x_{i+1}^{k_{i+1}}\dots x_n^{k_n}$ - вищий член симетричного полінома, то $k_1 \geq k_2 \geq ... \geq k_n$.

Дійсно, якщо для деякого i $(i = 1, 2, \dots, n-1)$ матимемо $k_i < k_{i+1}$, то член $ax_1^{k_1}x_2^{k_2}\dots x_i^{k_i}x_{i+1}^{k_{i+1}}\dots x_n^{k_n}$ не буде вищим за член $ax_1^{k_1}x_2^{k_2}\dots x_i^{k_{i+1}}x_{i+1}^{k_i}\dots x_n^{k_n}$ того ж симетричного полінома, що суперечить умові. Одночлен $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$, для якого $i_1 \geq i_2 \geq \dots \geq i_n$, називають **монотонним**.

3. Вищий член довільного симетричного полінома можна подати як вищий член деякого добутку елементарних симетричних поліномів.

Зокрема, вищий член $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ полінома $f(x_1, x_2, \dots, x_n)$, співпадає з вищим членом полінома $a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdot\dots\cdot\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}$
.

Дійсно, вищими членами елементарних симетричних поліномів $\sigma_1, \sigma_2, \dots, \sigma_{n-1}, \sigma_n$ є відповідно $x_1, x_1x_2, \dots, x_1x_2\dots x_{n-1}, x_1x_2\dots x_n$, а оскільки вищий член добутку поліномів дорівнює добутку вищих членів співмножників, то вищим членом останнього полінома буде:

$$\begin{aligned} &ax_1^{k_1-k_2}(x_1x_2)^{k_2-k_3}(x_1x_2x_3)^{k_3-k_4}\dots \\ &\qquad \dots(x_1x_2\dots x_{n-1})^{k_{n-1}-k_n}(x_1x_2\dots x_n)^{k_n} = ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}. \end{aligned}$$

4. Сума, різниця і добуток симетричних поліномів над деяким полем F є симетричними поліномами над цим полем.

Із цієї очевидної властивості випливає, що множина всіх симетричних поліномів із кільця $F[x_1, x_2, \dots, x_n]$ всіх поліномів від n змінних над полем F утворює підкільце, яке називають **кільцем симетричних поліномів** від n змінних над полем F.

8.2 Основна теорема про симетричні поліноми

Теорема 8.3. *(Основна теорема про симетричні поліноми). Довільний симетричний поліном $f(x_1, x_2, \ldots, x_n)$ від n змінних над полем F можна однозначно подати у вигляді полінома від елементарних симетричних поліномів $\sigma_1, \sigma_2, \ldots, \sigma_n$ з коефіцієнтами, які належать полю F.*

Доведення. Із того, що кожний симетричний поліном $f(x_1, x_2, \ldots, x_n)$ можна подати як деяку суму однорідних симетричних поліномів (оскільки довільний поліном $f(x_1, x_2, \ldots, x_n)$ є сумою кількох однорідних поліномів різних степенів), отже достатньо довести теорему для випадку однорідних симетричних поліномів.

а) *Можливість* подання. Нехай $a_0 x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ - вищий член деякого однорідного симетричного полінома $f(x_1, x_2, \ldots, x_n)$ степеня m. Утворимо поліном $f_1 = f - a_0 \sigma_1^{k_1-k_2} \sigma_2^{k_2-k_3} \cdot \ldots \cdot \sigma_{n-1}^{k_{n-1}-k_n} \sigma_n^{k_n} = f - \varphi_0$, який теж є однорідним симетричним (як різниця однорідних симетричних поліномів). Оскільки вищі члени поліномів f і φ_0 однакові (властивість 3 симетричних поліномів), то вищий член полінома f_1 буде нижчим за вищий член полінома f.

Нехай тепер $a_1 x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ - вищий член полінома f_1. Аналогічно, $f_2 = f_1 - a_1 \sigma_1^{l_1-l_2} \sigma_2^{l_2-l_3} \cdot \ldots \cdot \sigma_n^{l_n} = f_1 - \varphi_1$ - теж однорідний симетричний поліном, вищий член якого є нижчим за вищий член полінома f_1 і так далі.

Процес отримання послідовності поліномів $f, f_1, f_2, \ldots$ не є нескінченним, оскільки вищий член кожного полінома f_i є вищим від вищого члена полінома f_{i+1}, тому вищі члени всіх цих поліномів є попарно неподібними членами вигляду $a x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ степеня m, кількість яких очевидно скінченна.

Нехай процес завершується на $(r+1)$ кроці, тобто

$$f_{r+1} = f_r - a_r\sigma_1^{t_1-t_2}\sigma_2^{t_2-t_3}\cdot\dots\cdot\sigma_n^{t_n} = f_r - \varphi_r = 0.$$

В результаті отримаємо рівність $f = a_0\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdot\dots\cdot\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n} + a_1\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdot\dots\cdot\sigma_n^{l_n} + \dots + a_r\sigma_1^{t_1-t_2}\sigma_2^{t_2-t_3}\cdot\dots\cdot\sigma_n^{t_n} = \varphi_0 + \varphi_1 + \varphi_2 + \dots + \varphi_r$, яка і дає шукане подання симетричного полінома від n змінних над полем F у вигляді полінома від елементарних симетричних поліномів з коефіцієнтами з поля F:

$$f(x_1, x_2, \dots, x_n) = \varphi(\sigma_1, \sigma_2, \dots, \sigma_n). \tag{8.2}$$

б) *Єдиність* подання. Покажемо спочатку, що якщо поліном $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ від елементарних симетричних поліномів $\sigma_1, \sigma_2, \dots, \sigma_n$ відмінний від нуля, то й поліном $\bar{\varphi}(x_1, x_2, \dots, x_n)$ від змінних $x_1, x_2, \dots, x_n$, який отримують із $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ заміною $\sigma_1, \sigma_2, \dots, \sigma_n$ їх виразеннями через $x_1, x_2, \dots, x_n$, теж відмінний від нуля.

Замінивши в довільному, відмінному від нуля, члені $a\sigma_1^{k_1}\sigma_2^{k_2}\cdot\dots\cdot\sigma_n^{k_n}$ полінома $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n)$ змінні $\sigma_1, \sigma_2, \dots, \sigma_n$ їх вираженнями через $x_1, x_2, \dots, x_n$, отримаємо деякий поліном від змінних $x_1, x_2, \dots, x_n$, вищим членом якого є

$$ax_1^{k_1}(x_1x_2)^{k_2}\dots(x_1x_2\dots x_n)^{k_n} = ax_1^{m_1}x_2^{m_2}\dots x_n^{m_n},$$

де $m_1 = k_1 + k_2 + \dots + k_{n-1} + k_n, m_2 = k_2 + \dots + k_{n-1} + k_n, \dots, m_{n-1} = k_{n-1} + k_n$, $m_n = k_n$, звідки $k_1 = m_1 - m_2, k_2 = m_2 - m_3, \dots, k_{n-1} = m_{n-1} - m_n, k_n = m_n$.

Останні рівності показують однозначний взаємозв'язок показників $k_1, k_2, \dots, k_n$ члена $a\sigma_1^{k_1}\sigma_2^{k_2}\cdot\dots\cdot\sigma_n^{k_n}$ та показників $m_1, m_2, \dots, m_n$ вищого члена полінома, який з нього отримують, звідки випливає, що поліноми, утворені з різних членів полінома $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ заміною в них $\sigma_1, \sigma_2, \ldots, \sigma_n$ їх вираженнями через $x_1, x_2, \ldots, x_n$, мають різні (неподібні) вищі члени, оскільки в іншому випадку два поліноми мали б ті самі показники $m_1, m_2, \ldots, m_n$, а тоді і показники членів полінома $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$, з яких утворилися ці два поліноми, були б однаковими і, значить, ці члени теж були б подібними.

Замінимо в кожному відмінному від нуля члені полінома $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ змінні $\sigma_1, \sigma_2, \ldots, \sigma_n$ їх вираженнями через $x_1, x_2, \ldots, x_n$, знайдемо в кожному із утворених поліномів від змінних $x_1, x_2, \ldots, x_n$ вищі члени і відберемо із них вищий, який, згідно попередніх міркувань, не має серед них подібних. Як вищий серед усіх вищих членів, він є вищим і від усіх інших членів полінома $\bar{\varphi}(x_1, x_2, \ldots, x_n)$ і тому не знищиться жодним іншим членом цього полінома. Таким чином, в поліномі $\bar{\varphi}(x_1, x_2, \ldots, x_n)$ є, принаймні, один відмінний від нуля член, і тому поліном $\bar{\varphi}(x_1, x_2, \ldots, x_n)$ є відмінним від нуля.

Перейдемо тепер до безпосереднього доведення твердження теореми.

Нехай для деякого симетричного полінома $f(x_1, x_2, \ldots, x_n)$ існує два різні подання у вигляді полінома від $\sigma_1, \sigma_2, \ldots, \sigma_n$: $f(x_1, x_2, \ldots, x_n) = \varphi_1(\sigma_1, \sigma_2, \ldots, \sigma_n)$ і $f(x_1, x_2, \ldots, x_n) = \varphi_2(\sigma_1, \sigma_2, \ldots, \sigma_n)$.

Тоді $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) = \varphi_1(\sigma_1, \sigma_2, \ldots, \sigma_n) - \varphi_2(\sigma_1, \sigma_2, \ldots, \sigma_n)$ є відмінним від нуля поліномом від змінних $\sigma_1, \sigma_2, \ldots, \sigma_n$, а тому, згідно доведеного вище, поліном $\bar{\varphi}(x_1, x_2, \ldots, x_n)$, утворений заміною в $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ змінних $\sigma_1, \sigma_2, \ldots, \sigma_n$ їх вираженнями через $x_1, x_2, \ldots, x_n$, теж відмінний від нуля, що неможливо, оскільки при цій заміні кожний із поліномів $\varphi_1(\sigma_1, \sigma_2, \ldots, \sigma_n)$ і $\varphi_2(\sigma_1, \sigma_2, \ldots, \sigma_n)$ перетворюється в той самий поліном $f(x_1, x_2, \ldots, x_n)$. Таким чином, припущення про існування двох різних зображень полінома $f(x_1, x_2, \ldots, x_n)$ є невірним, оскільки привело до суперечності. $\square$

Із основної теореми про симетричні поліноми випливає наступний наслідок.

Наслідок 8.4. *Якщо $f(x)$ - поліном n степеня від однієї змінної x над полем F з коренями $\alpha_1, \alpha_2, \ldots, \alpha_n$ (які можуть не належати F), то будь-який симетричний поліном $g(x_1, x_2, \ldots, x_n)$ над полем F при $x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_n = \alpha_n$ набуває значення, яке є елементом поля F.*

Доведення. Нехай $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ - довільний поліном n степеня від однієї змінної x, корені якого $\alpha_1, \alpha_2, \ldots, \alpha_n$, можуть не належати полю F. Згідно основної теореми про симетричні поліноми, довільний симетричний поліном можна подати у вигляді полінома від елементарних симетричних поліномів з коефіцієнтами із поля F: $g(x_1, x_2, \ldots, x_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$. При $x_1 = \alpha_1$, $x_2 = \alpha_2, \ldots, x_n = \alpha_n$ матимемо $g(\alpha_1, \alpha_2, \ldots, \alpha_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$. За формулами Вієта елементарні симетричні поліноми дорівнюють

$$\sigma_1(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1 + \alpha_2 + \cdots + \alpha_n = -\frac{a_1}{a_0},$$

$$\sigma_2(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n = \frac{a_2}{a_0},$$

$$\cdots,$$

$$\sigma_n(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1\alpha_2 \ldots \alpha_n = (-1)^n\frac{a_n}{a_0}.$$

Тому $g(\alpha_1, \alpha_2, \ldots, \alpha_n) = \varphi(-\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, (-1)^n\frac{a_n}{a_0})$.

Із того, що права частина (як результат виконання операцій над елементами з поля F) належить полю F, випливає, що й ліва частина $g(\alpha_1, \alpha_2, \ldots, \alpha_n)$ належить F. $\square$

Через $s(ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n})$ позначають суму всіх членів вигляду $a_0x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ при всеможливих перестановках змінних.

Приклад 8.5. *Симетричний поліном $f = s(x_1^2x_2^2)$ від n змінних виразити через елементарні симетричні поліноми.*

Скористаємось методом невизначених коефіцієнтів. Оскільки кожний доданок полінома f має степінь 4, то розглянемо всеможливі поліноми від елементарних симетричних поліномів такого ж степеня (враховуючи і степені самих елементарних поліномів): σ_1^4, $\sigma_1^2\sigma_2$, $\sigma_1\sigma_3$, σ_2^2, σ_4. Серед цих поліномів виберемо ті, котрі містять змінні x_i в степені, не більшому за 2. Такими будуть: $\sigma_1\sigma_3$, σ_2^2, σ_4. Отже $f = A\sigma_1\sigma_3 + B\sigma_2^2 + C\sigma_4$. Для того, щоб знайти коефіцієнти A, B, C потрібно розглянути задану рівність на конкретних числових наборах значень змінних $x_1, \ldots, x_n$.

x_1	x_2	x_3	x_4	x_5	$\cdots$	f	σ_1	σ_2	σ_3	σ_4
1	*1*	*0*	*0*	*0*	$\cdots$	*1*	*2*	*1*	*0*	*0*
1	*1*	*1*	*0*	*0*	$\cdots$	*3*	*3*	*3*	*1*	*0*
1	*1*	*1*	*1*	*0*	$\cdots$	*6*	*4*	*6*	*4*	*1*

Звідки отримаємо лінійну систему рівнянь:

$$\begin{cases} 1 = B, \\ 3 = 3A + 9B, \\ 6 = 16A + 36B + C, \end{cases} \Rightarrow \quad \begin{array}{l} B = 1, \\ A = -2, \\ C = 2. \end{array}$$

Тобто $f = -2\sigma_1\sigma_3 + \sigma_2^2 + 2\sigma_4$.

8.3 Степеневі суми

Симетричні поліноми від змінних $x_1, x_2, \ldots, x_n$ вигляду $S_k = x_1^{k_1} + x_2^{k_2} + \cdots + x_n^{k_n}$ $(k \in \mathbb{N})$, які називають **степеневими сумами**, широко використовуються в алгебрі і часто потребують швидкого обчислення. Задача вираження степеневої суми S_k через елементарні симетричні поліноми при зростанні показника k стає громіздкою, тому запишемо рекурентні співвідношення для послідовного знаходження цих сум через $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Для $k \le n$, $n \in \mathbb{N}$ виконуються такі рівності:

$$S_{k-1}\sigma_1 = S_k + s(x_1^{k-1}x_2),$$

$$S_{k-2}\sigma_2 = s(x_1^{k-1}x_2) + s(x_1^{k-2}x_2x_3),$$

$$\cdots,$$

$$S_{k-m}\sigma_m = s(x_1^{k-m+1}x_2\ldots x_m)+s(x_1^{k-m}x_2\ldots x_mx_{m+1})\ (2 \le m \le k-2),$$

$$\cdots,$$

$$S_1\sigma_{k-1} = s(x_1^2x_2\ldots x_{k-1}) + k\sigma_k. \tag{8.3}$$

Для $k > n$, $n \in \mathbb{N}$ виконуються наступні рівності:

$$S_{k-1}\sigma_1 = S_k + s(x_1^{k-1}x_2),$$

$$S_{k-2}\sigma_2 = s(x_1^{k-1}x_2) + s(x_1^{k-2}x_2x_3),$$

$$\cdots,$$

$$S_{k-m}\sigma_m = s(x_1^{k-m+1}x_2\ldots x_m)+s(x_1^{k-m}x_2\ldots x_mx_{m+1})\ (2 \le m \le n-1),$$

$$\cdots,$$

$$S_{k-n}\sigma_n = s(x_1^{k-n+1}x_2\ldots x_n). \tag{8.4}$$

Спосіб доведення записаних рівностей розглянемо на прикладі другої з них. $S_{k-2}\sigma_2 = (x_1^{k-2} + x_2^{k-2} + \cdots + x_n^{k-2})(x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n) = (x_1^{k-1}x_2 + x_1^{k-1}x_3 + \cdots +$

$x_1^{k-1}x_n + x_2^{k-1}x_1 + x_2^{k-1}x_3 + \cdots + x_2^{k-1}x_n + x_n^{k-1}x_1 + x_n^{k-1}x_2 + \cdots + x_n^{k-1}x_{n-1}) + (x_1^{k-2}x_2x_3 + x_1^{k-2}x_3x_4 + \cdots + x_1^{k-2}x_{n-1}x_n + x_2^{k-2}x_1x_3 + x_2^{k-2}x_1x_4 + \cdots + x_2^{k-2}x_1x_n + \cdots + x_n^{k-2}x_1x_2 + \cdots + x_n^{k-2}x_{n-2}x_{n-1}) = s(x_1^{k-1}x_2) + s(x_1^{k-2}x_2x_3)$.

Помноживши i-ті рівності із (8.3) та (8.4) на $(-1)^i$ (де $i = 1, 2, \ldots, k-1$ та $i = 1, 2, \ldots, n$ відповідно), додавши утворені рівності і перенісши всі члени в одну частину, отримаємо наступні співвідношення:

$$S_k - S_{k-1}\sigma_1 + S_{k-2}\sigma_2 - \cdots + (-1)^{k-1}S_1\sigma_{k-1} + (-1)^k\sigma_k = 0, \ (k \leq n) \tag{8.5}$$

$$S_k - S_{k-1}\sigma_1 + S_{k-2}\sigma_2 - \cdots + (-1)^n S_{k-n}\sigma_n = 0. \ (k > n) \tag{8.6}$$

Останні два співвідношення називають **формулами Ньютона.**

Приклади 8.6. *Нехай $k \leq n$. Користуємось співвідношенням* (8.5).

$k = 1.$ $\quad S_1 = \sigma_1.$

$k = 2.$ $\quad S_2 - S_1\sigma_1 + 2\sigma_2 = 0$. Звідси $S_2 = \sigma_1^2 - 2\sigma_2$.

$k = 3.$ $\quad S_3 - S_2\sigma_1 + S_1\sigma_2 - 3\sigma_3 = 0$. Підставивши сюди отримані вирази для S_1 та S_2, матимемо, що $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Нехай $k > n$. Користуємось співвідношенням (8.6).

$k = 2, \ n = 1.$ $S_2 - S_1\sigma_1 = 0$, звідси $S_2 = \sigma_1^2$.

$k = 3, \ n = 2.$ $S_3 - S_2\sigma_1 + S_1\sigma_2 = 0$, звідси $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2$.

8.4 Дискримінант полінома

В кільці $F[x_1, x_2, \ldots, x_n]$ розглянемо поліном $\Delta_n = \prod\limits_{1 \le j < i \le n} (x_i - x_j)$, який можна подати у вигляді визначника Вандермонда

$$\Delta_n = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix}.$$

Оскільки визначник є функцією своїх стовпчиків, то довільна підстановка індексів (елемент симетричної групи) спричинить деяку перестановку місцями цих стовпчиків, що призведе тільки до можливої зміни знаку визначника. Тому Δ_n^2 буде поліномом симетричним і, згідно основної теореми про симетричні поліноми, його можна виразити у вигляді полінома від елементарних симетричних поліномів $\sigma_1, \sigma_2, \ldots, \sigma_n$:

$$\Delta_n^2 = \prod_{i \ne j} (x_i - x_j)^2 = D(\sigma_1, \sigma_2, \ldots, \sigma_n). \tag{8.7}$$

Поліном $D(\sigma_1, \sigma_2, \ldots, \sigma_n)$ від $\sigma_1(x_1, x_2, \ldots, x_n), \sigma_2(x_1, x_2, \ldots, x_n), \ldots, \sigma_n(x_1, x_2, \ldots, x_n)$ називають *дискримінантом сімейства* $x_1, x_2, \ldots, x_n$.

Для знаходження $D(\sigma_1, \sigma_2, \ldots, \sigma_n)$ скористаємось тим, що $\Delta_n^2 = \Delta_n \cdot \Delta_n^t$, оскільки $det\,\Delta_n^t = det\,\Delta_n$ (Δ_n^t -транспонований визначник Δ_n). Скориставшись правилом множення матриць, отримаємо

$$D(\sigma_1, \sigma_2, \ldots, \sigma_n) = \begin{vmatrix} n & S_1 & S_2 & \ldots & S_{n-1} \\ S_1 & S_2 & S_3 & \ldots & S_n \\ S_2 & S_3 & S_4 & \ldots & S_{n+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ S_{n-1} & S_n & S_{n+1} & \ldots & S_{2n-2} \end{vmatrix}, \tag{8.8}$$

де $S_k = x_1^k + x_2^k + \cdots + x_m^k$ $(k \in \mathbb{N})$- відомі нам степеневі суми. Обчисливши їх за відповідними рекурентними формулами, отримаємо явне вираження для $D(\sigma_1, \sigma_2, \ldots, \sigma_n)$.

Приклад 8.7. *Обчислити $D(\sigma_1, \sigma_2)$. Враховуючи, що $S_1 = \sigma_1$ і $S_2 = \sigma_1^2 - 2\sigma_2$, матимемо*

$$D(\sigma_1, \sigma_2) = \begin{vmatrix} 2 & \sigma_1 \\ \sigma_1 & \sigma_1^2 - 2\sigma_2 \end{vmatrix} = \sigma_1^2 - 4\sigma_2.$$

Дамо тепер означення дискримінанта полінома.

Нехай $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ - довільний нормований поліном з кільця $F[x]$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ – його корені (належать полю F або деякому його розширенню). Із формул Вієта маємо, що $\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^k a_k$.

Означення 8.8. *Дискримінант сімейства коренів $\alpha_1, \alpha_2, \ldots, \alpha_n$ полінома $f(x)$ (інакше, значення дискримінанта $D(\sigma_1, \sigma_2, \ldots, \sigma_n)$ при заміні $(-1)^k a_k$ замість σ_k), називається* **дискримінантом полінома** *$f(x)$ і позначається символом $D(f)$.*

Із означення дискримінанта випливає важливе твердження: $D(f) = 0$ *тоді і тільки тоді, коли поліном $f(x)$ має кратні корені.*

Приклади 8.9. *1. Обчислимо дискримінант нормованого полінома другого степеня $f(x) = x^2 + a_1x + a_2$.*

$$D(f) = \begin{vmatrix} 2 & S_1 \\ S_1 & S_2 \end{vmatrix} = \begin{vmatrix} 2 & \sigma_1 \\ \sigma_1 & \sigma_1^2 - 2\sigma_2 \end{vmatrix} = \sigma_1^2 - 4\sigma_2 = a_1^2 - 4a_2.$$

2. Обчислимо дискримінант нормованого полінома третього сте-

пеня $f(x) = x^3 + a_1x^2 + a_2x + a_3$.

$$D(f) = \begin{vmatrix} n & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{vmatrix}.$$

За рекурентними формулами отримаємо, що $S_1 = \sigma_1$, $S_2 = \sigma_1^2 - 2\sigma_2$, $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, $S_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2$, *звідки* $S_1 = -a_1$, $S_2 = a_1^2 - 2a_2$, $S_3 = -a_1^3 + 3a_1a_2 - 3a_3$, $S_4 = a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2$ *(оскільки* $\sigma_4 = 0$*).*

$$D(f) = \begin{vmatrix} n & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{vmatrix} = 3S_2S_4 + 2S_1S_2S_3 + S_2^3 - S_1^2S_4 - 3S_3^2 =$$

$$= a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 + 18a_1a_2a_3 - 27a_3^2.$$

Для неповного $(a_1 = 0)$ *полінома третього степеня* $f(x) = x^3 + a_2x + a_3$ *матимемо*

$$D(f) = -4a_2^3 - 27a_3^2.$$

8.5 Результант поліномів

Умова $D(f) = 0$ рівносильна наявності у полінома кратного кореня, що є критерієм наявності у цього полінома і його похідної спільного кореня (спільного множника), перевірка чого зводиться до алгоритму Евкліда. У зв'язку з цим, ймовірно, існує аналогічний критерій наявності спільного кореня (множника) для двох довільних поліномів $f(x), g(x) \in F[x]$.

Нехай

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n,$$
$$g(x) = b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m.$$

Означення 8.10. *Результантом $R(f, g)$ поліномів $f(x)$, $g(x) \in F[x]$ називається визначник*

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & \dots & \dots & a_n & \dots & \dots \\ & a_0 & a_1 & \dots & \dots & \dots & a_n & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & a_0 & a_1 & \dots & \dots & \dots & a_n \\ b_0 & b_1 & \dots & \dots & \dots & b_m & \dots & \dots \\ & b_0 & b_1 & \dots & \dots & \dots & b_m & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & b_0 & b_1 & \dots & \dots & \dots & b_m \end{vmatrix}, \qquad (8.9)$$

перші m рядків якого займають коефіцієнти полінома $f(x)$, а наступні n – полінома $g(x)$ (порожні місця заповнюються нулями).

Властивості результанта.

1.Умова $R(f, g) = 0$ виконується тоді і тільки тоді, коли $a_0 = b_0 = 0$ або $f(x)$ і $g(x)$ мають в $F[x]$ спільний множник ненульового степеня.

Напочатку переконаємось, що друга частина твердження виконується тоді і тільки тоді, коли існують поліноми $f_1(x), g_1(x)$, одночасно не рівні нулю, для яких

$$fg_1 + f_1g = 0, \ \deg f_1 < n, \ \deg g_1 < m. \qquad (8.10)$$

Дійсно, якщо $(f, g) = d, \deg d > 0$, то $f = f_1d$, $g = -g_1d$ і, значить, $fg_1 + f_1g = f_1dg_1 - f_1g_1d = 0$, при цьому $\deg f_1 < n, \deg g_1 < m$.

Якщо ж $a_0 = b_0 = 0$, то покладемо $f_1 = f,\ g_1 = -g$.

Навпаки, при виконанні умов (8.10), припущенні $(f, g) = 1$, та врахуванні єдиності розкладу в $F[x]$ на прості множники отримаємо, що із $fg_1 = -f_1 g$ випливає $f_1 \vdots f,\ g_1 \vdots g$, тобто $\deg f < n, \deg g < m$, звідки $a_0 = b_0 = 0$.

Доведемо тепер еквівалентність умов (8.10) та $R(f, g) = 0$. Нехай

$$\begin{aligned} f_1(x) &= a_0^{'} x^{n-1} + a_1^{'} x^{n-2} + \cdots + a_{n-1}^{'}, \\ g_1(x) &= b_0^{'} x^{m-1} + b_1^{'} x^{m-2} + \cdots + b_{m-1}^{'}. \end{aligned}$$

Обчислимо коефіцієнти полінома $fg_1 + f_1 g$ степеня $\leq n+m-1$ і запишемо умову (8.10) у вигляді квадратної однорідної системи лінійних рівнянь з $(n+m)$ невідомими $a_0^{'}, a_1^{'}, \ldots, a_{n-1}^{'}, b_0^{'}, b_1^{'}, \ldots, b_{m-1}^{'}$:

$$\begin{cases} a_0 b_0^{'} + \ldots\ldots\ldots\ldots\ldots\ldots + b_0 a_0^{'} + \ldots\ldots\ldots\ldots\ldots\ldots = 0, \\ a_1 b_0^{'} + a_0 b_1^{'} + \ldots\ldots\ldots\ldots + b_1 a_0^{'} + b_0 a_1^{'} + \ldots\ldots\ldots\ldots = 0, \\ a_2 b_0^{'} + a_1 b_1^{'} + a_0 b_2^{'} + \cdots + b_2 a_0^{'} + b_1 a_1^{'} + b_0 a_2^{'} + \cdots = 0, \\ \ldots\ldots \end{cases}$$

$$A = \begin{bmatrix} a_0 & \cdots & \cdots & \cdots & b_0 & \cdots & \cdots & \cdots \\ a_1 & a_0 & \cdots & \cdots & b_1 & b_0 & \cdots & \cdots \\ a_2 & a_1 & a_0 & \cdots & b_2 & b_1 & b_0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}.$$

Визначник матриці A, яка утворена з коефіцієнтів біля невідомих, (насправді, визначник транспонованої матриці A) співпадає із $R(f, g)$. Таким чином, отримана однорідна система має ненульовий розв'язок тільки тоді, коли $R(f, g) = 0$, а довільний ненульовий розв'язок і дає пару поліномів f_1, g_1, які задовольняють умову (8.10.)

2.Якщо F – поле, в якому містяться всі корені $\alpha_1, \alpha_2, \ldots, \alpha_n$ та $\beta_1, \beta_2, \ldots, \beta_m$ поліномів $f(x)$ і $g(x)$ відповідно, то

$$R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j) = a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j).$$

Для доведення розглянемо загальний випадок, коли всі $g(\alpha_i)$ та $f(\beta_j)$, де $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$, є попарно різними. Оскільки $R(f,g) = (-1)^{mn} R(g, f)$ (що випливає із означення), то для доведення досить переконатися у справедливості першого співвідношення. Для цього введемо нову змінну y і над кільцем $F[y]$ розглянемо поліноми $f(x)$, $g(x) - y$. Із означення результанта, після заміни b_m на $b_m - y$, отримаємо, що $R(f, g - y) = (-1)^n a_0^m y^n + \cdots + R(f,g)$ – поліном n-го степеня відносно змінної y зі старшим коефіцієнтом $(-1)^n a_0^m$ і вільним членом $R(f,g)$. Поліноми $f(x)$ і $g(x) - g(\alpha_i)$, маючи спільний корінь α_i, діляться на $x - \alpha_i$, тому, згідно властивості 1, їхній результант дорівнює нулю, тобто $R(f, g - g(\alpha_i)) = 0$.

Поліном $R(f, g - y)$, згідно теореми Безу, має ділитися на $y - g(\alpha_i)$, а оскільки всі $g(\alpha_i)$ є різними, то

$$R(f, g - y) = (-1)^n a_0^m \prod_{i=1}^{n} (y - g(\alpha_i)) = a_0^m \prod_{i=1}^{n} (g(\alpha_i) - y),$$

звідки (при $y = 0$) і отримується потрібний вираз.

Поширимо введене вище означення **дискримінанта** на випадок довільних (ненормованих) поліномів, вважаючи

$$D(f) = a_0^{2n-2} \prod_{1 \le j < i \le n} (\alpha_i - \alpha_j)^2 = [a_0^{n-1} \prod_{1 \le j < i \le n} (\alpha_i - \alpha_j)]^2, \; a_0 \ne 0.$$

3.Між дискримінантом полінома та результантом цього полінома і його похідною існує наступний зв'язок:

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} R(f, f'). \qquad (8.11)$$

Згідно властивості 2: $R(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i)$. Для знаходження $f'(\alpha_i)$ запишемо поліном $f(x)$ в полі його розкладу: $f(x) = a_0 \prod_{j=1}^{n} (x - \alpha_j)$, продиференціюємо цей вираз: $f'(x) = a_0 \sum_{i=1}^{n} \prod_{j \neq i} (x - \alpha_j)$ і покладемо $x = \alpha_i$. Отримане співвідношення $f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j)$ підставимо у вираз для результанта:

$$R(f, f') = a_0^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) = a_0(-1)^{\frac{n(n-1)}{2}} a_0^{2n-2} \prod_{j<i} (\alpha_i - \alpha_j)^2$$
$$= a_0(-1)^{\frac{n(n-1)}{2}} D(f),$$

звідки і випливає явне вираження дискримінанта полінома через результант цього полінома і його похідної.

Вправи 8.11. *(1) Подати у вигляді полінома від елементарних симетричних поліномів:*

(а) $f(x_1, x_2) = x_1^2 + 3x_1x_2 + x_2^2$;

(б) $f(x_1, x_2, x_3) = x_1^2x_2^2x_3^2 - 2x_1x_2 - 2x_1x_3 - 2x_2x_3$.

(2) Знайти дискримінант полінома $f(x)$:

(а) $f(x) = x^3 + 2x^2 - x - 2$;

(б) $f(x) = (x - 1)(x + 1)(x + 2)$.

(3) Знайти результант поліномів $f(x)$ *і* $g(x)$:

(а) $f(x) = 2x^3 - 3x^2 + x - 1$, $g(x) = 3x^2 - x + 2$;

(б) $f(x) = (x - 1)(x + 2)$, $g(x) = (x - 2)(x + 3)^2$.

9 Поліноми над числовими полями

9.1 Основна теорема алгебри

Свою гучну назву теорема, про яку піде мова, отримала ще тоді, коли одним із головних завдань алгебри було розв'язання алгебраїчних рівнянь. Відома вона також під назвами "основна теорема алгебри комплексних чисел", "теорема про існування кореня", "теорема про алгебраїчну замкнутість поля комплексних чисел", "основна теорема теорії поліномів". Подамо різні формулювання цього фундаментального твердження.

Теорема 9.1. *(Основна теорема алгебри комплексних чисел).*

a. Поле комплексних чисел є алгебраїчно замкнутим.

Інше формулювання (в термінах коренів):

b. Довільний поліном степеня $n \geq 1$ з довільними числовими коефіцієнтами має n комплексних коренів із врахуванням їх кратності.

Зауваження 9.2. *Якщо довільний поліном $f(x) \in F[x]$ має в полі F хоча б один корінь, то поле F є алгебраїчно замкнутим.*

Дійсно, тоді $f(x) = (x - \alpha_1) f_1(x),\ \alpha_1 \in F,\ f_1(x) \in F[x]$, однак за умовою для полінома $f_1(x)$ в F теж існує хоча б один корінь, тобто $f_1(x) = (x - \alpha_2) f_2(x), \alpha_2 \in F,\ f_2(x) \in F[x]$. Продовження цього процесу приведе до повного розкладу полінома $f(x)$ на лінійні множники, тобто поле F для довільного полінома $f(x)$ є алгебраїчно замкнутим.

У зв'язку із цим зауваженням, для доведення алгебраїчної замкнутості поля комплексних чисел достатньо встановити існування у довільного полінома хоча б одного комплексного кореня. Тому розглянемо ще одне формулювання основної теореми і доведемо її одним із відомих способів, в якому максимально використовується алгебраїчний апарат:

с. Довільний поліном ненульового степеня з довільними числовими коефіцієнтами має хоча б один комплексний корінь.

Неалгебраїчна частина доведення цієї теореми містить дві наступні леми.

Лема 9.3. *Для всіх $x \in R$, досить великих за абсолютною величиною, знак полінома $f(x)$ степеня $n \geq 1$ з дійсними коефіцієнтами співпадає із знаком його старшого члена a_0x^n.*

Доведення. Нехай $A = max\{|a_1|, |a_2|, \ldots, |a_n|\}$ і $r = \frac{A}{|a_0|} + 1$. Якщо вибрати $|x| > r$ (≥ 1), то отримаємо $|a_0| > \frac{A}{|x|-1}$, звідки

$$|a_0x^n| = |a_0||x^n| > \frac{A|x^n|}{|x|-1} > \frac{A(|x|^n - 1)}{|x|-1} =$$

$$= A(|x|^{n-1} + \cdots + |x| + 1) \geq |a_1||x|^{n-1} + \cdots + |a_{n-1}||x| + |a_n| =$$

$$= |a_1x^{n-1}| + \cdots + |a_{n-1}x| + |a_n| \geq |a_1x^{n-1} + \cdots + a_{n-1}x + a_n|,$$

тобто $|a_0x^n| > |a_1x^{n-1} + \cdots + a_{n-1}x + a_n|$ (абсолютна величина старшого члена більша за абсолютну величину суми всіх інших членів полінома). Із отриманого висновку випливає, що при достатньо великому за абсолютною величиною значенні x знак полінома $f(x)$ співпадає із знаком його старшого члена. □

Лема 9.4. *Довільний поліном непарного степеня з дійсними коефіцієнтами має хоча б один дійсний корінь.*

Доведення. Якщо у довільного полінома $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ з дійсними коефіцієнтами степінь n є числом непарним, то старший член a_0x^n цього полінома при додатних і від'ємних значеннях x матиме протилежні знаки, у зв'язку з чим (згідно леми 9.3) при достатньо великих значеннях x поліном $f(x)$ також матиме протилежні знаки, тобто існуватимуть такі два різні значення x ($x = a$ та $x = b$), при яких значення полінома $f(x)$ ($f(a)$ та $f(b)$) будуть пролежні за знаком. Оскільки функція $f(x)$ є неперервною на всій дійсній осі (відомий висновок із курсу математичного аналізу), зокрема, і на відрізку $[a, b]$, то, застосувавши до цього відрізка теорему Больцано-Коші, отримаємо висновок про існування на ньому хоча б одного такого дійсного числа c, для якого $f(c) = 0$, звідки число c і є дійсним коренем полінома $f(x)$. □

Подальше доведення основної теореми алгебри комплексних чисел міститиме алгебраїчні міркування, зокрема, доведення наступної леми опиратиметься на наслідок з теореми про існування поля розкладу полінома та наслідок з основної теореми теорії симетричних поліномів.

Лема 9.5. *Довільний поліном степеня* $n \geq 1$ *з дійсними коефіцієнтами має хоча б один комплексний корінь.*

Доведення. Нехай $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ - довільний поліном з дійсними коефіцієнтами степеня $n = 2^m \cdot l$, де m - ціле невід'ємне число, а l - деяке непарне натуральне число (відомо, що у вигляді $n = 2^m \cdot l$ можна подати довільне натуральне число n).

Доведення виконаємо методом математичної індукції за числом m. При $m = 0$ показник степеня $n = l$ є непарним числом, тому, згідно леми 9.4, $f(x)$ має принаймні один комплексний корінь. Припустивши, що лема 9.5 справедлива для довільного полінома з дійсними коефіцієнтами степеня $2^{m-1} \cdot l_1$, $(l_1 \geq 0)$, доведемо її справедливість для довільного полінома з дійсними коефіцієнтами степеня $2^m \cdot l$.

Для полінома $f(x)$, що розглядається над полем C, існує поле розкладу $\overline{C}$, в якому $f(x)$ має n коренів $\alpha_1, \alpha_2, \ldots, \alpha_n$. Вибравши довільне дійсне число t, утворимо всеможливі елементи $\beta_{ij} = \alpha_i \alpha_j + t(\alpha_i + \alpha_j)$, $i < j$, число яких дорівнює кількості комбінацій з n елементів по два, тобто

$$C_n^2 = \frac{n(n-1)}{2} = \frac{2^m \cdot l(2^m \cdot l - 1)}{2} = 2^{m-1} \cdot l(2^m \cdot l - 1) = 2^{m-1} \cdot l_1,$$

де $l_1 = l(2^m \cdot l - 1)$ - непарне число.

Утворимо поліном $f_t(x) = \prod\limits_{1 \le i < j \le n} (x - \beta_{ij})$, степінь якого дорівнює $2^{m-1} \cdot l_1$, коренями якого є виключно числа β_{ij}, а коефіцієнти є поліномами від α_i, α_j з дійсними коефіцієнтами (оскільки t - число дійсне). Очевидно, що довільна підстановка множини $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ зумовить лише переставляння лінійних множників полінома

$$f_t(x) = \prod_{1 \le i < j \le n} (x - \beta_{ij}) = \prod_{1 \le i < j \le n} (x - (\alpha_i \alpha_j + t(\alpha_i + \alpha_j)))$$

без зміни самого полінома, що можливо тільки за умови, коли при довільній підстановці множини $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ не змінюються коефіцієнти полінома $f_t(x)$. Таким чином, коефіцієнти полінома $f_t(x)$ є симетричними поліномами від $\alpha_1, \alpha_2, \ldots, \alpha_n$ над полем R.

Згідно наслідку з основної теореми про симетричні поліноми, коефіцієнти полінома $f_t(x)$ є дійсними числами (оскільки $\alpha_1, \alpha_2, \ldots, \alpha_n$ є коренями $f(x)$ з дійсними коефіцієнтами), у зв'язку з цим, за припущенням індукції, поліном $f_t(x)$ має хоча б один комплексний корінь. Оскільки коренями полінома $f_t(x)$ є виключно елементи $\beta_{ij} =$

$\alpha_i\alpha_j + t(\alpha_i + \alpha_j),\ i < j$, то хоча б один із цих елементів має бути комплексним числом. Таким чином, для довільного дійсного числа t знайдеться така пара індексів i, j $(1 \le i < j \le n)$, що елемент $\beta_{ij} = \alpha_i\alpha_j + t(\alpha_i + \alpha_j),\ i < j$ поля $\overline{C}$ є комплексним числом, при цьому різним дійсним числам t відповідають різні пари індексів. Із того, що множина дійсних чисел нескінченна, а кількість всеможливих пар індексів скінченна, випливає, що існують такі два різних дійсних числа t_1 і t_2, яким буде відповідати та сама пара індексів i, j, для яких $\alpha_i\alpha_j + t_1(\alpha_i + \alpha_j) = \gamma_1$ та $\alpha_i\alpha_j + t_2(\alpha_i + \alpha_j) = \gamma_2$ є комплексними числами. Після віднімання другої рівності від першої отримаємо $(\alpha_i + \alpha_j)(t_1 - t_2) = \gamma_1 - \gamma_2$, звідки

$$\alpha_i + \alpha_j = \frac{\gamma_1 - \gamma_2}{t_1 - t_2}. \tag{9.1}$$

Підставивши знайдену суму до будь-якої із попередніх рівностей (наприклад, до першої), знайдемо добуток коренів: $\alpha_i\alpha_j + t_1\frac{\gamma_1-\gamma_2}{t_1-t_2} = \gamma_1$, звідси

$$\alpha_i\alpha_j = \gamma_1 - t_1\frac{\gamma_1 - \gamma_2}{t_1 - t_2}. \tag{9.2}$$

Із виразів (9.1) і (9.2) видно, що сума і добуток коренів α_i та α_j є комплексними числами, а, значить, що й самі корені α_i та α_j є комплексними числами, звідки випливає, що серед коренів $\alpha_1, \alpha_2, \ldots, \alpha_n$ полінома $f(x)$ є комплексні (причому навіть два). □

Перейдемо тепер до завершального етапу доведення основної теореми алгебри комплексних чисел.

Якщо коефіцієнти полінома $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ степеня $n \ge 1$ є комплексними числами, то, замінивши їх комплексно спряженими числами, отримаємо поліном $\bar{f}(x) = \bar{a}_0x^n + \bar{a}_1x^{n-1} + \cdots + \bar{a}_{n-1}x + \bar{a}_n$, де $\bar{a}_i$ $(i = 0, 1, 2, \ldots, n)$ є комплексним числом, спряженим з a_i. Утворимо поліном

$$f^*(x) = f(x)\cdot \bar{f}(x) = b_0x^{2n} + b_1x^{2n-1} + \cdots + b_{2n-1}x + b_{2n},$$

де $b_k = \sum\limits_{i+j=k} a_i\bar{a}_j$ $(k = 0,1,2,\ldots,2n)$. Згідно із властивостями спряжених комплексних чисел, запишемо, що $\bar{b}_k = \sum\limits_{i+j=k} \bar{a}_i a_j = \sum\limits_{i+j=k} a_i\bar{a}_j = b_k$, звідки випливає, що всі коефіцієнти полінома $f^*(x)$ є дійсними числами. Тоді, за лемою 9.5, поліном $f^*(x)$ має хоча б один комплексний корінь β , тобто $f^*(\beta) = f(\beta)\cdot\bar{f}(\beta) = 0$, звідки або $f(\beta) = 0$, або $\bar{f}(\beta) = 0$. Якщо $f(\beta) = 0$, то число β є коренем полінома $f(x)$. Якщо ж $\bar{f}(\beta) = 0$, то, після заміни в цій рівності всіх комплексних чисел спряженими з ними числами, отримаємо $a_0\bar{\beta}^n + a_1\bar{\beta}^{n-1} + \cdots + a_{n-1}\bar{\beta} + a_n = 0$, тобто $f(\bar{\beta}) = 0$, звідки $\bar{\beta}$ є коренем $f(x)$.

Таким чином, поліном $f(x)$ має хоча б один комплексний корінь.

Наслідок 9.6. *Довільний поліном, степінь якого вищий за одиницю, звідний у полі комплексних чисел.*

Доведення. Згідно з основною теоремою, довільний поліном $f(x)$ степеня $n > 1$ має хоча б один комплексний корінь α. За наслідком з теореми Безу $f(x)$ ділиться на $(x-\alpha)$, тобто $f(x) = (x-\alpha)\cdot f_1(x)$. Оскільки степінь $f(x)$ більший за одиницю, то степінь $f_1(x)$ більший нуля. □

Із останнього твердження випливає необхідна і достатня умова незвідності полінома у полі комплексних чисел.

Для того, щоб поліном був незвідним у полі комплексних чисел, необхідно і достатнь, щоб його степінь дорівнював одиниці.

Наслідок 9.7. *Кожний поліном степеня n над полем комплексних чисел єдиним способом (з точністю до порядку множників) розкладається в цьому полі на лінійні множники*

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n), \tag{9.3}$$

де a_0 - старший коефіцієнт полінома, $\alpha_1, \alpha_2, \dots, \alpha_n$ - його корені.

Доведення. Згідно теореми 4.3, кожний поліном над полем F можна розкласти в добуток незвідних множників у цьому полі однозначно з точністю до сталого множника. В полі комплексних чисел кожний незвідний поліном має перший степінь, тому кількість таких лінійних множників дорівнюватиме степеню цього полінома. Винісши старші коефіцієнти усіх лінійних множників за їх межі і позначивши їх добуток через A, отримаємо наступний розклад полінома $f(x)$:

$$f(x) = A(x+\beta_1)(x+\beta_2)\cdot\dots\cdot(x+\beta_n).$$

Прирівнявши старші коефіцієнти в обох частинах цієї рівності, матимемо, що $A = a_0$. Числа $-\beta_1, -\beta_2, \dots, -\beta_n$ є коренями полінома $f(x)$, оскільки $f(-\beta_i) = 0$, $i = 1, 2, \dots, n$. Замінивши A на a_0, а $-\beta_i$ на α_i, отримаємо шуканий розклад (9.3). Оскільки сталі множники для незвідних поліномів цілком визначені, то цей розклад єдиний з точністю до порядку множників. □

Із отриманого розкладу випливає, що жодне комплексне число, відмінне від α_i, не може бути коренем полінома $f(x)$. Таким чином, доведений наслідок можна сформулювати інакше:

довільний поліном степеня n в полі комплексних чисел має n коренів.

Оскільки всі корені полінома $f(x)$ над полем $\mathbb{C}$ комплексних чисел належать цьому ж полю, то поле $\mathbb{C}$ є полем розкладу для будь-якого полінома $f(x)$ з комплексними коефіцієнтами. Ми отримали важливий висновок:

поле $\mathbb{C}$ комплексних чисел є алгебраїчно замкнутим.

9.2 Розклад полінома над полем $\mathbb{R}$ у добуток незвідних множників

За аналогією до попереднього, будь-який поліном степеня n з дійсними коефіцієнтами має точно n комплексних коренів. Але для рівнянь з дійсними коефіцієнтами *цікавими* є саме *дійсні* корені.

Наслідок 9.8. *Якщо комплексне число α є коренем полінома з дійсними коефіцієнтами кратності k, то спряжене комплексне число $\bar{\alpha}$ теж є коренем цього полінома кратності k.*

Доведення. Так як α є коренем полінома $f(x)$ кратності k, то $f(\alpha) = f'(\alpha) = ... = f^{(k-1)}(\alpha) = 0$, $f^{(k)}(\alpha) \neq 0$. Але всі похідні мають теж дійсні коефіцієнти. Тому, використовуючи рівність $f(\overline{\alpha}) = \overline{\overline{f}(\alpha)} = \overline{f(\alpha)}$ до кожного полінома – похідної $f^{(j)}(x)$, зробимо висновок, що $f^{(j)}(\overline{\alpha}) = 0$ $(j = 0, 1, 2, \ldots, k-1)$. З іншого боку, $f^{(k)}(\overline{\alpha}) \neq 0$, бо в противному разі спряжене число $\overline{\overline{\alpha}}$ теж було б коренем $f^{(k)}(x)$, що неможливо. Отже, $f(\overline{\alpha}) = f'(\overline{\alpha}) = \cdots = f^{(k-1)}(\overline{\alpha}) = 0$, $f^{(k)}(\overline{\alpha}) \neq 0$. Таким чином, $\overline{\alpha}$ – корінь k-тої кратності полінома $f(x)$. $\square$

Наслідок 9.9. *Кожний поліном з дійсними коефіцієнтами, степінь якого перевищує 2, є звідним у полі $\mathbb{R}$.*

Доведення. Нехай α – корінь полінома $f(x)$.

1. α – дійсне число. За теоремою Безу $f(x) = (x-\alpha)\cdot f_1(x)$, причому $f_1(x) \in \mathbb{R}[x]$ і є поліномом ненульового степеня, бо степінь $f(x)$ перевищує *2*. Отже, $f(x)$ звідний в полі $\mathbb{R}$.

2. α – комплексне число. Тоді $\overline{\alpha}$ – теж корінь $f(x)$, звідси $f(x)$ ділиться і на $(x-\alpha)$, і на $(x-\overline{\alpha})$, а, отже, і на їх добуток $\varphi(x)$, $\varphi(x) = (x-\alpha)\cdot(x-\overline{\alpha}) = x^2-(\alpha+\overline{\alpha})x+\alpha\overline{\alpha}$. Але $\varphi(x)$ має дійсні коефіцієнти, бо $\alpha+\overline{\alpha}$ і $\alpha\overline{\alpha}$ - дійсні числа.

Таким чином, $f(x)$ ділиться на $\varphi(x)$ з цього ж кільця $\mathbb{R}[x]$, тобто $f(x) = \varphi(x)\cdot f_1(x)$, звідси частка $f_1(x)$ теж буде поліномом над полем $\mathbb{R}$. Оскільки $\varphi(x)$ має степінь 2, а $f(x)$ – степінь, більший за 2, то $f_1(x)$ – ненульового степеня. Отже, $f(x)$ – звідний в $\mathbb{R}$. $\square$

З доведеного видно, що в канонічному розкладі $f(x)$ над полем $\mathbb{R}$ *не може бути поліномів вище другого степеня.*

Наслідок 9.10. *Довільний поліном $f(x)$ з дійсними коефіцієнтами однозначно розкладається на незвідні множники в полі $\mathbb{R}$:*

$$f(x) = a_n(x-z_1)^{k_1}\ldots(x-z_l)^{k_l}\cdot(x^2+p_{l+1}x+q_{l+1})^{k_{l+1}}\ldots(x^2+p_mx+q_m)^{k_m},$$

$$k_1+\cdots+k_l+2(k_{l+1}+\cdots+k_m) = n.$$

Сформульовані наслідки показують, що розклад полінома $f(x)$ в полі $\mathbb{C}$ або $\mathbb{R}$ на *незвідні* множники дає змогу знайти *всі* його корені.

9.3 Поліноми над полем раціональних чисел

Основна відмінність поліномів над полем $\mathbb{Q}$ від поліномів над полем $\mathbb{C}$ і над полем $\mathbb{R}$: існують поліноми з раціональними коефіцієнтами, *незвідні* у полі раціональних чисел, тоді як у кільці $\mathbb{C}[x]$ звідним є довільний поліном степеня більшого за 1, а в кільці $\mathbb{R}[x]$ звідним є кожний поліном степеня більше 2.

Теорема 9.11. *Для того, щоб поліном $f(x)$ з цілими коефіцієнтами був звідним у полі $\mathbb{Q}$ раціональних чисел, необхідно і достатньо, щоб він був звідним у кільці $\mathbb{Z}$ цілих чисел (тобто, щоб існували поліноми $f_1(x)$ і $f_2(x)$ ненульового степеня з цілими коефіцієнтами такі, що $f(x) = f_1(x) \cdot f_2(x)$).*

Доведення. Необхідність. Нехай поліном $f(x)$ з цілими коефіцієнтами звідний у полі $\mathbb{Q}$, тобто $f(x) = g_1(x) \cdot g_2(x)$, де $g_1(x)$, $g_2(x)$ – поліноми ненульового степеня з раціональними коефіцієнтами. Треба довести, що існують поліноми ненульового степеня $f_1(x)$ і $f_2(x)$ з цілими коефіцієнтами, добуток яких дорівнює $f(x)$.

Нехай після зведення коефіцієнтів до спільного знаменника і винесення цього знаменника за дужки поліном $g_1(x)$ має вигляд: $g_1(x) = \frac{\alpha_1}{\beta_1} \cdot s_1(x)$, де $s_1(x)$ – поліном з цілими коефіцієнтами, β_1 - спільний знаменник коефіцієнтів $g_1(x)$, а α_1 - найбільший спільний дільник коефіцієнтів полінома, що утворюється з $g_1(x)$ після зведення до спільного знаменника. Зрозуміло, що $s_1(x)$ є примітивним поліномом (відмінний від нуля поліном називається **примітивним**, якщо найбільший спільний дільник його коефіцієнтів дорівнює одиниці). Можна вважати, що $(\alpha_1, \beta_1) = 1$, бо інакше можна скоротити.

Аналогічно для $g_2(x)$ маємо: $g_2(x) = \frac{\alpha_2}{\beta_2} \cdot s_2(x)$, де $s_2(x)$ – примітивний поліном, а $(\alpha_2, \beta_2) = 1$. Отже, $f(x) = \frac{\alpha_1\alpha_2}{\beta_1\beta_2} s_1(x) \cdot s_2(x)$. Доведемо, що $\frac{\alpha_1\alpha_2}{\beta_1\beta_2}$ дорівнює цілому числу. Справді, припустимо супротивне, що $\frac{\alpha_1\alpha_2}{\beta_1\beta_2} = \frac{p}{q}$, де p і q - взаємно прості числа. Добуток $s_1(x) \cdot s_2(x) = s(x)$ теж є примітивним поліномом. Якщо c_k – якийсь коефіцієнт $s(x)$, то добуток $\frac{p}{q}c_k$ має бути цілим числом, при будь-яких k, оскільки $f(x) = \frac{p}{q} \cdot s(x)$ за умовою має цілі коефіцієнти. Із того, що p взаємно просте з q, випливає, що кожне c_k має ділитися на q. Звідси отримуємо суперечність з тим, що $s(x)$ – примітивний поліном. Отже, $\frac{\alpha_1\alpha_2}{\beta_1\beta_2} = m$ – ціле число.

Взявши $f_1(x) = m \cdot s_1(x)$, а $f_2(x) = s_2(x)$, одержимо $f(x) = f_1(x)f_2(x)$, де $f_1(x)$, $f_2(x)$ – поліноми ненульового степеня з цілими коефіцієнтами.

Достатність. Якщо $f(x)$ – звідний у кільці цілих чисел, то він тим більше звідний в полі раціональних чисел. Теорему доведено. □

Доведена теорема повністю зводить питання звідності поліномів у полі $\mathbb{Q}$ до звідності поліномів у кільці $\mathbb{Z}$ цілих чисел.

Теорема 9.12. *(Ейзенштейна) Якщо в поліномі з цілими коефіцієнтами $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n$ коефіцієнти a_n, a_{n-1},...,a_1 діляться на деяке просте число p (причому a_n не ділиться на p^2), а старший коефіцієнт a_0 не ділиться на p, то поліном $f(x)$ незвідний у полі раціональних чисел.*

Доведення. Досить показати, що $f(x)$ при цих умовах не може бути добутком двох поліномів з цілими коефіцієнтами. Припустимо супротивне, тобто що

$f(x) = (b_0x^r + b_1x^{r-1} + \cdots + b_{r-1}x + b_r)(c_0x^s + c_1x^{s-1} + \cdots + c_{s-1}x + c_s)$, $(r + s = n)$.

Нехай $r \geq s$. Тоді

$a_n = b_rc_s$,

$a_{n-1} = b_{r-1}c_s + b_rc_{s-1}$,

$a_{n-2} = b_{r-2}c_s + b_{r-1}c_{s-1} + b_r c_{s-2}$,

$\ldots$

$a_r = b_r c_0 + b_{r-1}c_1 + \cdots + b_{r-s}c_s$,

$\ldots$

$a_0 = b_0 c_0$.

За умовою a_n, тобто $b_r c_s$, має ділитися на p, але не може ділитися на p^2. Отже, на p ділиться лише одне із чисел: b_r або c_s. Нехай, наприклад, b_r ділиться на p, а c_s не ділиться. Але тоді із другої рівності дістанемо, що b_{r-1} ділиться на p (бо $a_{n-1}\vdots p$ за умовою, а c_s не ділиться). Тепер вже b_r і b_{r-1} діляться на p, тому з *3*-ї рівності видно, що й $b_{r-2}\vdots p$. Так можна показати, що всі коефіцієнти b_r, b_{r-1}, b_{r-2},...,b_1, b_0 діляться на p. Але це неможливо, бо тоді і a_0 ділилося б на p (це випливає з останньої рівності), що суперечить умові теореми. Теорему доведено. □

З теореми Ейзенштейна випливає існування поліномів довільного степеня з цілими коефіцієнтами, незвідних у полі раціональних чисел. Ця теорема дає **достатню** умову **незвідності** полінома в полі $\mathbb{Q}$.

10 Розміщення дійсних коренів полінома

10.1 Межі дійсних коренів

В окремих випадках немає потреби знаходити числові значення коренів полінома, досить лише знайти їх розміщення на площині. Оскільки це питання складне, то обмежимось розглядом питань, зв'язаних із розміщенням на дійсній осі коренів рівнянь з дійсними коефіцієнтами.

Зауваження 10.1. *Усі корені полінома $f(x)$ лежать всередині круга з центром в точці 0 і радіусом $N_0 = 1+\frac{A}{|a_0|}$, де $A = \max\{|a_1|, |a_2|, \ldots, |a_{n-1}|, |a_n|\}$.*

Зауваження 10.2. *Комплексні корені полінома з дійсними коефіцієнтами розміщенні симетрично відносно дійсної осі.*

Зауваження 10.3. *Усі дійсні корені полінома з дійсними коефіцієнтами містяться в інтервалі $(-N_0, N_0)$, де $N_0 = 1 + \frac{A}{|a_0|}$, $A = max\{|a_1|, |a_2|, \ldots, |a_{n-1}|, |a_n|\}$.*

Приклад 10.4. $7x^7 - x^5 + x^4 - 3x^2 + 5 = 0$. $A = 5$, $a_0 = 7$, *тому* $N_0 = 1 + \frac{5}{7} = 1\frac{5}{7}$. *Отже, дійсні корені рівняння лежать в інтервалі* $(-1\frac{5}{7}, 1\frac{5}{7})$.

Одним із точніших способів встановлення межі дійсних коренів полінома є спосіб **Ньютона**.

Теорема 10.5. *Число M є верхньою межею додатних коренів полінома $f(x)$, якщо при $x = M$ поліном $f(x)$ має додатне значення, а всі його похідні – невід'ємні значення.*

Доведення. Для функції дійсної змінної $f(x)$ справедлива формула *Тейлора*:

$$f(x) = f(M)+\frac{f'(M)}{1!}(x-M)+\frac{f''(M)}{2!}(x-M)^2+...+\frac{f^{(n)}(M)}{n!}(x-M)^n.$$

Звідси зразу видно, що при $x \geq M \quad f(x) > 0$, тобто всі дійсні корені полінома $f(x)$ менші за M. Теорему доведено. □

Оскільки знак значень полінома і його похідних в точці M збігається із знаком відповідних коефіцієнтів розкладу (Тейлора) за степенями $x - M$, то на практиці число M зручно підбирати за допомогою схеми **Горнера** послідовного ділення $f(x)$ на $x - M$. Як тільки в процесі ділення на $x - M$ отримується рядок з невід'ємних чисел, - можна приймати вибране M за верхню межу додатних коренів, бо дальше застосування схеми Горнера ніколи не приведе до від'ємних коефіцієнтів. Якщо ж заданий поліном вже має всі невід'ємні коефіцієнти, то можна вважати $M = 0$, тобто поліном не має додатних коренів.

Один із шляхів звуження меж, між якими треба шукати дійсні корені, полягає в тому, щоб окремо знаходити нижню і верхню межі додатних коренів та нижню і верхню межі від'ємних коренів, тобто такі чотири числа m_+, M_+, m_-, M_-, що всі додатні корені полінома лежать в інтервалі (m_+, M_+), а всі від'ємні – в інтервалі (m_-, M_-).

Якшо поліном має корінь **нуль**, то досить розглянути поліном, утворений із заданого діленням на x. Фактично досить знайти спосіб знаходження лише одного з цих чотирьох чисел, наприклад M_+ – верхньої межі додатних коренів. Знаходження інших трьох меж легко звести до знаходження верхньої межі додатних коренів допоміжних поліномів.

Так, виконавши в рівнянні $f(x) = 0$ заміну змінної $x = \frac{1}{t}$, одержимо рівняння $g(t) = 0$, корені якого t_i зв'язані з відповідними коренями x_i початкового рівняння співвідношенням $t_i = \frac{1}{x_i}$. Якщо M'_+ – верхня межа додатних коренів рівняння $g(t) = 0$, тобто $0 < t_i < M'_+$, то $x_i = \frac{1}{t_i} > \frac{1}{M'_+} > 0$. Отже, число $\frac{1}{M'_+}$ можна взяти за нижню межу додатних коренів полінома $f(x)$: $m_+ = \frac{1}{M'_+}$.

Аналогічно, заміна $x = -y$ переводить рівняння $f(x) = 0$ в рівняння $\varphi(y) = 0$, корені якого y_i зв'язані з коренями x_i рівняння

$f(x) = 0$ рівністю $y_i = -x_i$. Якщо y_i – всі додатні корені рівняння $\varphi(y) = 0$, то x_i – всі від'ємні корені рівняння $f(x) = 0$. Із нерівності $m''_+ < y_i < M''_+$ видно, що $-M''_+ < x_i < -m''_+$, тобто $m_- = -M''_+$, $M_- = -m''_+$.

10.2 Кількість дійсних коренів. Теорема Штурма.

Кількість дійсних коренів полінома з дійсними коефіцієнтами у багатьох випадках можна визначити за правилом Декарта. Спочатку – два зауваження.

1) Кількістю змін знаків в упорядкованій скінченній послідовності дійсних чисел c_1, c_2,...,c_m називають кількість пар сусідніх чисел цієї послідовності, які мають протилежні знаки. Наприклад, в послідовності –3, –7, 6, 4, –2, 1 є три зміни знаків, в послідовності 3, 7, 2, 1, 4 – нуль змін знаків. Нулі до уваги не беруть. Якщо перше і останнє число послідовності мають однакові знаки, то кількість змін знаків у ній парна, і навпаки.

2) Будемо вважати, що заданий поліном не має кратних коренів (адже їх завжди можна відокремити).

Правило Декарта

Кількість додатних коренів полінома з дійсними коефіцієнтами дорівнює кількості змін знаків у послідовності його коефіцієнтів або на парне число менше.

Приклад 10.6. $f(x) = x^5 - 8x^3 + 3$. $1\ 0\ -8\ 0\ 0\ 3$. *Кількість змін знаків дорівнює 2. Отже, додатних коренів або 2, або 0.*

Зауваження 10.7. *Правило Декарта можна застосовувати і для оцінки кількості від'ємних коренів полінома з дійсними коефіцієнтами. Для цього в рівнянні* $f(x) = 0$ *треба зробити заміну змінної*

$x = -y$. *Кількість від'ємних коренів рівняння* $f(x) = 0$ *дорівнює кількості додатних коренів рівняння* $f(-y) = 0$.

Приклад 10.8. $x^5 - 8x^3 + 3 = 0$. $x = -y$. $y^5 - 8y^3 - 3 = 0$. $1\ 0\ -8\ 0\ 0\ -3$ – *1 зміна. Кількість від'ємних коренів дорівнює 1.*

Зауваження 10.9. *Якщо задане рівняння* ***повне*** *(жоден коефіцієнт* $a_i \neq 0$*), то кількість від'ємних коренів дорівнює* ***кількості збережень*** *знаків або на парне число менше.*

Якщо позначити кількість **змін** знаків s, а кількість **збережень** знаків t, то $s + t = n$, де n – степінь рівняння.

Якщо відомо, що всі корені рівняння *дійсні*, то правило Декарта дає *точну* відповідь на питання про кількість дійсних коренів: кількість *додатних* коренів дорівнює кількості *змін* знаків у ряді коефіцієнтів полінома $f(x) = 0$, кількість *від'ємних* коренів дорівнює кількості *змін* знаків у ряді коефіцієнтів полінома $f(-x) = 0$.

Однак в більшості випадків наперед невідомо, чи всі корені рівняння є дійсними, тому правило Декарта в цих випадках носить тільки *оціночний* характер.

10.3 Відокремлення коренів методом Штурма

Будемо вважати, що поліном $f(x)$ не має *кратних* коренів.

Теорема Штурма дає повну відповідь на питання: скільки дійсних коренів полінома (рівняння) з дійсними коефіцієнтами знаходиться в у довільному, наперед заданому інтервалі (a, b) дійсної осі.

Нехай задано поліном $f(x)$. Знайдемо похідну $f'(x)$ і побудуємо для $f(x)$ та $f'(x)$ алгоритм, подібний до алгоритму *Евкліда*, з тою лише відмінністю, що всі остачі $r(x)$ візьмемо з протилежними знаками, тобто $F_k(x) = -r_k(x)$. Отримаємо:

$f(x) = f'(x) \cdot s_1(x) - F_1(x)$
$f'(x) = F_1(x) \cdot s_2(x) - F_2(x)$
$F_1(x) = F_2(x) \cdot s_3(x) - F_3(x)$
$\ldots$
$F_{m-2}(x) = F_{m-1}(x) \cdot s_m(x) - F_m$
$F_{m-1}(x) = F_m \cdot s_{m+1}(x), \ \ F_m = const.$

Послідовність поліномів $f(x)$, $f'(x)$, $F_1(x)$, $F_2(x), \ldots, F_{m-1}(x)$, F_m називається **рядом Штурма** для полінома $f(x)$. Деколи для зручності позначають $f(x) = F_{-1}(x)$, $f'(x) = F_0(x)$. У методі Штурма важливими є не самі функції $F_k(x)$, а їх *знаки*, тому ці функції можна знаходити з точністю до *сталого* додатного множника.

Приклад 10.10. *Записати ряд Штурма для полінома* $f(x) = x^3 - 6x + 1$.

$f'(x) = 3x^2 - 6 = 3(x^2 - 2) \Rightarrow F_0(x) = x^2 - 2.$

$$\begin{array}{l|l} x^3 - 6x + 1 & x^2 - 2 \\ \cline{2-2} x^3 - 2x & x \\ \hline \quad -4x + 1 \Rightarrow F_1(x) = 4x - 1 & \end{array}$$

$$\begin{array}{l|l} x^2 - 2 & 4x - 1 \\ \cline{2-2} 4x^2 - 8 & x + 1 \\ 4x^2 - x & \\ \hline \quad x - 8 & \\ \quad 4x - 32 & \\ \quad 4x - 1 & \\ \hline \quad -31 \Rightarrow F_2(x) = 1 & \end{array}$$

Отже: $F_{-1}(x) = x^3 - 6x + 1$, $F_0(x) = x^2 - 2$, $F_1(x) = 4x - 1$, $F_2 = 1$.

Якщо в ряді функцій Штурма взяти $x = a$, де a – якесь дійсне число, то послідовність функцій перетвориться в послідовність чисел

$f(a),\ f'(a),\ F_1(a), \dots, F_{m-1}(a),\ F_m.$

Кількість змін знаків у цій послідовності позначимо через $s(a)$ і назвемо її **кількістю змін знаків** у ряді **Штурма** в точці a.

Основні властивості ряду функцій Штурма

1. Ніякі дві **сусідні** функції ряду Штурма **не мають спільних** коренів.

Доведення. Нехай $F_k(x)$ і $F_{k+1}(x)$ мають спільний корінь α. $F_k(\alpha) = F_{k+1}(\alpha) = 0$. Тоді $F_{k-1}(\alpha) = F_k(\alpha) \cdot s_{k+1}(\alpha) - F_{k+1}(\alpha) = 0$. Аналогічно $F_{k-2}(\alpha) = \cdots = F_1(\alpha) = f'(\alpha) = f(\alpha) = 0$. Але $f'(\alpha) = f(\alpha) = 0$ означає, що α - кратний корінь $f(x)$, а $f(x)$ кратних коренів не має. Ця суперечність заперечує припущення і доводить властивість 1. □

2. Якщо α є **коренем** однієї з проміжних функцій ряду Штурма, то значення **сусідніх** з нею функцій ряду Штурма мають у цій точці **протилежні знаки**.

Доведення. Нехай $F_k(\alpha) = 0$. За властивістю 1 $F_{k-1}(\alpha) \neq 0$, $F_{k+1}(\alpha) \neq 0$.

$F_{k-1}(\alpha) = F_k(\alpha) \cdot s_{k+1}(\alpha) - F_{k+1}(\alpha) = -F_{k+1}(\alpha)$. Властивість 2 доведена. □

3. Якщо x, при зростанні, проходить через корінь якоїсь **проміжної** функції ряду Штурма, але **не проходить** через корінь $f(x)$, то кількість змін знаків у ряді Штурма при цьому **не змінюється**.

Доведення. Нехай α - корінь деякої функції $F_k(x)$, де $k \neq -1,\ k \neq m$. В точці α значення $F_{k-1}(\alpha)$ і $F_{k+1}(\alpha)$ не дорівнюють нулю і мають протилежні знаки. Оскільки функції $F_{k-1}(x)$ і $F_{k+1}(x)$ – неперервні, то існує окіл точки α, в якому $F_{k-1}(x)$ і $F_{k+1}(x)$ зберігають свої знаки.

Знайдемо кількість змін знаків в ряді функцій $F_{k-1}(x)$, $F_k(x)$, $F_{k+1}(x)$, якщо x зростає від $\alpha - \delta$ до $\alpha + \delta$. Можливі варіанти розподілу знаків:

x	Знак $F_{k-1}(x)$		Знак $F_k(x)$		Знак $F_{k+1}(x)$		$s(x)$	
	I	II	I	II	I	II	I	II
$\alpha - \delta < x < \alpha$	-	+			+	-	*1*	*1*
$x = \alpha$	-	+	*0*	*0*	+	-	*1*	*1*
$\alpha < x < \alpha + \delta$	-	+			+	-	*1*	*1*

Місця для знаків $F_k(x)$ в околі точки α не заповнені, бо вони не впливають на кількість змін знаків (незалежно від цих знаків буде одна зміна знаку). Отже, і при $x < \alpha$, і при $x > \alpha$ кількість змін знаків в ряді F_{k-1}, F_k, F_{k+1} однакове. Таким чином, в цілому число змін знаків залишається сталим для всього ряду Штурма. □

4. Якщо x при зростанні **проходить** через корінь полінома $f(x)$, то кількість змін знаків у ряді Штурма **зменшується на одиницю.**

Доведення. Нехай α - корінь самого полінома $f(x)$. Тоді $f(\alpha) = 0$, але $f'(\alpha) \neq 0$, тому що (за умовою) поліном не має кратних коренів. Виберемо δ так, щоб в околі $(\alpha-\delta, \alpha+\delta)$ функція $f'(x)$ не змінювала знак. Можливі два випадки:

а) $f'(x) > 0$ в цьому околі. Тоді $f(x)$ – зростаюча функція, а тому при $\alpha - \delta < x < \alpha$ матимемо $f(x) < 0$, а при $\alpha < x < \alpha + \delta$ – $f(x) > 0$.

б) $f'(x) < 0$ в цьому околі. Тоді $f(x)$ – спадна функція і тому при $\alpha - \delta < x < \alpha$ матимемо $f(x) > 0$, а при $\alpha < x < \alpha + \delta$ –

$f(x) < 0$.

x	Знак $f(x)$		Знак $f'(x)$		*s(x)*	
	а	б	а	б	а	б
$\alpha - \delta < x < \alpha$	-	+	+	-	*1*	*1*
$x = \alpha$	*0*	*0*	+	-	*0*	*0*
$\alpha < x < \alpha + \delta$	+	-	+	-	*0*	*0*

В обох випадках кількість змін знаків в цій частині f, f', ряду Штурма зменшується на одиницю.

Кількість змін знаків інших функцій ряду Штурма (на основі властивості 3) не змінюється, навіть якщо x проходить через корені деяких з них. □

Теорема 10.11. *(Штурма) Якщо* a *і* b $(a < b)$ *– довільні дійсні числа, які не є коренями полінома* $f(x)$*, то кількість* p *дійсних коренів полінома* $f(x)$ *в інтервалі* (a, b) *дорівнює* $p = s(a) - s(b)$*, де* $s(a)$ *і* $s(b)$ *– кількість змін знаків у ряді Штурма відповідно в точках* a *і* b*.*

Доведення. 1. Якщо x при зростанні не пройде через жодний корінь $f(x)$, то за властивістю 3 $s(a) = s(b)$.

2. Якщо x при зростання пройде через p коренів $f(x)$, а при проходженні через кожний з них кількість змін знаків зменшуватиметься на одиницю, то $s(a) - s(b) = p$. Теорема доведена. □

Зауваження 10.12. *1. Умова, що* a *і* b *не є коренями* $f(x)$ *не складає труднощів при застосуванні теореми Штурма, адже якщо* a *чи* b *є коренями* $f(x)$*, то питання про розміщення цього кореня вже розв'язане, а щоб знайти положення інших коренів треба розглянути поліном, одержаний від ділення* $f(x)$ *на* $x - a$ *(чи* $x - b$*).*

2. Якщо якась із проміжних функцій Штурма $F_k(x)$ не має дійсних коренів, то наступних функцій Штурма можна не знаходити і користуватись "укороченим" рядом: $f(x)$, $f'(x)$, $F_1(x), \ldots, F_k(x)$, адже кількість змін знаків у "залишковому" ряді $F_{k+1}(x), \ldots, F_m$ є сталим, що не вплине на різницю $s(a) - s(b)$.

3. Метод Штурма можна застосовувати і без попереднього відокремлення кратних коренів. Якщо $f(x)$ має кратні корені, то остання функція ряду Штурма $F_m(x)$ вже не є сталою. Але тоді $F_m(x)$ є спільним дільником всіх інших функцій ряду Штурма. Тому можна розглядати інший ряд поліномів: $\frac{f(x)}{F_m(x)}$, $\frac{f'(x)}{F_m(x)}$, $\frac{F_1(x)}{F_m(x)}$, ..., $\frac{F_{m-1}(x)}{F_m(x)}$, 1, який володіє всіма властивостями 1-4.

Застосування теореми Штурма

1. За допомогою ряду Штурма для довільного полінома $f(x)$ над полем дійсних чисел можна *точно* визначити *загальне* кількість дійсних коренів, а також кількість його *додатних* і *від'ємних* коренів. Для цього досить застосувати теорему Штурма до інтервалів $(-N_0, 0)$ і $(0, N_0)$. На практиці користуються інтервалами $(-\infty, 0)$, $(0, +\infty)$.

Приклад 10.13. $f(x) = x^3 - 6x + 1$, $F_0 = x^2 - 2$, $F_1 = 4x - 1$, $F_2 = 1$.

x	$f(x)$	$F_0(x)$	$F_1(x)$	F_2	$s(x)$
$-\infty$	-	+	-	+	*3*
0	+	-	-	+	*2*
$+\infty$	+	+	+	+	*0*

Отже, $f(x)$ має три дійсні корені, з них два додатних і один від'ємний.

2. За допомогою теореми Штурма можна здійснювати *відокремлення* дійсних коренів, тобто знаходити інтервали, в яких знаходиться точно один дійсний корінь (використовується в методах набли-

женого обчислення). Відокремлення коренів зводиться до підбору кінців потрібних інтервалів.

Приклад 10.14. $f(x) = x^3 - 6x + 1$. *Оскільки дійсні корені лежать у проміжку* $(-N_0, N_0)$, *то* $N_0 = 1 + \frac{A}{|a_0|} = 1 + \frac{6}{1} = 7$.

x	$f(x)$	$F_0(x)$	$F_1(x)$	F_2	$s(x)$
-7	-	+	-	+	3
-3	-	+	-	+	3
-2	+	+	-	+	2
0	+	-	-	+	2
1	-	-	+	+	1
2	-	+	+	+	1
3	+	+	+	+	0
7	+	+	+	+	0

З таблиці видно, що один корінь лежить в інтервалі $(-3, -2)$, другий – $(0, 1)$, третій – $(2, 3)$.

3. За допомогою теореми Штурма можна знайти просту **ознаку** того, що всі n коренів полінома $f(x)$ n-го степеня є **дійсні різні** числа.

Для цього треба, щоб у ряді Штурма, при зростанні x від $-\infty$ до $+\infty$ кількість змін знаків зменшилось на n. Всі корені будуть дійсними, якщо $s(-\infty) = n$, $s(+\infty) = 0$. Ясно, що це має місце тільки тоді, коли старші коефіцієнти всіх функцій Штурма мають одинаковий знак. Для того, щоб усі корені полінома $f(x)$ степеня n були **дійсні** і **різні**, необхідно і достатньо, щоб відповідний ряд Штурма складався з $n + 1$ поліномів, **старші** коефіцієнти яких усі **того самого знаку**.

Вправи 10.15. *(1) Знайти межі дійсних коренів поліномів, викори-*

стовуючи метод Ньютона:

(а) $f(x) = x^3 - 4x + 2$*;*

(б) $f(x) = 2x^4 + x^3 - 3x^2 - x + 2$*;*

(в) $f(x) = x^5 - x^3 + 2x + 1$.

(2) Відокремити дійсні корені поліномів на інтервалі довжиною 1:

(а) $f(x) = x^3 - 4x + 2$*;*

(б) $f(x) = 2x^4 + x^3 - 3x^2 - x + 2$*;*

(в) $f(x) = x^5 - x^3 + 2x + 1$.

11 Поліноми розбиттів

Розбиття натуральних чисел на доданки зустрічаються у багатьох розділах математики, тому не дивно, що і поліноми розбиттів також пронизують всю математику. Під поліномом розбиттів Белл розумів однорідний поліном степеня n від декількох змінних, означений при допомозі суми за різними невпорядкованими розбиттями натурального числа n на натуральні доданки. Значно раніше Варінг розглядав поліноми розбиттів, в яких пов'язані орбіти симетричних поліномів із степеневими сумами. Наслідком цієї формули є відома формула Варінга, яка виражає елементарні симетричні поліноми через степеневі суми. Ці симетричні поліноми вже розглядалися в одному із попередніх розділів підручника. Поліноми розбиттів часто виникають також у аналізі та теорії чисел. Метою цього параграфу є ознайомлення із окремими класами поліномів розбиттів та їх застосуваннями у різних галузях математики. Зауважимо, що у цьому параграфі всі теореми наводяться без доведення.

Введемо спочатку деякі допоміжні поняття та твердження, які полегшать розуміння подальшого матеріалу.

Наведемо основні поняття та твердження із числення трикутних матриць [20], які будуть використані у цьому розділі. Нехай K — деяке числове поле.

Означення 11.1. *[17] Трикутну таблицю*

$$A = \begin{pmatrix} a_{11} & & & \\ a_{21} & a_{22} & & \\ \vdots & \vdots & \ddots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}_n \tag{1}$$

чисел із числового поля K назвемо трикутною матрицею, елемент a_{11} — верхнім елементом цієї трикутної матриці, а число n— її порядком.

Означення 11.2. *[18] Нехай A — трикутна матриця, тоді числа*

$$ddet(A) = \sum_{r=1}^{n} \sum_{p_1+\ldots+p_r=n} (-1)^{n-r} \prod_{s=1}^{r} \{a_{p_1+\ldots+p_s,p_1+\ldots+p_{s-1}+1}\},$$

$$pper(A) = \sum_{r=1}^{n} \sum_{p_1+\ldots+p_r=n} \prod_{s=1}^{r} \{a_{p_1+\ldots+p_s,p_1+\ldots+p_{s-1}+1}\},$$

називаються відповідно парадетермінантом та параперманентом трикутної матриці. Тут підсумовування проводиться за множиною натуральних розвя'зків рівняння
$p_1 + \ldots + p_r = n.$

У цих означеннях використовується поняття факторіального добутку елементів, який позначують через $\{a_{ij}\}$, причому:

$$\{a_{ij}\} = \prod_{k=j}^{i} a_{ik}.$$

Означення 11.3. *Поліномами розбиттів називають поліноми виду*

$$P(x_1, \ldots, x_n) = \sum_{\lambda_1+\ldots+n\lambda_n=n} c(n; \lambda_1, \ldots, \lambda_n) \cdot x_1^{\lambda_1} \cdot \ldots \cdot x_n^{\lambda_n},$$

де $c(n; \lambda_1, \ldots, \lambda_n)$ – деяка дробово- раціональна функція своїх коефіцієнтів.

Поліном розбиттів може бути виражений у вигляді парафункції трикутних матриць похилого вигляду. Взагалі, справедлива наступна теорема

Теорема 11.4. *Нехай*

$$A(x_1, x_2, \ldots, x_n) = \begin{pmatrix} \tau_{11}x_1 & & & & \\ \tau_{21}\frac{x_2}{x_1} & \tau_{22}x_1 & & & \\ \vdots & \ldots & \ddots & & \\ \tau_{n-1,1}\frac{x_{n-1}}{x_{n-2}} & \tau_{n-1,2}\frac{x_{n-2}}{x_{n-3}} & \ldots & \tau_{n-1,n-1}x_1 & \\ \tau_{n,1}\frac{x_n}{x_{n-1}} & \tau_{n,2}\frac{x_{n-1}}{x_{n-2}} & \ldots & \tau_{n,n-1}\frac{x_2}{x_1} & \tau_{nn}x_1 \end{pmatrix}$$

– деяка трикутна матриця, в якій τ_{ij} – деякі раціональні функції аргументів i та j, тоді справедливі рівності

$$ddet(A) = \sum_{\lambda_1+\ldots+n\lambda_n=n} c_1(n; \lambda_1, \ldots, \lambda_n) \cdot x_1^{\lambda_1} \cdot \ldots \cdot x_n^{\lambda_n},$$

$$pper(A) = \sum_{\lambda_1+\ldots+n\lambda_n=n} c_2(n; \lambda_1, \ldots, \lambda_n) \cdot x_1^{\lambda_1} \cdot \ldots \cdot x_n^{\lambda_n}.$$

Досить поширеними виявляються поліноми розбиттів, що наводяться у наступних теоремах.

Теорема 11.5. *Нехай*

$$Z_m(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 & & & & & & \\ \frac{x_2}{x_1} & x_1 & & & & & \\ \ldots & \ldots & \ddots & & & & \\ \frac{x_n}{x_{n-1}} & \frac{x_{n-1}}{x_{n-2}} & \ldots & x_1 & & & \\ 0 & \frac{x_n}{x_{n-1}} & \ldots & \frac{x_2}{x_1} & x_1 & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ddots & \\ 0 & \ldots & 0 & \frac{x_n}{x_{n-1}} & \ldots & \frac{x_2}{x_1} & x_1 \end{pmatrix}_m,$$

$n \leqslant m$, тоді справедливі тотожності:

$$\operatorname{pper}(Z_m(x_1, \ldots, x_n)) =$$
$$= \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=m} \frac{(\lambda_1+\lambda_2+\ldots+\lambda_n)!}{\lambda_1!\lambda_2!\cdot\ldots\cdot\lambda_n!} \cdot x_1^{\lambda_1} x_2^{\lambda_2} \cdot \ldots \cdot x_n^{\lambda_n},$$

$$\operatorname{ddet}(Z_m(x_1, \ldots, x_n)) =$$
$$= \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=m} (-1)^{m-(\lambda_1+\lambda_2+\ldots+\lambda_n)} \frac{(\lambda_1+\lambda_2+\ldots+\lambda_n)!}{\lambda_1!\lambda_2!\cdot\ldots\cdot\lambda_n!} \times$$
$$\times x_1^{\lambda_1} x_2^{\lambda_2} \cdot \ldots \cdot x_n^{\lambda_n},$$

де λ_i, $i = 1, 2, \ldots, n$ — цілі невід'ємні числа.

11.1 Деякі загальні твердження про поліноми розбиттів

У цьому параграфі ми розглянемо деякі загальні класи поліномів розбиттів та їх зображення парафункціями трикутних матриць.

Теорема 2.5. *Нехай поліноми*

$$x_n(y_1, y_2, \ldots, y_n), n = 0, 1, \ldots$$

задані рекурентним співвідношенням

$$x_n = a_n y_1 x_{n-1} - a_n y_2 x_{n-2} + \ldots + (-1)^{n-2} a_n y_{n-1} x_1 + (-1)^{n-1} a_n y_n x_0,$$

де $x_0 = 1$, *тоді справедливі рівності*

$$x_n = \operatorname{ddet}\begin{pmatrix} a_1 y_1 & & & \\ \frac{y_2}{y_1} & a_2 y_1 & & \\ \vdots & \ldots & \ddots & \\ \frac{y_n}{y_{n-1}} & \frac{y_{n-1}}{y_{n-2}} & \ldots & a_n y_1 \end{pmatrix},$$

$$x_n = \sum_{r=1}^{n} (-1)^{n-r} \sum_{\alpha_1+\alpha_2+\ldots+\alpha_r=n} a_{\alpha_1} a_{\alpha_1+\alpha_2} \cdot \ldots \cdot a_{\alpha_1+\alpha_2+\ldots+\alpha_r} y_{\alpha_1} y_{\alpha_2} \cdot \ldots \cdot y_{\alpha_r},$$

де $\alpha_i > 0, i = 1, 2, \ldots, r.$

Теорема 11.6. *Нехай поліноми*

$$x_n(y_1, y_2, \ldots, y_n), n = 0, 1, \ldots$$

задані рекурентним співвідношенням

$$x_n = a_n y_1 x_{n-1} + a_n y_2 x_{n-2} + \ldots + a_n y_{n-1} x_1 + a_n y_n x_0,$$

де $x_0 = 1$, *тоді справедливі рівності*

$$x_n = \operatorname{pper}\begin{pmatrix} a_1 y_1 & & & \\ \frac{y_2}{y_1} & a_2 y_1 & & \\ \vdots & \ldots & \ddots & \\ \frac{y_n}{y_{n-1}} & \frac{y_{n-1}}{y_{n-2}} & \ldots & a_n y_1 \end{pmatrix},$$

$$x_n = \sum_{r=1}^{n} \sum_{\alpha_1+\alpha_2+\ldots+\alpha_r=n} a_{\alpha_1} a_{\alpha_1+\alpha_2} \cdot \ldots \cdot a_{\alpha_1+\alpha_2+\ldots+\alpha_r} y_{\alpha_1} y_{\alpha_2} \cdot \ldots \cdot y_{\alpha_r},$$

де $\alpha_i > 0, i = 1, 2, \ldots, r.$

Досить часто у різних розділах математики зустрічаються поліноми розбиттів, що зображуються парафункціями трикутних матриць із першим довільним стовпцем.

Теорема 11.7. *Нехай поліноми*

$$y_n(x_1, x_2, \ldots, x_n), n = 0, 1, \ldots$$

задаються рекурентним співвідношенням

$$y_n = x_1 y_{n-1} - x_2 y_{n-2} + \ldots + (-1)^{n-2} x_{n-1} y_1 + (-1)^{n-1} a_n x_n y_0,$$

де $y_0 = 1$, *тоді справедливі рівності*

$$y_n = \operatorname{ddet} \begin{pmatrix} a_1 x_1 & & & \\ a_2 \frac{x_2}{x_1} & x_1 & & \\ \vdots & \ldots & \ddots & \\ a_n \frac{x_n}{x_{n-1}} & \ldots & \frac{x_2}{x_1} & x_1 \end{pmatrix},$$

$$y_n = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{n-k} \left(\sum_{i=1}^{n} \lambda_i a_i \right) \frac{(k-1)!}{\lambda_1! \lambda_2! \cdot \ldots \cdot \lambda_n!} \times$$

$$\times x_1^{\lambda_1} x_2^{\lambda_2} \cdot \ldots \cdot x_n^{\lambda_n},$$

де $k = \lambda_1 + \lambda_2 + \ldots + \lambda_n.$

Теорема 11.8. *Нехай поліноми*

$$y_n(x_1, x_2, \ldots, x_n), n = 0, 1, \ldots$$

задані рекурентним співвідношенням

$$y_n = x_1 y_{n-1} + x_2 y_{n-2} + \ldots + x_{n-1} y_1 + a_n x_n y_0,$$

де $y_0 = 1$, *тоді справедливі рівності*

$$y_n = \operatorname{pper} \begin{pmatrix} a_1 x_1 & & & \\ a_2 \frac{x_2}{x_1} & x_1 & & \\ \vdots & \ldots & \ddots & \\ a_n \frac{x_n}{x_{n-1}} & \ldots & \frac{x_2}{x_1} & x_1 \end{pmatrix},$$

$$y_n = \sum_{\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n = n} \left(\sum_{i=1}^{n} \lambda_i a_i \right) \frac{(k-1)!}{\lambda_1! \lambda_2! \cdot \ldots \cdot \lambda_n!} x_1^{\lambda_1} x_2^{\lambda_2} \cdot \ldots \cdot x_n^{\lambda_n},$$

де $k = \lambda_1 + \lambda_2 + \ldots + \lambda_n$.

Якщо у парафункціях трикутних матриць два перші стовпці загальні, то справедлива теорема

Теорема 11.9. *Якщо поліноми задані рекурентним рівнянням*

$$y_n = x_1 y_{n-1} - x_2 y_{n-2} + x_3 y_{n-3} - \ldots + (-1)^{n-3} x_{n-2} y_2 +$$

$$+ (-1)^{n-2} \tau_{n2} x_{n-1} y_1 + (-1)^{n-1} \tau_{n1} \tau_{n2} x_n y_0,$$

де $y_0 = 1$, *тоді справедливі рівності*

$$y_n = \left\langle \begin{array}{cccccc} \tau_{11} x_1 & & & & & \\ \tau_{21} \frac{x_2}{x_1} & \tau_{22} x_1 & & & & \\ \tau_{31} \frac{x_3}{x_2} & \tau_{32} \frac{x_2}{x_1} & x_1 & & & \\ \vdots & \ldots & \ldots & \ddots & & \\ \tau_{n-1,1} \frac{x_{n-1}}{x_{n-2}} & \tau_{n-1,2} \frac{x_{n-2}}{x_{n-3}} & \frac{x_{n-3}}{x_{n-4}} & \cdots & x_1 & \\ \tau_{n1} \frac{x_n}{x_{n-1}} & \tau_{n2} \frac{x_{n-1}}{x_{n-2}} & \frac{x_{n-2}}{x_{n-3}} & \cdots & \frac{x_2}{x_1} & x_1 \end{array} \right\rangle_n$$

$$y_n = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{n-k} \frac{A(\lambda,\tau)}{\lambda_1!\cdot\ldots\cdot\lambda_n!} x_1^{\lambda_1}\cdot\ldots\cdot x_n^{\lambda_n},$$

де

$$A(\lambda,\tau) = \left(\lambda_1(\lambda_1-1)\tau_{11}\tau_{22} + \sum_{i=2}^{n-1}\lambda_1\lambda_i\tau_{11}\tau_{i+1,2}\right)\cdot(k-2)!+$$

$$+\sum_{i=1}^{n-1}\lambda_{i+1}\tau_{i+1,1}\tau_{i+1,2}\cdot(k-1)!$$

Наведена теорема узагальнює попередню теорему.

Можна провести і подальші узагальнення. Справедлива наступна

Теорема 11.10. *Рівності*

$$y_n = \left\langle \begin{array}{ccccc} \tau_{11}x_1 & & & & \\ \tau_{21}\frac{x_2}{x_1} & & & & \\ \vdots & \ddots & & & \\ \tau_{n-1,1}\frac{x_{n-1}}{x_{n-2}} & \cdots & \tau_{n-1,n-1}x_1 & & \\ \tau_{n1}\frac{x_n}{x_{n-1}} & \cdots & \tau_{n,n-1}\frac{x_2}{x_1} & \tau_{nn}x_1 \end{array} \right\rangle_n$$

$$y_n = x_1y_{n-1} - x_2y_{n-2} + x_3y_{n-3} - \ldots +$$
$$(-1)^{n-m-1}x_{n-m}y_m + (-1)^{n-m}\{\tau_{nm}\}_m x_{n-m+1}\times$$
$$\times y_{m-1} + (-1)^{n-m+1}\{\tau_{n,m-1}\}_m x_{n-m+2}y_{m-2}+$$
$$+\ldots + (-1)^{n-1}\{\tau_{n1}\}_m x_n y_0$$

$$y_n = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{n-k}\sum_{i=m}^{n} A(\lambda,\tau,i)\times$$

$$\times\frac{x_1^{\lambda_1}\cdot\ldots\cdot x_n^{\lambda_n}}{\lambda_1!\cdot\ldots\cdot\lambda_n!},$$

де $\tau_{ij}=1$ *при* $m+1\le j\le n$,

$$A(\lambda,\tau,i)=$$

$$\sum_{r=1}^{m}(k-r)!\sum_{\substack{\alpha_1+\ldots+\alpha_r=m,\\ \alpha_j\in\{1^{\lambda_1},2^{\lambda_2},\ldots,n^{\lambda_n}\},j=1,\ldots,r}}\lambda_{\alpha_1}\lambda_{\alpha_2}\cdot\ldots\cdot\lambda_{\alpha_{r-1}}\lambda_{i-m+\alpha_r}\times$$

$$\times\{\tau_{i,m-\alpha_r+1}\}_m\prod_{s=1}^{r-1}\{\tau_{\alpha_1+\ldots+\alpha_s,\alpha_1+\ldots+\alpha_{s-1}+1}\}_m,$$

причому

$$\underbrace{\lambda_{\alpha_j}\lambda_{\alpha_j}\cdot\ldots\cdot\lambda_{\alpha_j}}_{k}=\lambda_{\alpha_j}^{\underline{k}}=$$

$$=\lambda_{\alpha_j}(\lambda_{\alpha_j}-1)\cdot\ldots\cdot(\lambda_{\alpha_j}-k+1),\ j=1,\ldots,r,$$

рівносильні між собою.

Важливим виявляється також наслідок цієї теореми.

Наслідок 2.7. *Наступні рівності рівносильні між собою:*

$$y_n=\left\langle\begin{array}{cccc}\tau_{11}x_1 & & & \\ \tau_{21}\frac{x_2}{x_1} & & & \\ \vdots & \ddots & & \\ \tau_{n-1,1}\frac{x_{n-1}}{x_{n-2}} & \cdots & \tau_{n-1,n-1}x_1 & \\ \tau_{n1}\frac{x_n}{x_{n-1}} & \cdots & \tau_{n,n-1}\frac{x_2}{x_1} & \tau_{nn}x_1\end{array}\right\rangle_n$$

$$y_n=\{\tau_{nn}\}x_1y_{n-1}-\{\tau_{n,n-1}\}x_2y_{n-2}+$$

$$+\{\tau_{n,n-2}\}x_3y_{n-3}-\ldots+(-1)^{n-2}\{\tau_{n2}\}x_{n-1}y_1+$$

$$+(-1)^{n-1}\{\tau_{n1}\}x_n y_0$$

$$y_n = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{n-k} A(\lambda,\tau,n)\frac{x_1^{\lambda_1}\cdot\ldots\cdot x_n^{\lambda_n}}{\lambda_1!\cdot\ldots\cdot\lambda_n!},$$

де

$$A(\lambda,\tau,n) = \begin{pmatrix} (k-1)! \\ (k-2)! \\ \vdots \\ (k-n)! \end{pmatrix} \times$$

$$\times \begin{bmatrix} \lambda_1\tau_{11} & & & \\ \frac{\lambda_2}{\lambda_1}\tau_{21} & \lambda_1\tau_{22} & & \\ \vdots & \ldots & \ddots & \\ \frac{\lambda_n}{\lambda_{n-1}}\tau_{n1} & \frac{\lambda_{n-1}}{\lambda_{n-2}}\tau_{n2} & \ldots & \lambda_1\tau_{nn} \end{bmatrix},$$

де добуток

$$\underbrace{\lambda_i\cdot\ldots\cdot\lambda_i}_{k}$$

розглядається як спадний факторіальний степінь $\lambda_{\overline{i}}^{\underline{k}}$.

11.2 Поліноми розбиттів у теорії чисел

Нехай $p(n)$ – число невпорядкованих розбиттів натурального числа n в суму натуральних доданків, а $\sigma(n)$ – сума всіх натуральних дільників даного числа n. У монографії Холла (див. [19], стор. 58) наводиться тотожність

$$\frac{d}{dx}\left(\sum_{i=0}^{\infty} p(i)x^i\right) = \left(\sum_{i=0}^{\infty} p(i)x^i\right)\cdot\left(\sum_{i=1}^{\infty} \sigma(i)x^{i-1}\right).$$

Із цієї тотожності можна вивести [20] такі взаємно обернені поліноми розбиттів

$$\sigma(n)=\sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n}(-1)^{(\lambda_1+\ldots+\lambda_n)-1}\frac{(\lambda_1+\ldots+\lambda_n-1)!n}{\lambda_1!\cdot\ldots\cdot\lambda_n!}p(1)^{\lambda_1}\cdot\ldots\cdot p(n)^{\lambda_n}$$

$$p(n)=\sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n}\frac{1}{\lambda_1!(1!)^{\lambda_1}\cdot\ldots\cdot\lambda_n!(n!)^{\lambda_n}}(\sigma(1))^{\lambda_1}\cdot\ldots\cdot(\sigma(n))^{\lambda_n}$$

та їх зображення у вигляді парафункцій трикутних матриць:

$$p(n)=\begin{bmatrix}\sigma(1) & & & & \\ \frac{\sigma(2)}{\sigma(1)} & \frac{1}{2}\cdot\sigma(1) & & & \\ \vdots & \ldots & \ddots & & \\ \frac{\sigma(n-1)}{\sigma(n-2)} & \frac{\sigma(n-2)}{\sigma(n-3)} & \ldots & \frac{1}{n-1}\cdot\sigma(1) & \\ \frac{\sigma(n)}{\sigma(n-1)} & \frac{\sigma(n-1)}{\sigma(n-2)} & \ldots & \frac{\sigma(2)}{\sigma(1)} & \frac{1}{n}\cdot\sigma(1)\end{bmatrix}_n$$

$$\sigma(n)=(-1)^{n-1}\left\langle\begin{matrix}p(1) & & & & \\ 2\cdot\frac{p(2)}{p(1)} & p(1) & & & \\ \vdots & \ldots & \ddots & & \\ (n-1)\frac{p(n-1)}{p(n-2)} & \frac{p(n-2)}{p(n-3)} & \ldots & p(1) & \\ n\frac{p(n)}{p(n-1)} & \frac{p(n-1)}{p(n-2)} & \ldots & \frac{p(2)}{p(1)} & p(1)\end{matrix}\right\rangle_n$$

Проте можна встановити і загальніші результати Нехай $b_m(n)$ – число m-арних розбиттів натурального числа n, на степені числа m.

Генератрисою функції натурального аргументу $b_m(n)$ слугує функція

$$f_m(x)=\sum_{n=0}^{\infty}b_m(n)x^n=\prod_{n=0}^{\infty}(1-x^{m^n})^{-1}.$$

При $m=2$ отримаємо бінарні розбиття натурального числа n на степені двійки. Наприклад, існує чотири бінарні розбиття натурального числа 5 :

$$\begin{aligned} 5 = &\ 2^0 + 2^0 + 2^0 + 2^0 + 2^0 + 2^0, \\ 5 = &\ 2^1 + 2^0 + 2^0 + 2^0 + 2^0, \\ 5 = &\ 2^1 + 2^1 + 2^0, \\ 5 = &\ 2^2 + 2^0. \end{aligned}$$

У 1750 році Ойлер встановив рекурентні співвідношення для обчислення числа бінарних розбиттів натурального числа n :

$$b_2(2n+1) = b_2(2n),$$

$$b_2(2n) = b_2(2n-1) + b_2(n), b_2(0) = 1.$$

Нехай $\xi_m(n)$ – сума всіх дільників натурального числа n, що є степенями числа m. Наприклад,

$$\xi_2(1) = 2^0 = 1,$$

$$\xi_2(2) = 2^0 + 2^1 = 3,$$

$$\xi_2(3) = 2^0 = 1,$$

$$\xi_2(4) = 2^0 + 2^1 + 2^2 = 7,$$

$$\xi_2(5) = 2^0 = 1,$$

$$\xi_2(6) = 2^0 + 2^1 = 3.$$

Прийнято вважати, що $\xi_m(0) = 1$. Очевидно, що функція натурального аргументу $\xi_m(n)$, при $m = 1$, співпадає з функцією натурального аргументу $\sigma(n)$.

Поряд із означеними вище двома функціями натурального аргументу $b_m(n)$ і $\xi_m(n)$, розглядають ще одну функцію натурального аргументу $d_m(n)$, генератрисою якої є функція

$$g_m(x) = \frac{1}{f_m(x)} = \sum_{n=0}^{\infty} d_m(n)x^n = \prod_{n=0}^{\infty}(1 - x^{m^n}).$$

Зазначимо, що функцію $d_m(n)$ можна задати ще так:

$$d_m(n)=\begin{cases}0, \text{якщо n не є сумою різних степенів числа m}\\ 1, \text{якщо n є сумою парного числа різних степенів числа m}\\ -1, \text{якщоnєсумоюнепарногочисларізнихстепенівчислаm},\end{cases}$$

причому $d_m(0) = 1$.

Наведемо кілька перших членів числової послідовності $d_m(n)$ при $m = 3$:

$$d_3(1) = -1, d_3(2) = 0, d_3(3) = -1, d_3(4) = 1, d_3(5) = 0, d_3(6) = 0,$$

$$d_3(7) = 0, d_3(8) = 0, d_3(9) = -1, d_3(10) = 1.$$

Наведені вище три функції натурального аргументу та їхні зв'язки вивчалися у статтях [21],[22]. Результатами досліджень цих робіт є наступні теореми:

Теорема 11.11. *Для довільного натурального n, m-арні розбиття $b_m(n)$ можна подати у вигляді многочлена розбиттів*

$$b_m(n) = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} \frac{1}{\lambda_1!1^{\lambda_1}\lambda_2!2^{\lambda_2}\cdot\ldots\cdot\lambda_n!n^{\lambda_n}}\xi_m(1)^{\lambda_1}\times$$

$$\times\xi_m(2)^{\lambda_2}\cdot\ldots\cdot\xi_m(n)^{\lambda_n}.$$

У наступній теоремі зв'язки між функціями $b_m(n)$ та $d_m(n)$ виражаються при допомозі матриць Хессенберга.

Теорема 11.12. *Для довільного натурального n справедливі рівності:*

$$b_m(n) = (-1)^n \det \begin{pmatrix} d_m(1) & 1 & 0 & \cdots & 0 \\ d_m(2) & d_m(1) & 1 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ d_m(n-1) & d_m(n-2) & d_m(n-3) & \cdots & 1 \\ d_m(n) & d_m(n-1) & d_m(n-2) & \cdots & d_m(1) \end{pmatrix},$$

$$d_m(n) = (-1)^n \det \begin{pmatrix} b_m(1) & 1 & 0 & \cdots & 0 \\ b_m(2) & b_m(1) & 1 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ b_m(n-1) & b_m(n-2) & b_m(n-3) & \cdots & 1 \\ b_m(n) & b_m(n-1) & b_m(n-2) & \cdots & b_m(1) \end{pmatrix}.$$

Теорема 11.13. *Для довільного натурального n справедливі рівності:*

$$b_m(n) = \frac{1}{n}\sum_{j=0}^{n-1} \xi_m(n-j) b_m(j),$$

$$d_m(n) = -\frac{1}{n}\sum_{j=0}^{n-1} \xi_m(n-j) d_m(j).$$

Теорема 11.14. *Справедливі рівності:*

$$b_m(n) = \begin{bmatrix} \xi_m(1) & & & & \\ \frac{\xi_m(2)}{\xi_m(1)} & \frac{1}{2}\xi_m(1) & & & \\ \vdots & \cdots & \ddots & & \\ \frac{\xi_m(n-1)}{\xi_m(n-2)} & \frac{\xi_m(n-2)}{\xi_m(n-3)} & \cdots & \frac{1}{n-1}\xi_m(1) & \\ \frac{\xi_m(n)}{\xi_m(n-1)} & \frac{\xi_m(n-1)}{\xi_m(n-2)} & \cdots & \frac{\xi_m(2)}{\xi_m(1)} & \frac{1}{n}\xi_m(1) \end{bmatrix},$$

$$d_m(n) = \begin{bmatrix} -\xi_m(1) & & & & \\ \frac{\xi_m(2)}{\xi_m(1)} & -\frac{1}{2}\xi_m(1) & & & \\ \vdots & \dots & \ddots & & \\ \frac{\xi_m(n-1)}{\xi_m(n-2)} & \frac{\xi_m(n-2)}{\xi_m(n-3)} & \dots & -\frac{1}{n-1}\xi_m(1) & \\ \frac{\xi_m(n)}{\xi_m(n-1)} & \frac{\xi_m(n-1)}{\xi_m(n-2)} & \dots & \frac{\xi_m(2)}{\xi_m(1)} & -\frac{1}{n}\xi_m(1) \end{bmatrix} =$$

$$= (-1)^n \left\langle \begin{matrix} \xi_m(1) & & & & \\ \frac{\xi_m(2)}{\xi_m(1)} & \frac{1}{2}\xi_m(1) & & & \\ \vdots & \dots & \ddots & & \\ \frac{\xi_m(n-1)}{\xi_m(n-2)} & \frac{\xi_m(n-2)}{\xi_m(n-3)} & \dots & \frac{1}{n-1}\xi_m(1) & \\ \frac{\xi_m(n)}{\xi_m(n-1)} & \frac{\xi_m(n-1)}{\xi_m(n-2)} & \dots & \frac{\xi_m(2)}{\xi_m(1)} & \frac{1}{n}\xi_m(1) \end{matrix} \right\rangle,$$

$$\xi_m(n) = (-1)^{n-1} \left\langle \begin{matrix} b_m(1) & & & & \\ 2 \cdot \frac{b_m(2)}{b_m(1)} & b_m(1) & & & \\ \vdots & \dots & \ddots & & \\ (n-1) \cdot \frac{b_m(n-1)}{b_m(n-2)} & \frac{b_m(n-2)}{b_m(n-3)} & \dots & b_m(1) & \\ n \cdot \frac{b_m(n)}{b_m(n-1)} & \frac{b_m(n-1)}{b_m(n-2)} & \dots & \frac{b_m(2)}{b_m(1)} & b_m(1) \end{matrix} \right\rangle,$$

$$\xi_m(n) =$$

$$= (-1)^{n-1} \left\langle \begin{matrix} -d_m(1) & & & & \\ -2 \cdot \frac{d_m(2)}{d_m(1)} & d_m(1) & & & \\ \vdots & \dots & \ddots & & \\ -(n-1) \cdot \frac{d_m(n-1)}{d_m(n-2)} & \frac{d_m(n-2)}{d_m(n-3)} & \dots & d_m(1) & \\ -n \cdot \frac{d_m(n)}{d_m(n-1)} & \frac{d_m(n-1)}{d_m(n-2)} & \dots & \frac{d_m(2)}{d_m(1)} & d_m(1) \end{matrix} \right\rangle =$$

$$= (-1)^n \left\langle \begin{matrix} d_m(1) & & & & \\ 2 \cdot \frac{d_m(2)}{d_m(1)} & d_m(1) & & & \\ \vdots & \dots & \ddots & & \\ (n-1) \cdot \frac{d_m(n-1)}{d_m(n-2)} & \frac{d_m(n-2)}{d_m(n-3)} & \dots & d_m(1) & \\ n \cdot \frac{d_m(n)}{d_m(n-1)} & \frac{d_m(n-1)}{d_m(n-2)} & \dots & \frac{d_m(2)}{d_m(1)} & d_m(1) \end{matrix} \right\rangle,$$

$$b_m(n) = (-1)^n \left\langle \begin{array}{ccccc} d_m(1) & & & & \\ \frac{d_m(2)}{d_m(1)} & d_m(1) & & & \\ \vdots & \dots & \ddots & & \\ \frac{d_m(n-1)}{d_m(n-2)} & \frac{d_m(n-2)}{d_m(n-3)} & \dots & d_m(1) & \\ \frac{d_m(n)}{d_m(n-1)} & \frac{d_m(n-1)}{d_m(n-2)} & \dots & \frac{d_m(2)}{d_m(1)} & d_m(1) \end{array} \right\rangle,$$

$$d_m(n) = (-1)^n \left\langle \begin{array}{ccccc} b_m(1) & & & & \\ \frac{b_m(2)}{b_m(1)} & b_m(1) & & & \\ \vdots & \dots & \ddots & & \\ \frac{b_m(n-1)}{b_m(n-2)} & \frac{b_m(n-2)}{b_m(n-3)} & \dots & b_m(1) & \\ \frac{b_m(n)}{b_m(n-1)} & \frac{b_m(n-1)}{b_m(n-2)} & \dots & \frac{b_m(2)}{b_m(1)} & b_m(1) \end{array} \right\rangle.$$

Наведемо ще одну теорему, в якій встановлено поліноми разбиттів, які пов'язують між собою m-арні числа
$b_m(n), \xi_m(n), d_m(n)$.

Теорема 11.15. *Справедливі рівності:*

$$d_m(n) = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^k \frac{\xi_m^{\lambda_1}(1)\cdot\ldots\cdot\xi_m^{\lambda_n}(n)}{\lambda_1!\cdot\ldots\cdot\lambda_n! 1^{\lambda_1}\cdot\ldots\cdot n^{\lambda_n}},$$

$$\xi_m(n) = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{k-1} \frac{n(k-1)!}{\lambda_1!\cdot\ldots\cdot\lambda_n!} \cdot b_m^{\lambda_1}(1)\cdot\ldots\cdot b_m^{\lambda_n}(n),$$

$$\xi_m(n) = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{k} \frac{n(k-1)!}{\lambda_1!\cdot\ldots\cdot\lambda_n!} \cdot d_m^{\lambda_1}(1)\cdot\ldots\cdot d_m^{\lambda_n}(n),$$

$$b_m(n) = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{k} \frac{k!}{\lambda_1!\cdot\ldots\cdot\lambda_n!} \cdot d_m^{\lambda_1}(1)\cdot\ldots\cdot d_m^{\lambda_n}(n),$$

$$d_m(n) = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} (-1)^{k} \frac{k!}{\lambda_1!\cdot\ldots\cdot\lambda_n!} \cdot b_m^{\lambda_1}(1)\cdot\ldots\cdot b_m^{\lambda_n}(n),$$

де $k = \lambda_1 + \lambda_2 + \ldots + \lambda_n$.

11.3 Поліноми розбиттів у алгебрі та аналізі

Важливим класом поліномів розбиттів є поліноми розбиттів вигляду

$$B(fx_1, fx_2, \ldots, fx_n) =$$

$$= \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} \frac{n!f_k}{\lambda_1!1!^{\lambda_1}\lambda_2!2!^{\lambda_2}\cdot\ldots\cdot\lambda_n!n!^{\lambda_n}} x_1^{\lambda_1}\cdot\ldots\cdot x_n^{\lambda_n},$$

де $f^k = f_k$. Їх називають поліномами Белла. Вони виникають при диференціюванні складених функцій (формула Фаа ді Бруно), при оберненні формальних степеневих рядів тощо. При $f = 1$, ці поліноми зображуються у вигляді параперманента трикутної матриці

$$\left(\begin{array}{ccccc} x_1 & & & & \\ \frac{1}{1}\cdot\frac{x_2}{x_1} & x_1 & & & \\ \frac{1}{2}\cdot\frac{x_3}{x_2} & \frac{2}{1}\cdot\frac{x_2}{x_1} & x_1 & & \\ \vdots & \cdots & \cdots & \ddots & \\ \frac{1}{n-1}\cdot\frac{x_n}{x_{n-1}} & \frac{2}{n-2}\cdot\frac{x_{n-1}}{x_{n-2}} & \cdots & \frac{n-1}{1}\cdot\frac{x_2}{x_1} & x_1 \end{array}\right) =$$

$$= \left(\frac{j}{i-j+j\cdot\delta_{ij}}\cdot\frac{x_{i-j+1}}{x_{i-j}}\right)_{1\le j\le i\le n},$$

яку називають трикутною матрицею Белла.

Поліном розбиття вигляду

$$C_n(x_1,\ldots,x_n) = \sum_{\lambda_1+2\lambda_2+\ldots+n\lambda_n=n} \frac{n!}{\lambda_1!1^{\lambda_1}\cdot\ldots\cdot\lambda_n!n^{\lambda_n}}\cdot x_1^{\lambda_1}\cdot\ldots\cdot x_n^{\lambda_n}$$

називають цикловим індикатором симетричної групи. Його можна зобразити компактно у вигляді параперманента

$$\left[(j-(j-1)\cdot\delta_{ij})\cdot\frac{x_{i-j+1}}{x_{i-j}}\right]_{1\le j\le i\le n}.$$

Наведемо коротенькі відомості про основні симетричні поліноми та їх зображення парафункціями трикутних матриць. Нехай

$$\sigma_k(x_1, x_2, \ldots, x_n),\ \ s_k(x_1, x_2, \ldots, x_n),\ \ p_k(x_1, x_2, \ldots, x_n)$$

— симетричні поліноми задані відповідними генератрисами. Встановимо три можливі пари формул обернення між цими симетричними поліномами. Генератриси цих поліномів задовольняють співвідношення

$$\sigma(z)p(-z) = 1,$$

$$p(z)s(z) = p^{'}(z),$$

$$\sigma(z)s(-z) = -\sigma^{'}(z).$$

Зрівнюючи коефіцієнти біля z^k, отримаємо три рекурентні рівняння:

$$\sum_{i=0}^{k}(-1)^i \sigma_i p_{k-i} = 0,$$

$$kp_k = \sum_{i=1}^{k} s_i p_{k-i},$$

$$k\sigma_k = \sum_{i=1}^{k}(-1)^{i-1} s_i \sigma_{k-i}.$$

Перша рекурентна рівність дає дві формули обернення. Інші дві запишемо відповідно у вигляді:

$$p_k = \frac{s_1}{k} \cdot p_{k-1} + \frac{s_2}{k} \cdot p_{k-2} + \ldots + \frac{s_{k-1}}{k} \cdot p_1 + \frac{s_k}{k},$$

$$\sigma_k = \frac{s_1}{k}\sigma_{k-1} - \frac{s_2}{k} \cdot \sigma_{k-2} + \ldots + (-1)^{k-2} s_{k-1}\sigma_1 + (-1)^{k-1} s_1.$$

Праві частини цих рівностей можуть бути виражені відповідно через параперманент та парадетермінант

$$p_k = \left[\begin{array}{lllll} s_1 & & & & \\ \frac{s_2}{s_1} & \frac{s_1}{2} & & & \\ \vdots & \dots & \ddots & & \\ \frac{s_{k-1}}{s_{k-2}} & \frac{s_{k-2}}{s_{k-3}} & \dots & \frac{s_1}{k-1} & \\ \frac{s_k}{s_{k-1}} & \frac{s_{k-1}}{s_{k-2}} & \dots & \frac{s_2}{s_1} & \frac{s_1}{k} \end{array}\right]_k ,$$

$$\sigma_k = \left\langle\begin{array}{lllll} s_1 & & & & \\ \frac{s_2}{s_1} & \frac{s_1}{2} & & & \\ \vdots & \dots & \ddots & & \\ \frac{s_{k-1}}{s_{k-2}} & \frac{s_{k-2}}{s_{k-3}} & \dots & \frac{s_1}{k-1} & \\ \frac{s_k}{s_{k-1}} & \frac{s_{k-1}}{s_{k-2}} & \dots & \frac{s_2}{s_1} & \frac{s_1}{k} \end{array}\right\rangle_k .$$

Легко записати і відповідні обернені співвідношення:

$$s_k = (-1)^{k-1}\left\langle\begin{array}{ccccc} p_1 & & & & \\ 2\cdot\frac{p_2}{p_1} & p_1 & & & \\ \vdots & \dots & \ddots & & \\ (k-1)\cdot\frac{p_{k-1}}{p_{k-2}} & \frac{p_{k-2}}{p_{k-3}} & \dots & p_1 & \\ k\cdot\frac{p_k}{p_{k-1}} & \frac{p_{k-1}}{p_{k-2}} & \dots & \frac{p_2}{p_1} & p_1 \end{array}\right\rangle_k$$

$$s_k = \left\langle\begin{array}{ccccc} \sigma_1 & & & & \\ 2\cdot\frac{\sigma_2}{\sigma_1} & \sigma_1 & & & \\ \vdots & \dots & \ddots & & \\ (k-1)\cdot\frac{\sigma_{k-1}}{\sigma_{k-2}} & \frac{\sigma_{k-2}}{\sigma_{k-3}} & \dots & \sigma_1 & \\ k\cdot\frac{\sigma_k}{\sigma_{k-1}} & \frac{\sigma_{k-1}}{\sigma_{k-2}} & \dots & \frac{\sigma_2}{\sigma_1} & \sigma_1 \end{array}\right\rangle_k .$$

Від парафункцій цих матриць, при допомозі попередніх загальних теорем легко перейти до відповідних поліномів розбиттів.

Бібліографія

[1] А.И. Кострикин, *Введение в алгебру.* Часть I. *Основы алгебры*, Физматлит, 2001.

[2] А.И. Кострикин, *Введение в алгебру.* Часть III. *Основные структуры*, Физматлит, 2001.

[3] А.И. Кострикин, *Введение в алгебру.* – М., Наука, 1977. – 496с.

[4] А.Г. Курош *Курс высшей алгебры*, М.: Наука, 1968. – 325с.

[5] С.Т. Завало, *Курс алгебри.* – Київ, Вища школа, 1985, – 504с.

[6] А.Г. Курош, *Курс высшей алгебри.* – М., Наука, 1975. – 432с.

[7] Л.Я. Окунев, *Высшая алгебра.* – М., Учпедтиз, 1958. – 336с.

[8] Д.К. Фаддеев, *Лекции по алгебре.* – М., Наука, 1984. – 416с.

[9] С.Т. Завало, В.М. Костарчук, Б.І. Хацет. *Алгебра і теорія чисел.ч.1,2.* – Київ, Вища школа, 1976, – 384с.

[10] С.Т. Завало, С.С. Левіщенко, В.В. Пилаєв, І.О. Рокицький. *Алгебра і теорія чисел. Приклади ч.1.* – Київ, Вища школа, 1983, – 232с.

[11] Л.Я. Окунев, П.И. Титов. *Сборник задач по высшей алгебре.* – М., Просвещение, 1964, – 184с.

[12] Д.К. Фаддєєв, І.С. Сомінський. *Збірник задач з вищої алгебри.* – Київ, Вища школа, 1971, – 316с.

[13] С.Т. Завало, С.С. Левіщенко, В.В. Пилаєв, І.О. Рокицький. *Алгебра і теорія чисел. Приклади ч.1,2.* – Київ, Вища школа, 1986, – 264с.

[14] В.У. Грибанов, П.И. Титов. *Сборник упражнений по теории чисел.* – М., Просвещение, 1964, – 144с.

[15] Винберг Э.Б. *Алгебра многочленов.* — М.: Просвещение, 1980. – 176с.

[16] В.В. Прасолов. *Многочлены.* — МЦНМО, 2003. – 336с.

[17] Заторський Р.А. Про паравизначники та параперманенти трикутних матриць / Р.А. Заторський // Математичні студії. – 2002. – Т.17, №1. – С. 3-17.

[18] Ганюшкін О.Г. До паравизначників і параперманентів трикутних матриць / О.Г. Ганюшкін, Р.А. Заторський, І.І. Ліщинський // Вісник КНУ, Серія: фіз.-мат. науки. – 2005. – Вип. 1. – С. 35-41.

[19] Холл М. Комбинаторика / М. Холл;[Пер. с англ.] – М.: Мир, 1970. – 237 с.

[20] Заторський Р.А. Числення трикутних матриць та його застосування / Р.А. Заторський. – Івано-Франківськ: Сімик, 2010. – 508 с.

[21] Kachi Y. On the m-ary partition numbers / Y. Kachi, P. Tzermias // Algebra and Discrete Mathematics. – 2015. – Vol. 19, №1. – P. 67-76.

[22] Zatorsky R. Parafunctions of triangular matrices and m-ary partitions of number / R.A. Zatorsky, S.D. Stefluk. // ADM. – 2016. – V.21, №1. – P. 144-152.

Навчальне видання

ПИЛИПІВ Володимир Михайлович
ЗАТОРСЬКИЙ Роман Андрійович
ЛІЩИНСЬКИЙ Іван Іванович

КІЛЬЦЕ ПОЛІНОМІВ

Навчальний посібник

Головний редактор Василь ГОЛОВЧАК

Підп. до друку 14.02.2023. Формат 60 x 84 /16.
Папір офсет. Гарнітура “Times New Roman”.
Ум. друк. арк. 6,4. Зам. №3. Наклад 100 прим.

Віддруковано в друкарні КП фірми “ЛІК”.
м. Івано-Франківськ, вул. Василіянок, 48. Тел. (0342) 54-80-27.

Свідоцтво про внесення суб’єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції ІФ №16 від 06.09.2001 р.