**Дрогобицький державний педагогічний університет
імені Івана Франка**

**Леся Комарницька,
Юрій Матурін**

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

Тексти лекцій

Частина 2

**Дрогобич
2023**

УДК 511+512(075.8)
К 63

Рекомендовано до друку вченою радою Дрогобицького державного педагогічного університету імені Івана Франка (протокол № 11 від 21 вересня 2023 р.)

Рецензенти:

Дільний В.М., доктор фізико-математичних наук, професор кафедри вищої математики Національного університету «Львівська Політехніка»;

Хаць Р.В., кандидат фізико-математичних наук, доцент кафедри математики та економіки Дрогобицького державного педагогічного університету імені Івана Франка.

Відповідальний за випуск:

Війчук Т.І., кандидат педагогічних наук, доцент кафедри математики та економіки Дрогобицького державного педагогічного університету імені Івана Франка.

Комарницька Л., Матурін Ю.

К 63 **Алгебра і теорія чисел :** тексти лекцій. Частина 2. Дрогобич : ДДПУ ім. І. Франка, 2023. 112 с.

Тексти лекцій написано відповідно до робочої програми навчальної дисципліни «Алгебра і теорія чисел» для підготовки фахівців освітньо-кваліфікаційного рівня «Бакалавр», затвердженої науково-методичною радою Дрогобицького державного педагогічного університету імені Івана Франка (протокол № 7 від 19.09.2023 р.). Тут висвітлено такі питання, як многочлени від однієї та кількох змінних, многочлени над числовими полями і алгебраїчні числа.

Розрахований на студентів педагогічних закладів вищої освіти, викладачів вищої математики.

Бібліографія 5 назв.

З М І С Т

В С Т У П

Посібник написано відповідно до чинної програми і підручника [1]. У ньому висвітлено такі питання, як многочлени від однієї та кількох змінних, многочлени над полями комплексних, дійсних і раціональних чисел, алгебраїчні числа.

Матеріал посібника поділений на теми, а теми – на пункти. Виклад матеріалу супроводиться розглядом конкретних прикладів.

У кінці кожної теми наведено запитання для самоконтролю, які повинні сприяти активному засвоєнню теорії.

Доцільно зазначити, що нумерація формул, теорем, означень, малюнків ведеться заново у кожній темі.

Цей посібник дає необхідний мінімум матеріалу з розглянутих питань, є доступним не лише студентам денної форми навчання, а й студентам-заочникам.

Розділ І. МНОГОЧЛЕНИ ВІД ОДНІЄЇ ЗМІННОЇ

Тема 1. Кільце многочленів над областю цілісності

З поняттям многочлена ми зустрічалися ще в середній школі, а також при вивченні математичного аналізу і алгебри на першому курсі.

Нехай R – деяка область цілісності.

Означення 1. **Многочленом (поліномом) від однієї змінної** над областю цілісності R називається вираз вигляду:

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

де n – довільне ціле невід'ємне число, $a_n, a_{n-1}, ..., a_1, a_0$ – елементи R, а $x, x^2, ..., x^{n-1}, x^n$ – деякі символи; x^k називається ***k*-м степенем змінної *x*** (або невідомого x), a_k – ***k*-м коефіцієнтом** многочлена (1) або коефіцієнтом при x^k (k=0,…, n).

Многочлени від однієї змінної x позначатимемо маленькими латинськими буквами: $f(x), g(x), q(x)$ і т.д., сукупність усіх многочленів від x над областю цілісності R – символом $R[x]$.

Означення 2. Вираз $a_k x^k$ (k=1,…,n) називається ***k*-м членом** або **членом *k*-го степеня** многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \qquad (2)$$

a_0 – нульовим або вільним членом, причому записи a_0 і $a_0 x^0$ рівнозначні. Якщо $a_k = 0$ (тобто є нульовим елементом області цілісності R), то кажуть, що k-й член многочлена $f(x)$ дорівнює нулю або його немає.

Означення 3. Відмінний від нуля член многочлена $f(x)$, степінь якого більший за степінь усіх інших відмінних від нуля членів цього многочлена, називається **старшим членом**, його коефіцієнт – **старшим коефіцієнтом**, його степінь – **степенем** многочлена $f(x)$.

Степінь многочлена $f(x)$ позначають $\deg f$ (від англ. слова *degree* – «степінь»). Степінь многочлена a_0, де $a_0 \neq 0$, дорівнює нулю.

Наприклад, $f(x)=2x^3-3x+5$, deg $f=3$, $2x^3$ – старший член, 2 – старший коефіцієнт.

Вираз (2) називають **канонічною формою** многочлена $f(x)$. Ця форма запису характеризується тим, що члени упорядковано за спаданням степеня x^k. Вживається також назва «**многочлен стандартного вигляду**».

Якщо всі коефіцієнти многочлена (в тому числі і вільний член) рівні 0, то такий многочлен називатимемо **нуль-многочленом** і позначатимемо $\Theta(x)$. Степінь нуль-многочлена не визначається.

Які ж дії можна виконувати над многочленами?

Нехай дано два многочлени над областю цілісності R:

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0,$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\ldots+b_1x+b_0.$$

Означення 4. Многочлени $f(x)$ і $g(x)$ називаються **рівними** між собою і записуються $f(x)=g(x)$, якщо канонічні форми цих многочленів збігаються, тобто $n=m$ і $a_k=b_k$ (k=0,…,n).

Будемо вважати, що $n\geq m\geq 0$.

Означення 5. **Сумою** многочленів $f(x)$ і $g(x)$ називають многочлен

$$s(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_{m+1}x^{m+1}+(a_m+b_m)x^m+(a_{m-1}+b_{m-1})x^{m-1}+\ldots+$$
$$+(a_1+b_1)x+(a_0+b_0),$$

і записують $s(x)=f(x)+g(x)$.

З цього означення випливають такі **наслідки:**

1. Степінь суми двох многочленів не перевищує більшого з степенів заданих многочленів:

$$\deg(f+g)\leq\max\{\deg f,\deg g\}.$$

2. Для довільного многочлена $f(x)\in R[x]$ і $\theta(x)\in R[x]$

$$f(x)+\theta(x)=f(x).$$

Означення 6. **Добутком** многочленів $f(x)$ і $g(x)$ називають многочлен

$$p(x)=c_{n+m}x^{n+m}+c_{n+m-1}x^{n+m-1}+\ldots+c_1x+c_0,$$

де $c_k = \sum_{j=0}^{k} a_{k-j} b_j = a_k b_0 + a_{k-1} b_1 + \ldots + a_1 b_{k-1} + a_0 b_k$ $(k = 0, \ldots, n+m)$, $a_{k-j} = 0$ при $k - j > n$, $b_j = 0$ при $j > m$. Або в іншій формі: $c_k = \sum_{i+j=k} a_i b_j$, $a_i = 0$ $(i > n)$, $b_j = 0$ $(j > m)$.

З цього означення випливають такі **наслідки**:

1. Якщо $f(x)$ і $g(x)$ не є нуль-многочленами, то

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

2. Добуток двох многочленів, з яких хоч один є нуль-многочленом, дорівнює нуль-многочлену:

$$f(x) = \theta(x) \vee g(x) = \theta(x) \Rightarrow f(x) g(x) = \theta(x).$$

Нуль-многочлен $\theta(x)$ можна розглядати як нульовий елемент кільця R, і тому часто замість $\theta(x)$ писатимемо 0.

Теорема 1. Сукупність $R[x]$ усіх многочленів над областю цілісності R є область цілісності відносно операцій додавання та множення многочленів.

Д о в е д е н н я. Покажемо спочатку, що $R[x]$ є комутативне кільце. Асоціативність додавання многочленів

$$(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$$

випливає безпосередньо з асоціативності додавання елементів у кільці R, бо

$$(a_k + b_k) + c_k = a_k + (b_k + c_k),$$

тут $h(x) = \sum_{k=0}^{l} c_k x^k$.

Нульовим елементом в $R[x]$ є нуль-многочлен $\theta(x)$ (див. наслідок 2 з означення 5).

Для довільного многочлена $f(x) \in R[x]$ в $R[x]$ існує протилежний елемент, а саме многочлен $-f(x) = \sum_{k=0}^{n} (-a_k) x^k$.

Комутативність додавання многочленів

$$f(x) + g(x) = g(x) + f(x)$$

теж випливає з комутативності додавання елементів кільця R, бо

$$a_k + b_k = b_k + a_k .$$

Аналогічно доводиться асоціативність і комутативність множення многочленів.

Дистрибутивний закон

$$(f(x) + g(x))h(x) = f(x)h(x) + g(x)h(x)$$

випливає з такої ж очевидної рівності

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

Отже, $R[x]$ – комутативне кільце.

Покажемо, що в $R[x]$ не існує дільників нуля. Нехай $f(x), g(x) \in R[x],\ f(x) \neq \theta(x), g(x) \neq \theta(x),$ і їхні старші коефіцієнти дорівнюють a_n та b_m відповідно; отже, $a_n \neq 0, b_m \neq 0.$ Тоді многочлен $f(x)g(x)$ має старший коефіцієнт $a_n b_m \neq 0$ (бо в R немає дільників нуля), і тому $f(x)g(x) \neq \theta(x).$

Отже,

$$f(x) \neq \theta(x) \wedge g(x) \neq \theta(x) \Rightarrow f(x)g(x) \neq \theta(x),$$

звідки, з врахування наслідка 2 з означення 6 випливає, що добуток двох многочленів є нуль-многочлен тоді і тільки тоді, коли хоч один з цих многочленів є нуль-многочленом.

Таким чином, $R[x]$ – область цілісності. Теорему доведено.

Оскільки $R[x]$ є кільце, то можна розглядати різницю будь-яких многочленів (аналогічно сумі).

Справедливе також твердження: $R[x]$ є кільце з одиницею тоді і тільки тоді, коли R є кільце з одиницею.

Теорема Безу.
Алгебраїчна і функціональна рівності многочленів

Нехай многочлен $f(x)$ з кільця $R[x]$ має канонічну форму

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

і $\alpha \in R$. Тоді елемент

$$f(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0$$

називають **значенням многочлена *f*(*x*) при** $x=\alpha$ (або значенням многочлена для аргумента α).

Теорема 2 (Теорема Безу). Нехай задано многочлен $f(x)$ з кільця $R[x]$ і $\alpha \in R$. Тоді в кільці $R[x]$ існує такий многочлен $g(x)$, що

$$f(x)=(x-\alpha)g(x)+f(\alpha).$$

Д о в е д е н н я. Якщо $f(x)$ – нульовий многочлен, то в цьому випадку $f(\alpha)=0$ і можна покласти $g(x)=0$. Нехай

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$$

– ненульовий многочлен, тоді

$$f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\ldots+a_1\alpha+a_0$$

і, віднявши почленно ці рівності,

$$f(x)-f(\alpha)=a_n(x^n-\alpha^n)+a_{n-1}(x^{n-1}-\alpha^{n-1})+\ldots+a_1(x-\alpha)=$$
$$=(x-\alpha)[a_n(x^{n-1}+\alpha x^{n-2}+\ldots+\alpha^{n-1})+\ldots+a_2(x+\alpha)+a_1].$$

Отже,

$$f(x)=(x-\alpha)g(x)+f(\alpha),$$

де $g(x)=a_n(x^{n-1}+\alpha x^{n-2}+\ldots+\alpha^{n-1})+\ldots+a_2(x+\alpha)+a_1\in R[x]$.

Теорему доведено.

Часто **теорему Безу** формулюють так:

Остача від ділення многочлена $f(x)\in R[x]$ на $x-\alpha$, $\alpha\in R$, дорівнює $f(\alpha)$.

Приклад. Знайти остачу від ділення многочлена $f(x)=2x^4-x+1$ на двочлен $x+2$.

Остача дорівнює $f(-2)=2\cdot(-2)^4-(-2)+1=32+2+1=35$.

Означення 7. Елемент $\alpha\in R$ називається **коренем** многочлена $f(x)\in R[x]$, якщо $f(\alpha)=0$.

Теорема 3. Елемент $\alpha\in R$ є коренем многочлена $f(x)\in R[x]$ тоді і тільки тоді, коли лінійний двочлен $x-\alpha$ є дільником многочлена $f(x)$.

Д о в е д е н н я. *Необхідність.* Нехай α – корінь многочлена $f(x)$, тобто $f(\alpha)=0$. За теоремою Безу, $f(x)=(x-\alpha)g(x)$, тобто $x-\alpha$ є дільником $f(x)$.

Достатність. Припустимо тепер, що $x-\alpha$ є дільником многочлена $f(x)$; тоді існує $g(x)\in R[x]$ такий, що $f(x)=(x-\alpha)g(x)$. А тоді $f(\alpha)=(\alpha-\alpha)g(\alpha)=0$, тобто $\alpha-$ корінь многочлена $f(x)$.

Теорема 4 (про можливе число коренів многочлена).

Кожен многочлен $f(x)\in R[x]$ степеня n має не більше n різних коренів.

Д о в е д е н н я. Доведення проводимо методом математичної індукції за змінною n.

1. Якщо $\deg f=0$, тобто $f(x)=a_0$, де $a_0\in R$ і $a_0\neq 0$, то многочлен $f(x)$ має нуль коренів.

2. Припустимо, що теорема правильна для многочлена степеня, меншого ніж n.

3. Доведемо, що тоді теорема правильна для многочлена степеня n. Нехай $f(x)\in R[x]$ і $\deg f=n$. Якщо f не має коренів в R, то теорема правильна. Нехай $f(x)$ має хоча б один корінь в R: $x=\alpha$. За теоремою Безу, $f(x)=(x-\alpha)g(x)$, $g(x)\in R[x]$, причому $\deg g=n-1$. За припущенням індукції, многочлен $g(x)$ має не більше, ніж $n-1$ різних коренів. Тому многочлен $f(x)$ має не більше, ніж n різних коренів.

Наслідок. Якщо многочлен $f(x)\in R[x]$ степеня n має в області цілісності R більше, ніж n різних коренів, то $f(x)$ є нуль-многочленом.

Перейдемо тепер до питання про алгебраїчну і функціональну рівності многочленів. Нехай

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\in R[x].$$

Позначимо через $f^*(\alpha)$ функцію

$$f^*(\alpha)=\{(\lambda,a_n\lambda^n+a_{n-1}\lambda^{n-1}+\ldots+a_1\lambda+a_0)/\lambda\in R\},$$

яка кожному елементу $\lambda \in R$ ставить у відповідність значення многочлена $f(x)$ для аргумента λ.

Отже, кожний многочлен $f(x) \in R[x]$ визначає функцію $f^*: R \to R$ (або, інакше кажучи, породжує функцію f^*).

Але виявляється, що для деяких областей цілісності R різні многочлени можуть визначати одну і ту ж функцію. Розглянемо такий приклад. Нехай R – поле класів лишків цілих чисел за модулем 2, тобто $\mathbb{Z}_2 = \left(\{\bar{0}, \bar{1}\}, +, *\right)$. Многочлени

$f(x)=x+x^2$ (тобто $f(x)=\bar{1} \cdot x^2 + \bar{1} \cdot x + \bar{0}$)

$g(x)=x-x^2$ (тобто $g(x)=-\bar{1} \cdot x^2 + \bar{1} \cdot x + \bar{0}$)

$h(x)=0$ (тобто $h(x)=\bar{0}$)

визначають одну і ту ж функцію, бо

$f(\bar{0})=g(\bar{0})=h(\bar{0})=\bar{0}$ і

$f(\bar{1})=g(\bar{1})=h(\bar{1})=\bar{0}$.

Теорема 5. Нехай $R[x]$ – область цілісності многочленів над нескінченною областю цілісності R. Многочлени $f(x), g(x) \in R[x]$ рівні тоді і тільки тоді, коли рівні функції f^* і g^*, які вони визначають.

Д о в е д е н н я. *Необхідність*. Припустимо, що $f(x) = g(x)$. Якщо f і g – нуль-многочлени, то $f^* = g^*$. Припустимо, що f і g – ненульові многочлени степеня n:

$$f(x) = a_n x^n + \ldots + a_1 x + a_0,$$

$$g(x) = b_n x^n + \ldots + b_1 x + b_0.$$

Оскільки, $f(x) = g(x)$, то $\forall k = 0, \ldots, n \;\; a_k = b_k$.

Для $\forall \lambda \in R$ маємо:

$$f^*(\lambda) = a_n \lambda^n + \ldots + a_1 \lambda + a_0, \;\; g^*(\lambda) = b_n \lambda^n + \ldots + b_1 \lambda + b_0.$$

Звідси, оскільки $\forall k = 0, \ldots, n \;\; a_k = b_k \qquad f^* = g^*$.

Достатність. Припустимо, що $f^* = g^*$, тобто для $\forall \lambda \in R$ $f(\lambda) = g(\lambda)$:

$$a_n \lambda^n + \ldots + a_1 \lambda + a_0 = b_n \lambda^n + \ldots + b_1 \lambda + b_0.$$

Тоді для многочлена $h(x) = f(x) - g(x)$ виконується умова:

$$\forall \lambda \in R \;\; h(\lambda) = 0.$$

Оскільки множина R нескінченна, то ця умова означає, що многочлен $h(x)$ має нескінченну множину різних коренів. А за наслідком з теореми 4, $h(x)$ є нульовим многочленом, тобто $f(x)-g(x)=0$ і $f(x)=g(x)$. Таким чином, з того, що $f^*=g^*$, випливає, що $f=g$. Теорему доведено.

Отже, в наведеному вище прикладі многочлени $f(x)$, $g(x)$, $h(x)$ рівні в функціональному розумінні, але не в алгебраїчному розумінні.

З теореми 5 випливає, зокрема, що якщо R – довільне числове поле, то з алгебраїчної рівності многочленів випливає їх функціональна рівність і навпаки.

Питання для самоконтролю

1. Дайте означення многочлена від однієї змінної.
2. Дайте означення рівності многочленів, суми і добутку многочленів.
3. Доведіть, що сукупність усіх многочленів над областю цілісності є область цілісності відносно операцій додавання та множення многочленів.
4. Сформулюйте та доведіть теорему Безу.
5. Дайте означення кореня многочлена. Скільки різних коренів має многочлен n-го степеня?
6. Що означає рівність многочленів у функціональному розумінні?

Тема 2. Многочлени над полем. Ділення многочленів з остачею. Схема Горнера

Досі ми розглядали кільце многочленів над областю цілісності R. Тепер вимагатимемо, щоб область цілісності R була **полем**, тобто щоб в R для довільного елемента $a\neq 0$ існував обернений елемент a^{-1}.

Отже, розглядатимемо **многочлени над полем** P. Оскільки будь-яке поле є областю цілісності з одиницею, то сукупність усіх многочленів над полем P є область цілісності з одиницею відносно додавання і множення многочленів, яку позначатимемо $P[x]$. Проте $P[x]$ полем не є. Більш того, для жодного многочлена ненульового степеня з $P[x]$ не існує оберненого елемента. Справді, нехай $f(x) \in P[x]$, $\deg f \geq 1$. Тоді рівність $f(x) \cdot g(x) = 1$ неможлива ні при якому $g(x) \in P[x]$, бо $g(x)$ не може бути нуль-многочленом, тому $\deg(f \cdot g) = \deg f + \deg g \geq 1$, звідки $f(x) \cdot g(x) \neq 1$. Якщо ж $\deg f = 0$, то для елемента f існує обернений в $P[x]$, і цей обернений елемент теж є многочлен нульового степеня. Інакше кажучи, дільниками одиниці в області цілісності $P[x]$ є многочлени нульового степеня (відмінні від нуля константи).

Отже, два різні многочлени з $P[x]$, як правило, не діляться один на одного. Але для $P[x]$ можна побудувати теорію подільності, аналогічну теорії подільності цілих чисел, якщо операцію ділення многочленів замінити більш загальною операцією ділення з остачею.

Кажуть, що многочлен $f(x) \in P[x]$ **ділиться з остачею** на многочлен $g(x) \neq 0$ з кільця $P[x]$, якщо в $P[x]$ існують такі многочлени $s(x)$ і $r(x)$, що:

1) $f(x) = g(x) \cdot s(x) + r(x)$;

2) $r(x) = 0$ або $\deg r < \deg g$.

При цьому $f(x)$ називають **діленим**, $g(x)$ – **дільником**, $s(x)$ – **часткою**, $r(x)$ – **остачею**.

Отже, умова для чисел, щоб остача була менша за модуль дільника, у випадку многочленів замінюється умовою, щоб степінь остачі був менший від степеня дільника.

Теорема (про ділення з остачею). Довільний многочлен $f(x)$ з кільця $P[x]$ ділиться з остачею на будь-який ненульовий многочлен

$g(x)$ з цього кільця, причому частка і остача визначаються однозначно.

Тобто:

$$\forall f(x), g(x) \in P[x],\ g(x) \neq 0 \qquad \exists!\, s(x), r(x) \in P[x]:$$

$$f(x) = g(x) \cdot s(x) + r(x), \quad r(x) = 0 \text{ або } \deg r < \deg g\,. \qquad (1)$$

Д о в е д е н н я. Доведемо спочатку *існування* в кільці $P[x]$ многочленів $s(x)$ і $r(x)$ таких, що задовольняють умову (1). Нехай

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \quad (\deg f = n),$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 \quad (\deg g = m).$$

Якщо $f(x) = 0$ або $n < m$, то $f(x) = g(x) \cdot 0 + f(x)$ і можна вважати, що $s(x) = 0$, $r(x) = f(x)$. Тому залишається розглянути випадок, коли $n \geq m$.

Проведемо доведення методом математичної індукції за змінною n. При $n = 0$ $(n \geq m)$ маємо, що $m = 0$, $f(x) = a_0$, $g(x) = b_0 \neq 0$, тому $s(x) = \dfrac{a_0}{b_0}$, $r(x) = 0$. Очевидно, $s(x) \in P[x]$, бо $\dfrac{a_0}{b_0} \in P$.

Припустимо, що теорема справедлива для всіх многочленів степеня, меншого ніж n, і доведемо її для многочленів степеня n. Розглянемо многочлен

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

де $a_n \neq 0$ і $b_m \neq 0$. Старший член многочлена $\dfrac{a_n}{b_m} x^{n-m} g(x)$ дорівнює $a_n x^n$, тобто старшому члену многочлена $f(x)$. Тому $\deg p < n$ і, за припущенням індукції, $p(x)$ можна поділити з остачею на $g(x)$:

$$p(x) = g(x) \cdot s_1(x) + r_1(x), \qquad s_1(x), r_1(x) \in P[x]\ ,$$

$$r_1(x) = 0 \qquad \text{або} \qquad \deg r_1 < \deg g\,.$$

Отже, $\quad f(x) - \dfrac{a_n}{b_m} x^{n-m} g(x) = g(x) \cdot s_1(x) + r_1(x)$, звідки

$$f(x) = g(x)\left(s_1(x) + \frac{a_n}{b_m} x^{n-m} \right) + r_1(x) = g(x) \cdot s(x) + r(x),$$

де $$s(x) = s_1(x) + \frac{a_n}{b_m} x^{n-m}, \quad r(x) = r_1(x).$$

Очевидно, що $s(x), r(x) \in P[x]$ і що $r(x) = 0$ або $\deg r < \deg g$.

Покажемо тепер *єдиність* частки $s(x)$ і остачі $r(x)$. Припустимо протилежне, тобто що можливі два записи:

$$f(x) = g(x) \cdot s(x) + r(x), \quad r(x) = 0 \text{ або } \deg r < \deg g,$$

$$f(x) = g(x) \cdot s_1(x) + r_1(x), \quad r_1(x) = 0 \text{ або } \deg r_1 < \deg g.$$

Віднімемо почленно ці рівності:

$$g(x)\big(s(x) - s_1(x)\big) = r_1(x) - r(x), \quad r_1(x) - r(x) = 0 \text{ або } \deg(r_1 - r) < \deg g.$$

Якщо $r_1(x) - r(x) \neq 0$, то і $s(x) - s_1(x) \neq 0$ (бо кільце $P[x]$ не має дільників нуля і за умовою $g(x) \neq 0$), і, крім того,

$$\deg(r_1 - r) = \deg g + \deg(s - s_1) \geq \deg g.$$

Ми прийшли до суперечності. Отже, $r(x) = r_1(x)$ і тому $s(x) = s_1(x)$, що свідчить про єдиність частки і остачі. Теорему доведено.

Наслідок. Кільце $P[x]$ многочленів над полем P є евклідове кільце.

Цей наслідок випливає з того, що $P[x]$ є область цілісності та існує відображення $\varphi: \quad P[x] \setminus \{0\} \to \mathbb{N}^0$ таке, що має місце ділення з остачею. При цьому відображення φ задається так:

$$\varphi(f(x)) \overset{df}{=} \deg f \in \mathbb{N}^0,$$

тобто кожному многочлену $f(x) \in P[x]$, відмінному від нуля, ставиться у відповідність його степінь.

Основними методами ділення многочлена на многочлен є **метод ділення кутом** та **метод невизначених коефіцієнтів**. Розглянемо приклад.

$$f(x) = 3x^5 + x^4 - 10x^3 + 12x^2 + 10x - 8, \quad g(x) = 3x^2 + x - 1.$$

Ділимо «кутом»:

$$
\begin{array}{l|l}
3x^5+x^4-10x^3+12x^2+10x-8 & 3x^2+x-1 \\
\cline{2-2}
3x^5+x^4-\quad x^3 & x^3-3x+5 \\
\cline{1-1}
-9x^3+12x^2+10x-8 & \\
-9x^3-3x^2+3x & \\
\cline{1-1}
15x^2+7x-8 & \\
15x^2+5x-5 & \\
\cline{1-1}
2x-3 &
\end{array}
$$

Отже, частка $s(x)=x^3-3x+5$, остача $r(x)=2x-3$.

Частку $s(x)$ і остачу $r(x)$ можна знаходити і методом невизначених коефіцієнтів, а саме: в загальному випадку $s(x)$ шукають у вигляді многочлена з невизначеними коефіцієнтами степеня $n-m$, а $r(x)$ – степеня $m-1$ ($n=\deg f$, $m=\deg g$). Розглянемо цей метод для випадку, коли $g(x)=x-\alpha$, тобто коли многочлен-дільник є лінійний двочлен.

Ділення многочлена на двочлен $x-\alpha$. Схема Горнера

Нехай маємо многочлен

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0.$$

Поділимо його на двочлен $x-\alpha$:

$$f(x)=(x-\alpha)s(x)+r(x).$$

Очевидно, що $r(x)$ є многочлен степеня не вище нульового, тобто константа, а $s(x)$ – многочлен степеня $n-1$. Використовуючи метод невизначених коефіцієнтів, отримаємо

$$a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=(x-\alpha)(A_{n-1}x^{n-1}+A_{n-2}x^{n-2}+\ldots+A_1x+A_0)+r=$$
$$=A_{n-1}x^n+A_{n-2}x^{n-1}+\ldots+A_1x^2+A_0x-$$
$$-\alpha A_{n-1}x^{n-1}-\alpha A_{n-2}x^{n-2}-\ldots-\alpha A_1x-\alpha A_0+r=$$
$$=A_{n-1}x^n+(A_{n-2}-\alpha A_{n-1})x^{n-1}+(A_{n-3}-\alpha A_{n-2})x^{n-2}+\ldots+(A_1-\alpha A_2)x^2+$$
$$+(A_0-\alpha A_1)x+(r-\alpha A_0).$$

Прирівняємо коефіцієнти при однакових степенях:

$$
\begin{aligned}
a_n &= A_{n-1}\\
a_{n-1} &= A_{n-2} - \alpha A_{n-1}\\
a_{n-2} &= A_{n-3} - \alpha A_{n-2}\\
&\cdots\cdots\cdots\cdots\cdots\\
a_2 &= A_1 - \alpha A_2\\
a_1 &= A_0 - \alpha A_1\\
a_0 &= r - \alpha A_0.
\end{aligned}
$$

Звідси

$$
\begin{aligned}
A_{n-1} &= a_n\\
A_{n-2} &= a_{n-1} + \alpha A_{n-1}\\
A_{n-3} &= a_{n-2} + \alpha A_{n-2}\\
&\cdots\cdots\cdots\cdots\cdots\\
A_1 &= a_2 + \alpha A_2\\
A_0 &= a_1 + \alpha A_1\\
r &= a_0 + \alpha A_0.
\end{aligned}
\qquad (2)
$$

Формули (2) можна записати у вигляді таблиці, яка називається **схемою Горнера** (на честь англійського математика Горнера (1768–1837)):

	a_n	a_{n-1}	a_{n-2}	…	a_2	a_1	a_0
α	$\underbrace{a_n}_{A_{n-1}}$	$\underbrace{\alpha A_{n-1} + a_{n-1}}_{A_{n-2}}$	$\underbrace{\alpha A_{n-2} + a_{n-2}}_{A_{n-3}}$	…	$\underbrace{\alpha A_2 + a_2}_{A_1}$	$\underbrace{\alpha A_1 + a_1}_{A_0}$	$\underbrace{\alpha A_0 + a_0}_{r}$

Виконуючи ділення за цією схемою, кожний наступний коефіцієнт A_{k-1} частки й остачу r дістають множенням щойно обчисленого коефіцієнта A_k на α і додаванням до знайденого добутку відповідного коефіцієнта a_k даного многочлена.

Зауважимо, що ділення з остачею многочлена $f(x)$ на лінійний двочлен вигляду $x-\alpha$ здійсненне в кільці многочленів як над полем P, так і над будь-якою областю цілісності R.

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

	2	0	3	-1	1	2
-1	2	-2	5	-6	7	-5

Отже, $s(x) = 2x^4 - 2x^3 + 5x^2 - 6x + 7$, $r = -5$. Виконаємо перевірку за теоремою Безу: $r = f(-1) = -2 - 3 - 1 - 1 + 2 = -5$.

Розклад многочлена за степенями $x - \alpha$

Схему Горнера особливо зручно використовувати тоді, коли знайдену частку $s(x)$ треба знову ділити на який-небудь лінійний множник. За допомогою такого ділення можна дістати розклад довільного многочлена $f(x)$ за степенями $x - \alpha$.

Нехай $f(x)$ – многочлен n-го степеня над полем P, $\alpha \in P$. Поділимо $f(x)$ на $x - \alpha$:

$$f(x) = (x - \alpha) f_1(x) + c_0,$$

де $f_1(x)$ – многочлен $(n-1)$-го степеня з $P[x]$, c_0 – елемент поля P. Якщо $n > 1$, то аналогічно маємо:

$$f_1(x) = (x - \alpha) f_2(x) + c_1,$$
$$f_2(x) = (x - \alpha) f_3(x) + c_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..$$
$$f_{n-1}(x) = (x - \alpha) f_n(x) + c_{n-1}.$$

Очевидно, $f_n(x)$ є многочленом нульового степеня; візьмемо $f_n(x) = c_n$.

Підставимо кожну з цих рівностей, починаючи з другої, в попередню, отримаємо:

$$f(x) = (x-\alpha)\big((x-\alpha) f_2(x) + c_1\big) + c_0 = (x-\alpha)^2 f_2(x) + c_1(x-\alpha) + c_0 =$$
$$= (x-\alpha)^2\big((x-\alpha) f_3(x) + c_2\big) + c_1(x-\alpha) + c_0 =$$
$$= (x-\alpha)^3 f_3(x) + c_2(x-\alpha)^2 + c_1(x-\alpha) + c_0 = \ldots =$$
$$= c_n(x-\alpha)^n + c_{n-1}(x-\alpha)^{n-1} + \ldots + c_2(x-\alpha)^2 + c_1(x-\alpha) + c_0,$$

тобто

$$f(x) = c_n(x-\alpha)^n + c_{n-1}(x-\alpha)^{n-1} + \ldots + c_2(x-\alpha)^2 + c_1(x-\alpha) + c_0. \qquad (3)$$

Отже, многочлен $f(x)$ над полем P ми подали як многочлен того самого степеня над тим самим полем, але від змінної $y = x - \alpha$.

З'ясуємо, чому рівні коефіцієнти $c_n, c_{n-1}, ..., c_2, c_1, c_0$.

c_0 – остача від ділення $f(x)$ на $x - \alpha$, тобто $f(\alpha)$ (за теоремою Безу),

c_1 – остача від ділення $f_1(x)$ на $x - \alpha$, тобто $f_1(\alpha)$,

……,

c_{n-1} – остача від ділення $f_{n-1}(x)$ на $x - \alpha$, тобто $f_{n-1}(\alpha)$,

c_n – остання частка в процесі послідовного ділення.

Приклад. Знайти розклад многочлена $f(x) = 2x^5 - x^4 + x^3 - 3x^2 + 2x - 4$ за степенями двочлена $x - 1$.

	2	-1	1	-3	2	-4
1	2	1	2	-1	1	**-3**
1	2	3	5	4	**5**	
1	2	5	10	**14**		
1	2	7	**17**			
1	2	**9**				
1	**2**					

Отже, $f(x) = 2(x-1)^5 + 9(x-1)^4 + 17(x-1)^3 + 14(x-1)^2 + 5(x-1) - 3$.

Аналогічно зробимо перевірку. Маємо многочлен $f(x-1)$. Зробимо заміну $x - 1 = y$, звідки $x = y + 1$.

Многочлен $f(x) = 2y^5 + 9y^4 + 17y^3 + 14y^2 + 5y - 3$ розкладемо за степенями $x = y + 1$:

	2	9	17	14	5	-3
-1	2	7	10	4	1	**-4**
-1	2	5	5	-1	**2**	
-1	2	3	2	**-3**		
-1	2	1	**1**			
-1	2	**-1**				
-1	**2**					

Формула Тейлора

Дамо означення похідної від многочлена.

Означення. Похідною від многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

називається многочлен

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 2a_2 x + a_1 .$$

Похідну від многочлена нульового степеня, а також похідну від нуль-многочлена беруть рівною нулю.

З цього означення випливає, що похідна від многочлена над полем P є знову многочлен над полем P.

Уважатимемо, що P є поле характеристики 0 (тобто $n \cdot e = 0$ лише при $n = 0$). При цій умові можна твердити, що $\deg f' = \deg f - 1$, якщо $\deg f \geq 1$, бо з умови $a_n \neq 0$ при будь-якому $n \geq 1$ випливає $n a_n \neq 0$. Якщо ж P має характеристику $p \geq 1$, то многочлен $g(x) = x^p$ степеня p має похідною нуль-многочлен, бо $p \cdot x^{p-1} = 0$.

Аналогічно також можна означити другу похідну $f''(x)$ від многочлена $f(x)$, третю $f'''(x)$ і т. д.

Знайдемо усі похідні многочлена $f(x)$ до n-го порядку і їх значення при $x = \alpha$, виходячи з формули (3):

$f'(x) = n c_n (x-\alpha)^{n-1} + (n-1) c_{n-1} (x-\alpha)^{n-2} + \ldots + 2c_2 (x-\alpha) + c_1$;

$f'(\alpha) = c_1 = 1! c_1$;

$f''(x) = n(n-1) c_n (x-\alpha)^{n-2} + (n-1)(n-2) c_{n-1} (x-\alpha)^{n-3} + \ldots + 2c_2$;

$f''(\alpha) = 2c_2 = 2! c_2$; .....

$f^{(n-1)}(\alpha) = (n-1)! c_{n-1}$;

$f^{(n)}(\alpha) = n! c_n$.

Знайдемо з цих рівностей $c_1, c_2, \ldots, c_n$ і підставимо у формулу (3), враховуючи, що $c_0 = f(\alpha)$. Отримаємо інший запис формули (3):

$$f(x) = \frac{f^{(n)}(\alpha)}{n!}(x-\alpha)^n + \frac{f^{(n-1)}(\alpha)}{(n-1)!}(x-\alpha)^{n-1} + \ldots + \frac{f''(\alpha)}{2!}(x-\alpha)^2 + \frac{f'(\alpha)}{1!}(x-\alpha) + f(\alpha). \quad (4)$$

Отримана формула (4) називається **формулою Тейлора** для многочленів, причому вона має місце лише для многочленів над полем характеристики 0.

Питання для самоконтролю

1. Що означає, що многочлен $f(x)$ ділиться з остачею на многочлен $g(x)$? Сформулюйте теорему про ділення многочленів з остачею.
2. Охарактеризуйте основні методи ділення многочленів.
3. Для чого використовується схема Горнера?
4. Як розкласти многочлен за степенями $x-\alpha$, використовуючи схему Горнера?
5. Виведіть формулу Тейлора для многочлена *n*-го степеня.

Тема 3. Властивості подільності многочленів. Найбільший спільний дільник многочленів. Алгоритм Евкліда. НСК двох многочленів

Кажуть, що многочлен $f(x)\in P[x]$ ділиться на многочлен $g(x)\in P[x]$ і записують $f(x)\vdots g(x)$, якщо остача $r(x)$ при діленні $f(x)$ на $g(x)$ дорівнює нулю, тобто якщо існує многочлен $s(x)\in P[x]$ такий, що

$$f(x)=g(x)s(x).$$

Якщо $f(x)\vdots g(x)$, то кажуть, що $g(x)$ ділить $f(x)$ або є дільником $f(x)$ і записують $g(x)/f(x)$.

Зауважимо, що нуль-многочлен ділиться на довільний многочлен, відмінний від нуля, при цьому частка теж є нуль-многочлен.

Властивості подільності многочленів у кільці $P[x]$**:**

1. $\forall f(x),g(x),h(x)\in P[x]\quad f(x)\vdots g(x)\wedge g(x)\vdots h(x)\Rightarrow f(x)\vdots h(x)$.
2. $\forall f(x),g(x),h(x)\in P[x]\quad f(x)\vdots h(x)\wedge g(x)\vdots h(x)\Rightarrow (f(x)+g(x))\vdots h(x)$.

3. $\forall f(x), h(x) \in P[x] \quad f(x) \vdots h(x) \Rightarrow \forall g(x) \in P[x] \quad f(x)g(x) \vdots h(x)$.

4. $\forall f_1(x), ..., f_m(x), h(x) \in P[x]$

$f_1(x) \vdots h(x) \wedge ... \wedge f_m(x) \vdots h(x) \Rightarrow \forall g_1(x), ..., g_m(x) \in P[x]$

$(f_1(x)g_1(x) + ... + f_m(x)g_m(x)) \vdots h(x)$.

5. $\forall f(x) \in P[x] \ \forall c \in P \setminus \{0\} \quad f(x) \vdots c$.

6. $\forall f(x), g(x) \in P[x] \ \forall c \in P \setminus \{0\} \quad f(x) \vdots g(x) \Rightarrow f(x) \vdots cg(x)$.

7. $\forall f(x), g(x) \in P[x] \quad f(x) \vdots g(x) \wedge g(x) \vdots f(x) \Rightarrow \exists c \in P \quad f(x) = cg(x)$.

Остання властивість говорить про те, що, якщо многочлени $f(x)$, $g(x)$ з кільця $P[x]$ асоційовані (тобто діляться один на одного), то вони відрізняються лише множником, який є відмінною від нуля константою: $f(x) = cg(x)$ або $g(x) = \frac{1}{c} f(x)$. (Нагадаємо, що два елементи області цілісності з одиницею називаються асоційованими, якщо вони відрізняються лише множником, що є дільником одиниці, а дільниками одиниці в кільці $P[x]$ є всі відмінні від нуля константи).

Розглянемо тепер питання про будову ідеалів кільця $P[x]$. Непорожня множина I многочленів $f(x) \in P[x]$ є ідеалом кільця $P[x]$, якщо вона є групою відносно додавання і якщо $\forall f(x) \in I$ $\forall g(x) \in P[x] \quad f(x)g(x) \in I$.

Оскільки кільце $P[x]$ є евклідове кільце (див. наслідок з теореми про ділення многочленів з остачею), то $P[x]$ є кільце головних ідеалів. Причому будь-який головний ідеал кільця $P[x]$ має вигляд $(f) = \{f(x)g(x)\}$, де $f(x)$ – фіксований, а $g(x)$ – довільний многочлен з $P[x]$. Інакше кажучи, (f) (ідеал, породжений елементом $f(x)$) складається з усіх многочленів кільця $P[x]$, які діляться на $f(x)$. Оскільки $P[x]$ – кільце головних ідеалів, то для довільного ідеалу I кільця $P[x]$ знайдеться многочлен $f(x)$ такий, що $I = (f)$.

Перейдемо до питання про найбільшого спільного дільника двох многочленів.

Означення 1. Многочлен $d(x) \in P[x]$ називається **спільним дільником** многочленів $f(x)$ і $g(x)$ з $P[x]$, якщо $f(x) \vdots d(x)$ і $g(x) \vdots d(x)$.

Означення 2. Спільний дільник многочленів $f(x)$ і $g(x)$, який ділиться на кожний інший спільний дільник цих многочленів, називається **найбільшим спільним дільником** (НСД) многочленів $f(x)$ і $g(x)$ і позначається символом (f, g).

Ці означення узагальнюються на випадок більше як двох многочленів.

НСД двох многочленів визначається однозначно з точністю до сталого множника. Справді, якщо $d(x)$ і $d_1(x)$ – НСД двох многочленів, то $d(x) \vdots d_1(x)$, а $d_1(x) \vdots d(x)$. Тоді $d(x)$ і $d_1(x)$ асоційовані, тобто $d_1(x) = cd(x)$, де c – константа, відмінна від нуля.

Означення 3. Многочлени $f(x), g(x) \in P[x]$ називаються **взаємно простими,** якщо кожний їхній спільний дільник є многочленом нульового степеня (відмінною від нуля константою). При цьому записують $(f, g)=1$.

Теорема 1. Для будь-яких двох многочленів $f(x), g(x) \in P[x]$ існує найбільший спільний дільник $d(x)$, причому $d(x)$ можна подати у вигляді

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

де $u(x), v(x)$ – деякі многочлени з $P[x]$.

Д о в е д е н н я цієї теореми випливає з відповідної теореми, справедливої для будь-якого кільця головних ідеалів.

Наслідок. Многочлени $f(x), g(x) \in P[x]$ взаємно прості тоді і тільки тоді, коли існують многочлени $u(x), v(x) \in P[x]$ такі, що

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

Взаємно прості многочлени мають такі ***властивості:***

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

Розглянемо тепер спосіб знаходження НСД двох многочленів.

Оскільки $P[x]$ є евклідове кільце, у ньому застосовна процедура знаходження НСД за допомогою послідовного ділення з остачею або алгоритму Евкліда. Розглянемо **алгоритм Евкліда** стосовно знаходження НСД двох многочленів.

Нехай дано многочлени $f(x)$ і $g(x)$, причому $\deg f \geq \deg g$. Виконаємо послідовне ділення з остачею, яке можна записати за допомогою системи рівностей:

$$\begin{aligned} f(x) &= g(x)s_1(x) + r_1(x), \\ g(x) &= r_1(x)s_2(x) + r_2(x), \\ r_1(x) &= r_2(x)s_3(x) + r_3(x), \\ &\text{– – – – – – – – – – – – – –} \\ r_{n-2}(x) &= r_{n-1}(x)s_n(x) + r_n(x), \\ r_{n-1}(x) &= r_n(x)s_{n+1}(x). \end{aligned} \qquad (1)$$

Тут ми виходимо з того, що після скінченного числа ділень остача $r_{n+1}(x) = 0$. Справді, з означення остачі, $\deg r_1 < \deg g$, $\deg r_2 < \deg r_1, ...,$ тобто маємо ланцюжок нерівностей $\deg g > \deg r_1 > \deg r_2 > ...$. Це означає, що або якась з остач $r_k(x)$ дорівнюватиме 0, або степінь остачі дорівнюватиме 0. Якщо $\deg r_n = 0$, то $r_{n+1} = 0$, бо будь-який многочлен ділиться на многочлен нульового степеня. Отже, алгоритм Евкліда для многочленів зводиться до *скінченного* числа ділень з остачею.

Покажемо, що остання відмінна від нуля остача $r_n(x)$ у системі рівностей (1) і є НСД многочленів $f(x)$ і $g(x)$. Остання рівність означає, що $r_n(x)$ є дільником $r_{n-1}(x)$. Оскільки кожен з доданків правої частини передостанньої рівності ділиться на $r_n(x)$ $(r_{n-1} \vdots r_n \wedge r_n \vdots r_n)$, то і її ліва частина – на $r_n(x)$, тобто $r_n(x)$ є дільником $r_{n-2}(x)$. Аналогічно можна показати, що $r_n(x)$ є дільником $r_{n-3}, r_{n-4}, ..., r_2, r_1, g, f$. Отже, $r_n(x)$ є спільним дільником $f(x)$ і $g(x)$.

Покажемо тепер, що $r_n(x)$ ділиться на будь-який спільний дільник многочленів $f(x)$ і $g(x)$. Нехай $h(x)$ – довільно вибраний спільний дільник многочленів $f(x)$ і $g(x)$. Тоді з першої рівності

(1) випливає, що $r_1(x) \vdots h(x)$, з другої – що $r_2(x) \vdots h(x)$, з третьої – що $r_3(x) \vdots h(x)$ і т. д. З передостанньої рівності випливає, що $r_n(x) \vdots h(x)$. Таким чином, многочлен $r_n(x)$ є спільним дільником $f(x)$ і $g(x)$, і ділиться на будь-який спільний дільник цих многочленів, тобто $r_n(x)$ є найбільшим спільним дільником многочленів $f(x)$ і $g(x)$.

Отже, ми довели **теорему 2**:

Для будь-яких двох многочленів $f(x)$ і $g(x)$ з кільця $P[x]$ (з яких хоча б один відмінний від 0) існує найбільший спільний дільник, який дорівнює останній відмінний від нуля остачі в алгоритмі Евкліда.

Якщо треба знайти НСД більше як двох многочленів $f_1(x), f_2(x),..., f_n(x)$, то його шукають так:

$$(f_1, f_2) = d_1(x),$$
$$(d_1, f_3) = d_2(x),$$
$$(d_{2,} f_4) = d_3(x),$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$(d_{n-2}, f_n) = d_{n-1}(x).$$

Тоді $(f_1, f_2,..., f_n) = d_{n-1}(x)$. Справді, $f_k(x)$, $k = 1,...,n$, ділиться на $d_{n-1}(x)$, бо $f_k(x) \vdots d_{k-1}(x), d_{k-1}(x) \vdots d_k(x), d_k(x) \vdots d_{k+1}(x)$ і т.д., $d_{n-2}(x) \vdots d_{n-1}(x)$. Якщо тепер $d(x)$ – будь-який спільний дільник для $f_1, f_2,..., f_n$, то він є також дільником для $d_1(x), d_2(x),..., d_{n-1}(x)$. Отже, $d_{n-1}(x)$ – найбільший спільний дільник многочленів $f_1, f_2,..., f_n$.

У кільці $P[x]$ многочленів над полем P можна означити і найменше спільне кратне елементів.

Означення 4. **Спільним кратним** многочленів $f(x), g(x) \in P[x]$ називається будь-який многочлен $s(x) \in P[x]$ такий, що $s(x) \vdots f(x) \wedge s(x) \vdots g(x)$. **Найменшим спільним кратним** (НСК) многочленів $f(x)$, $g(x)$ називається спільне кратне $f(x)$ і $g(x)$, на яке ділиться будь-яке інше спільне кратне цих многочленів. НСК многочленів $f(x)$ і $g(x)$ позначають $[f, g]$.

Теорема 3. Для будь-яких відмінних від нуля многочленів $f(x)$ і $g(x)$ з кільця $P[x]$ найменше спільне кратне існує і визначається однозначно з точністю до сталого множника за формулою

$$[f,g]=\frac{f(x)g(x)}{(f,g)}.$$

Д о в е д е н н я. Розглянемо многочлен

$$q(x)=\frac{f(x)g(x)}{d(x)},$$

де $d(x)=(f,g)$. Очевидно, що $q(x)$ є спільне кратне $f(x)$ і $g(x)$, бо

$$q(x)=\frac{f(x)}{d(x)}g(x)=\frac{g(x)}{d(x)}f(x).$$

Нехай тепер $s(x)$ – будь-яке інше спільне кратне многочленів $f(x)$ і $g(x)$; тоді $s(x)\vdots f(x)$ і $s(x)\vdots g(x)$, і тому $s(x)=s_1(x)f(x)$, причому

$$\frac{s(x)}{g(x)}=\frac{s_1(x)f(x)}{g(x)}=p(x)$$

– многочлен з $P[x]$.

Многочлени $f(x)$ і $g(x)$ можна подати у вигляді $f(x)=d(x)f_1(x),\quad g(x)=d(x)g_1(x),$ де $f_1(x),g_1(x)\in P[x]$, причому $(f_1,g_1)=1$. Тоді

$$p(x)=\frac{s_1(x)f_1(x)d(x)}{g_1(x)d(x)}=\frac{s_1(x)f_1(x)}{g_1(x)}.$$

Оскільки $(f_1,g_1)=1$, то $s_1(x)\vdots g_1(x)$.

Нехай $\frac{s_1(x)}{g_1(x)}=t(x)\in P[x]$, тоді $s_1(x)=g_1(x)t(x)$, звідки

$$s(x)=s_1(x)f(x)=f(x)g_1(x)t(x)=\frac{f(x)g(x)}{d(x)}t(x)=q(x)t(x),$$

тобто $s(x)\vdots q(x)$.

Отже, $q(x)$ є найменше спільне кратне $f(x)$ і $g(x)$. Якщо $q_1(x)$ – будь-яке інше НСК цих многочленів, то $q(x)\vdots q_1(x)$ і $q_1(x)\vdots q(x)$, звідки ясно, що $q(x)$ і $q_1(x)$ відрізняються лише сталим множником. Теорему доведено.

Аналогічно до НСД можна розглядати НСК довільного числа многочленів.

Приклад. Знайти НСД і НСК многочленів:

$$f(x)=x^4-4,\ g(x)=4x^3-x^2+8x-2.$$

Застосуємо алгоритм Евкліда. Поділимо многочлен вищого степеня $f(x)$ на многочлен нижчого степеня $g(x)$. Многочлен $f(x)$ домножимо на 4, щоб уникнути дробових коефіцієнтів. При цьому частка й остача теж помножаться на 4, але це істотного значення не має, оскільки всі многочлени ми визначаємо з точністю до сталого множника.

$$\begin{array}{r|l} x^4-4 & 4x^3-x^2+8x-2 \\ \underline{-4x^4-16} & x+1 \\ 4x^4-x^3+8x^2-2x & \\ \hline x^3-8x^2+2x-16 & \text{(домножуємо на 4)} \\ \underline{-4x^3-32x^2+8x-64} & \\ 4x^3-x^2+8x-2 & \\ \hline -31x^2-62 & \text{(ділимо на (–31))} \end{array}$$

$$\begin{array}{r|l} -4x^3-x^2+8x-2 & x^2+2 \\ \underline{4x^3+8x} & 4x-1 \\ -x^2-2 & \\ \underline{-x^2-2} & \\ 0 & \end{array}$$

Отже, $(f,g)=x^2+2.$

$$[f,g]=\frac{fg}{(f,g)}=\frac{(x^4-4)(4x^3-x^2+8x-2)}{x^2+2}=(x^2-2)(4x^3-x^2+8x-2)=$$

$$=4x^5-x^4-16x+4.$$

Питання для самоконтролю

1. Сформулюйте основні властивості подільності многочленів.
2. Дайте означення спільного дільника, найбільшого спільного дільника двох або більше многочленів.
3. Які многочлени називаються взаємно простими? Які властивості вони мають?
4. Розкрийте суть алгоритму Евкліда для знаходження НСД двох многочленів.
5. Дайте означення спільного кратного, найменшого спільного кратного многочленів.
6. Сформулюйте і доведіть теорему про найменше спільне кратне двох многочленів.

Тема 4. Звідні та незвідні многочлени над полем. Розклад многочленів на незвідні множники

Розглянемо, які з елементів області цілісності $P[x]$ є нерозкладними або простими.

Нагадаємо, що елемент області цілісності називається **нерозкладним** або **простим**, якщо він не є дільником одиниці і не має нетривіальних дільників. Переформулюємо це означення стосовно кільця многочленів над полем P, увівши для нерозкладного (простого) многочлена спеціальний термін – незвідний.

Означення 1. Многочлен $f(x) \in P[x]$ називається **незвідним** у полі P, якщо він не є константою і не має в $P[x]$ дільників, відмінних від констант і від многочленів вигляду $cf(x)$, де c – константа.

Інакше кажучи, $f(x) \in P[x]$ – незвідний у полі P, якщо $\deg f \geq 1$ і якщо з рівності $f(x) = g(x)s(x)$, де $g(x), s(x) \in P[x]$, випливає, що $\deg g = 0$ або $\deg s = 0$.

Розкладні (або складені) елементи області цілісності $P[x]$ називатимемо звідними многочленами у полі.

Означення 2. Многочлен $f(x) \in P[x]$ називається **звідним** у полі P, якщо $\deg f \geq 1$ і в кільці $P[x]$ існують такі многочлени $g(x), s(x)$, що $f(x) = g(x)s(x)$, причому $\deg g \geq 1$ і $\deg s \geq 1$.

Отже, будь-який многочлен, вищий від нульового степеня, є або звідним, або незвідним у даному полі. Звідність чи незвідність многочлена є поняття відносне і залежить від поля P, над яким розглядається многочлен. Наприклад, многочлен $x^2 - 2$ незвідний у полі раціональних чисел Q, але звідний у полі R дійсних чисел, бо справджується рівність $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Многочлен $x^2 + 1$ незвідний у полях Q, R, але звідний у полі C комплексних чисел, бо $x^2 + 1 = (x + i)(x - i)$.

До многочленів нульового степеня поняття звідності і незвідності не застосовується. Вони відіграють у теорії подільності многочленів ту саму роль, що й числа ± 1 – у теорії подільності цілих чисел.

Теорема 1. Многочлен першого степеня над довільним полем P незвідний у цьому полі.

Д о в е д е н н я. Припустимо, що многочлен $f(x)$ першого степеня звідний. Тоді $f(x) = g(x)s(x)$, причому $\deg g \geq 1$ і $\deg s \geq 1$. Але $\deg f = \deg g + \deg s \geq 1 + 1$, тобто $\deg f \geq 2$, що суперечить умові.

Незвідні над полем P многочлени мають такі найпростіші ***властивості:***

1. Якщо $p(x)$ – многочлен, незвідний у даному полі, то і многочлен $cp(x)$, де c – довільна відмінна від нуля константа, незвідний у цьому полі.

2. Якщо $p(x)$ – незвідний у даному полі многочлен, а $f(x)$ – довільний многочлен над цим полем, то або $f(x) \vdots p(x)$, або ці многочлени взаємно прості.

3. Якщо незвідний у даному полі многочлен $p(x)$ ділиться на інший незвідний у цьому полі многочлен $q(x)$, то вони відрізняються тільки сталим множником.

Перші дві з цих властивостей випливають з властивостей простих елементів довільної області цілісності. Доведемо третю властивість. За умовою, $p(x)$ і $q(x)$ мають спільний дільник $q(x)$ ненульового степеня і тому не взаємно прості. Оскільки $p(x)$ – незвідний многочлен, то за властивістю 2, $q(x) \vdots p(x)$. Отже, многочлени $p(x)$ і $q(x)$ діляться один на одного і тому є асоційованими (тобто відрізняються лише множником нульового степеня).

Фундаментальну роль у теорії подільності цілих чисел відіграє основна теорема арифметики, тобто теорема про можливість і єдиність розкладу довільного цілого числа (відмінного від 0, ±1) у добуток простих множників. Аналогічне твердження справедливе і для многочленів.

Теорема 2. Кожний многочлен $f(x)$ ненульового степеня над полем P можна подати у вигляді

$$f(x) = p_1(x)\,p_2(x)\ldots p_l(x), \qquad (1)$$

де всі $p_k(x)$ є незвідними многочленами у полі P. Зображення (1) єдине з точністю до сталих множників і до порядку нумерації многочленів $p_k(x)$.

Зображення (1) називають **розкладом многочлена** $f(x)$ **на незвідні множники** (або у добуток незвідних множників) у полі P.

Д о в е д е н н я. Доведемо теорему методом математичної індукції. Покажемо спочатку можливість розкладу (1). Якщо $f(x)$ – незвідний многочлен, то теорема справджується. Припустимо, що теорема справджується для всіх многочленів степеня меншого, ніж

n і доведемо її істинність для многочлена степеня n. Якщо $f(x)$ – звідний над полем P, то $f(x) = f_1(x) f_2(x)$, де $\deg f_1 < n, \deg f_2 < n$. За припущенням індукції для многочленів f_1, f_2 зображення (1) можливе, тобто

$$f_1(x) = p_1(x) p_2(x) ... p_i(x),$$
$$f_2(x) = p_{i+1}(x) p_{i+2}(x) ... p_l(x),$$

звідки

$$f(x) = p_1(x) p_2(x) ... p_l(x).$$

Отже, розклад $f(x)$ у вигляді (1) завжди існує.

Доведемо його єдиність (теж методом математичної індукції). Нехай існує інший розклад

$$f(x) = q_1(x) q_2(x) ... q_s(x), \qquad (2)$$

де $q_j(x)$ – незвідні многочлени над полем P. Якщо $f(x)$ – незвідний многочлен, то єдиність має місце. Припустимо, що теорема правильна для всіх многочленів степеня меншого, ніж n, і доведемо її істинність для всіх многочленів степеня n. Оскільки для $f(x)$ справджуються рівності (1) і (2), то

$$p_1(x) p_2(x) ... p_l(x) = q_1(x) q_2(x) ... q_s(x). \qquad (3)$$

Ліва частина ділиться на $p_1(x)$, тому в правій частині існує многочлен $q_i(x)$, який ділиться на $p_1(x)$. Припустимо, що $q_1(x) \vdots p_1(x)$. Тоді за властивістю 3 незвідних многочленів $q_1(x) = c p_1(x)$. Поділимо обидві частини рівності (3) на $p_1(x)$, отримаємо:

$$p_2(x) ... p_l(x) = c q_2(x) .. q_s(x).$$

Позначимо $r(x) = p_2(x) ... p_l(x)$. Тоді $\deg r < n$, за припущенням індукції розклад $r(x)$ на незвідні множники єдиний, тобто $l = s, p_i = q_i \quad (i = 2, ..., l)$. Отже, розклад $f(x)$ єдиний. Теорему доведено.

Наслідок. Довільний многочлен ненульового степеня над полем P можна подати у вигляді

$$f(x) = [p_1(x)]^{k_1} [p_2(x)]^{k_2} ... [p_m(x)]^{k_m}, \qquad (4)$$

де $p_1(x), p_2(x),..., p_m(x)$ – попарно різні многочлени, незвідні у полі *P*. Це зображення єдине з точністю до сталих множників.

Зображення (4) називається **канонічним розкладом** $f(x)$ у полі *P*. Розклад (4) випливає з (1), якщо враховувати, що деякі з незвідних множників $p_i(x)$ можуть повторюватися.

Означення 3. Якщо многочлен $p_i(x)$ входить у канонічний розклад (4) у степені з показником k_i, то кажуть, що $p_i(x)$ є **множником кратності** k_i многочлена $f(x)$. Множники, кратність яких більша за одиницю, називаються **кратними множниками многочлена**.

Інакше кажучи, незвідний многочлен $p_i(x)$ є множником k_i-ї кратності многочлена $f(x)$, якщо $f(x) \vdots [p_i(x)]^{k_i}$, але не $f(x) \vdots [p_i(x)]^{k_i+1}$.

Приклад. Розкласти многочлен $f(x) = x^4 - 6x^2 + 9$ на незвідні множники у полі *Q* і полі *R*.

Розклади мають вигляд:

$f(x) = (x^2 - 3)^2$ – у полі *Q*,

$f(x) = (x - \sqrt{3})^2 (x + \sqrt{3})^2$ – у полі *R*. Обидва множники тут мають кратність 2.

До многочленів можна застосувати метод знаходження НСД, подібний до методу розкладання на прості множники в арифметиці.

Теорема 3. Якщо многочлени $f(x)$ і $g(x)$ розкладені на незвідні множники у довільному полі *P*, то їх найбільший спільний дільник (f, g) дорівнює добутку всіх незвідних многочленів, які входять у розклад як $f(x)$, так і $g(x)$. Якщо таких спільних незвідних множників немає, то многочлени $f(x)$ і $g(x)$ взаємно прості, тобто $(f, g)=1$.

Д о в е д е н н я. Припустимо спочатку, що розклади $f(x)$ і $g(x)$ мають спільні незвідні множники $d_1(x), d_2(x),..., d_r(x)$. Тоді

розклади $f(x)$ і $g(x)$ на незвідні множники можна записати у вигляді:

$$f(x) = d_1(x)d_2(x)...d_r(x)p_{r+1}(x)...p_l(x),$$
$$g(x) = d_1(x)d_2(x)...d_r(x)q_{r+1}(x)...q_m(x).$$

Многочлен $d(x) = d_1(x)d_2(x)...d_r(x)$ – спільний дільник многочленів $f(x)$ і $g(x)$. Він є і найбільшим спільним дільником. Справді, якщо $d'(x)$ – довільний спільний дільник $f(x)$ і $g(x)$, то його розклад на незвідні множники має вигляд:

$$d'(x) = d_{i1}(x)d_{i2}(x)...d_{is}(x),$$

де $d_{i1}(x),...,d_{is}(x)$ – якісь із многочленів $d_1(x),...,d_r(x)$. Отже, $d(x) \vdots d'(x)$ і тому є найбільшим спільним дільником.

Якщо спільних незвідних множників у розкладах $f(x)$ і $g(x)$ немає, то $(f,g)=1$. Справді, якщо б $(f,g) = d(x), \deg d \geq 1$, то на підставі теореми 2 многочлени $f(x)$ і $g(x)$ мали б хоч один незвідний спільний дільник, що суперечить умові. Теорему доведено.

Ця теорема поширюється на випадок більшого числа заданих многочленів.

Приклад. Знайдемо НСД многочленів

$$f(x) = x^3 + 6x^2 + 12x + 8, \;\; g(x) = x^3 + 3x^2 - 4.$$

Розкладемо ці многочлени на незвідні множники над полем *R*:

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

Тоді $(f,g) = (x+2)^2 = x^2 + 4x + 4.$

Питання для самоконтролю

1. Дайте означення звідного і незвідного многочленів у заданому полі.
2. Сформулюйте найпростіші властивості незвідних над заданим полем многочленів.
3. Сформулюйте і доведіть теорему про розклад многочлена на незвідні множники у заданому полі та наслідок з неї.

4. Як знайти НСД многочленів, використовуючи їхні розклади на незвідні множники?

Тема 5. Формальна похідна многочлена. Виділення кратних множників многочлена. Кратні корені многочлена

З курсу математичного аналізу відомо, що кожний многочлен n-го степеня з дійсними коефіцієнтами $f(x)$, який розглядається як функція на множині всіх дійсних чисел, має в кожній точці x похідну $f'(x)$, яка теж є многочленом, причому $(n-1)$-го степеня. Тобто довільний многочлен над полем дійсних чисел R має в кожній точці похідну. Якщо многочлен $f(x)$ розглядати над деяким абстрактним полем P, то означення похідної в цьому випадку буде формальним. Це означення ми дали при виведенні формули Тейлора, причому вважалося, що поле P, над яким задано многочлен, є поле характеристики нуль. Нагадаємо це означення.

Похідною від многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

називається многочлен

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 2a_2 x + a_1,$$

причому похідна многочлена нульового степеня і нуль-многочлена вважається рівною нулю.

Для похідних від многочленів над довільним полем виконуються такі рівності:

1. $\forall f(x), g(x) \in P[x]$ $\quad (f(x) + g(x))' = f'(x) + g'(x)$;
2. $\forall f(x), g(x) \in P[x]$ $\quad (f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$;
3. $\forall f(x) \in P[x], \forall c \in P$ $\quad (cf(x))' = cf'(x)$;
4. $\forall f(x) \in P[x], \forall k \in Z$ $\quad ([f(x)]^k)' = k[f(x)]^{k-1} f'(x)$.

Нехай $f(x)$ – деякий многочлен над полем P. Нагадаємо, що якщо незвідний множник $q(x)$ входить у канонічний розклад $f(x)$ у степені з показником k, то $q(x)$ називається множником

кратності k многочлена $f(x)$ (або по-іншому, якщо $f(x) \vdots [q(x)]^k$, але $f(x) \not\vdots [q(x)]^{k+1}$).

Теорема 1. Якщо незвідний у полі P характеристики 0 многочлен $q(x)$ є множником кратності $k \geq 2$ многочлена $f(x)$, то він є множником кратності $k-1$ для похідної $f'(x)$. Якщо $q(x)$ є множником першої кратності многочлена $f(x)$, то він не входить у розклад похідної $f'(x)$ на незвідні множники.

Д о в е д е н н я. За умовою теореми,

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

де $\varphi(x) \not\vdots q(x)$, тобто $(\varphi(x), q(x)) = 1$ (властивість 2 незвідних многочленів). Знайдемо похідну:

$$f'(x) = k[q(x)]^{k-1} q'(x)\varphi(x) + [q(x)]^k \varphi'(x) =$$
$$= [q(x)]^{k-1}\left(kq'(x)\varphi(x) + q(x)\varphi'(x)\right).$$

Позначимо через $s(x) = kq'(x)\varphi(x) + q(x)\varphi'(x)$. Щоб довести, що $q(x)$ є для $f'(x)$ множником кратності $k-1$, треба показати, що $s(x) \not\vdots q(x)$, а для цього досить показати, що $kq'(x)\varphi(x) \not\vdots q(x)$.

Оскільки $\deg q'(x) < \deg q(x)$, то $q'(x) \not\vdots q(x)$, тобто $(q'(x), q(x)) = 1$ (властивість 2 незвідних многочленів).

Таким чином, $(\varphi, q) = 1 \wedge (q', q) = 1$, то за властивістю 1 взаємно простих многочленів $(q'\varphi, q) = 1$. Тому $kq'(x)\varphi(x) \not\vdots q(x)$, що й треба було довести.

Доведемо другу частину теореми. Якщо кратність k множника $q(x)$ дорівнюватиме 1, то отримаємо:

$$f'(x) = q'(x)\varphi(x) + q(x)\varphi'(x).$$

Оскільки $q'(x)\varphi(x) \not\vdots q(x)$, то і $f'(x) \not\vdots q(x)$. Це означає, що $q(x)$ не входить в розклад $f'(x)$ на незвідні множники. Теорему доведено.

Наслідок. Для того, щоб многочлен $f(x)$ не мав кратних множників, необхідно і достатньо, щоб $f(x)$ був взаємно простим із своєю похідною $f'(x)$.

Д о в е д е н н я. Якщо всі незвідні множники многочлена $f(x)$ мають кратність 1, то в розкладі $f'(x)$ на незвідні множники не буде жодного множника, спільного з множниками многочлена $f(x)$. Тоді $(f, f')=1$. Якщо ж $f(x)$ має хоч один кратний множник $q(x)$, то $(f, f')\vdots q(x)$ і тому (f, f') не може бути константою.

Відомо, що всякий многочлен над полем P можна єдиним способом подати у вигляді добутку многочленів нижчих степенів, незвідних у цьому полі:

$$f(x)=[p_1(x)]^{k_1}[p_2(x)]^{k_2}...[p_l(x)]^{k_l}. \qquad (1)$$

Позначимо через $\varphi_1(x)$ добуток усіх незвідних множників першої кратності в розкладі (1) многочлена $f(x)$, через $\varphi_2(x)$ – добуток усіх незвідних множників другої кратності і т. д. Тоді розклад (1) можна записати в такому вигляді:

$$f(x)=\varphi_1(x)[\varphi_2(x)]^2[\varphi_3(x)]^3...[\varphi_m(x)]^m,$$

або скорочено

$$f=\varphi_1\varphi_2^2\varphi_3^3...\varphi_m^m. \qquad (2)$$

Якщо многочлен не має множників кратності $k<m$, то вважають, що $\varphi_k=1$.

Наприклад, нехай розклад многочлена $f(x)$ на незвідні множники в полі *R* має вигляд:

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

Тоді
$$\varphi_1(x)=(x^2+1)(x-1),$$
$$\varphi_2(x)=x+1,$$
$$\varphi_3(x)=x-2,$$
$$\varphi_4(x)=1,$$
$$\varphi_5(x)=x.$$

Подання многочлена у вигляді (2) називається **відокремленням кратних множників.**

Покажемо, що многочлени $\varphi_1, \varphi_2, ..., \varphi_m$ можна визначити, знаючи лише коефіцієнти многочлена $f(x)$.

Оскільки φ_1 є добутком незвідних множників многочлена f кратності $k=1$, то в f' жодний з цих множників (за теоремою 1) входити не буде. φ_2 є добутком незвідних множників кратності $k=2$, то в f' ці множники входять з кратністю одиниця. Аналогічно, якщо f має множником φ_k^k, то f' матиме множник φ_k^{k-1}. Отже,

$$f' = \varphi_2\varphi_3^2 ... \varphi_m^{m-1}\psi_1,$$

де ψ_1 не ділиться на $\varphi_1, \varphi_2, ..., \varphi_m$. Тоді за теоремою 3 теми 4

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

Знайдемо тепер

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

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

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

Аналогічно:

$$d_3 = (d_2, d_2') = \varphi_4\varphi_5^4 ... \varphi_m^{m-3}$$

$$- - - - - - - - - - - - - - - -$$

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

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

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

Знайдемо тепер кожний із множників φ_i. Для цього поділимо f на d_1:

$$q_1 = \frac{f}{d_1} = \varphi_1\varphi_2 ... \varphi_m.$$

Аналогічно

$$q_2 = \frac{d_1}{d_2} = \varphi_2\varphi_3 ... \varphi_m$$

$$q_3 = \frac{d_2}{d_3} = \varphi_3\varphi_4 ... \varphi_m$$

$$- - - - - - - - - - - - \qquad (3)$$

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

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

Тепер з формули (3) отримаємо шукані множники φ_i:

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

Отже, ми приходимо до *висновку:*

У довільного многочлена над полем P можна відокремити кратні множники за допомогою скінченного числа раціональних дій над деякими многочленами.

Схему знаходження многочленів φ_i можна подати у вигляді таблиці:

f	$\} q_1 = \frac{f}{d_1}$	$\} \varphi_1 = \frac{q_1}{q_2}$
$d_1 = (f, f')$	$\} q_2 = \frac{d_1}{d_2}$	$\} \varphi_2 = \frac{q_2}{q_3}$
$d_2 = (d_1, d_1')$	$\} q_3 = \frac{d_2}{d_3}$	
– – – – – – – –	- - - - - - - - - - - - - - - -	- - - - - - - - - - - - -
$d_{m-1} = (d_{m-2}, d_{m-2}')$	$\} q_m = \frac{d_{m-1}}{d_m}$	$\varphi_m = q_m$
$d_m = 1$		

Відокремлення кратних множників значно спрощує знаходження коренів многочленів.

Нагадаємо, що елемент α поля P називається **коренем многочлена** $f(x)$ з кільця $P[x]$, якщо $f(\alpha) = 0$.

Елемент $\alpha \in P$ є коренем многочлена $f(x) \in P[x]$ тоді і тільки тоді, коли лінійний двочлен $x - \alpha$ є дільником многочлена $f(x)$.

Цю теорему можна прийняти за нове означення кореня многочлена, яке рівносильне вже дійсному, а саме: елемент α поля P називається **коренем многочлена** $f(x)$ з кільця $P[x]$, якщо $f(x)$ ділиться на $x - \alpha$.

Означення 1. Елемент $\alpha \in P$ називається ***k*-кратним коренем** (або коренем k-ї кратності) многочлена $f(x) \in P[x]$, якщо $f(x)$ ділиться на $(x-\alpha)^k$, але не ділиться на $(x-\alpha)^{k+1}$.

Корені кратності 1 називаються **простими**; корені, кратність яких більша за 1, – кратними, причому двократні та трикратні корені іноді називаються також подвійними та потрійними відповідно.

Теорема 2. Для того, щоб елемент α був коренем кратності k многочлена $f(x)$, необхідно і достатньо, щоб

$$f(\alpha)=f'(\alpha)=...=f^{(k-1)}(\alpha)=0 \quad \text{і} \quad f^{(k)}(\alpha)\neq 0 \qquad (4)$$

Д о в е д е н н я. *Необхідність.* Нехай α – корінь $f(x)$ кратності k. Це означає, що $x-\alpha$ є незвідним множником k-ї кратності многочлена $f(x)$. Тоді за теоремою 1, $x-\alpha$ є незвідним множником похідної $f'(x)$ кратності $k-1$, тобто α є коренем $(k-1)$-ї кратності многочлена $f'(x)$. Аналогічно, α є коренем $(k-2)$-ї кратності многочлена $f''(x)$, і так далі, $f^{(k-1)}(x)$ має $x-\alpha$ своїм множником кратності 1, а $f^{(k)}(x)$ цього множника не має зовсім, і тому, за теоремою 3 теми 1, $f^{(k)}(\alpha)\neq 0$.

Достатність. Нехай виконується умова (4). Тоді α є коренем $f(x)$. Позначимо кратність цього кореня через l і покажемо, що $l=k$. З доведеного випливає, що

$$f(\alpha)=f'(\alpha)=...=f^{(l-1)}(\alpha)=0,\ f^{(l)}(\alpha)\neq 0. \qquad (5)$$

Якби було $l<k$, то з (4) випливало б, що $f^{(l)}(\alpha)=0$, а це суперечить (5). Аналогічно відкидаємо припущення $l>k$. Отже, $l=k$. Теорему доведено.

Приклад. Безпосередньою перевіркою переконуємось, що многочлен $f(x)=x^3-x^2-8x+12$ має в полі R корінь $\alpha=2$. Визначимо його кратність.

$$f'(x)=3x^2-2x-8; \qquad f'(2)=0;$$
$$f''(x)=6x-2; \qquad f''(2)=10\neq 0,$$

тому $x=2$ є коренем кратності 2.

Теорема 3 (Вієта). Якщо $\alpha_1,\alpha_2,...,\alpha_n$ – корені зведеного многочлена $f(x)=x^n+a_{n-1}x^{n-1}+...+a_1x+a_0\in P[x]$ (тобто $a_n=1$), то справедливі формули:

$$\alpha_1+\alpha_2+\ldots+\alpha_n=-a_{n-1}$$
$$\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_1\alpha_n+\alpha_2\alpha_3+\ldots+\alpha_{n-1}\alpha_n=a_{n-2},$$
$$\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\ldots+\alpha_{n-2}\alpha_{n-1}\alpha_n=-a_{n-3}, \qquad (6)$$
$$\text{- -}$$
$$\alpha_1\alpha_2\ldots\alpha_n=(-1)^n a_0.$$

Д о в е д е н н я. Розглянемо випадок $n=2$: $f(x)=x^2+px+q$. Якщо α_1,α_2- корені, то $x^2+px+q=(x-\alpha_1)(x-\alpha_2)=x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2$. Звідси

$$\alpha_1+\alpha_2=-p,$$
$$\alpha_1\alpha_2=q.$$

Розглянемо $n=3$:

$f(x)=x^3+a_2x^2+a_1x+a_0=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)=$

$=(x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2)(x-\alpha_3)=x^3-(\alpha_1+\alpha_2)x^2+\alpha_1\alpha_2x-\alpha_3x^2+\alpha_3(\alpha_1+\alpha_2)x-$

$-\alpha_1\alpha_2\alpha_3=x^3-(\alpha_1+\alpha_2+\alpha_3)x^2+(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)x-\alpha_1\alpha_2\alpha_3.$

Прирівняємо коефіцієнти при однакових степенях:

$$\alpha_1+\alpha_2+\alpha_3=-a_2,$$
$$\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=a_1,$$
$$\alpha_1\alpha_2\alpha_3=-a_0.$$

Аналогічно, $f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$.

Розкриваючи дужки в правій частині останньої рівності і зводячи подібні члени, прирівнюємо відповідні коефіцієнти і отримаємо формули (6).

Теорема 3′. Якщо в многочлені $f(x)$ $a_n\neq1$, то формули Вієта мають вигляд:

$$\alpha_1+\alpha_2+\ldots+\alpha_n=-\frac{a_{n-1}}{a_n},$$
$$\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_1\alpha_n+\alpha_2\alpha_3+\ldots+\alpha_{n-1}\alpha_n=\frac{a_{n-2}}{a_n},$$
$$\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\ldots+\alpha_{n-2}\alpha_{n-1}\alpha_n=-\frac{a_{n-3}}{a_n},$$
$$\text{- -}$$
$$\alpha_1\alpha_2\ldots\alpha_n=(-1)^n\frac{a_0}{a_n}.$$

Приклад. Записати формули Вієта для многочлена

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

Якщо $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ – корені, тоді

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -\frac{0}{2} = 0,$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_3\alpha_4 = \frac{-3}{2} = -\frac{3}{2},$$

$$\alpha_1\alpha_2\alpha_3 + \ldots + \alpha_2\alpha_3\alpha_4 = -\frac{5}{2},$$

$$\alpha_1\alpha_2\alpha_3\alpha_4 = \frac{-2}{2} = -1.$$

Питання для самоконтролю

1. Дайте означення похідної від многочлена *n*-го степеня.
2. Сформулюйте необхідну і достатню умову того, щоб многочлен не мав кратних множників.
3. Опишіть алгоритм відокремлення кратних множників многочлена.
4. Дайте означення *k*-кратного кореня многочлена. Які корені називаються простими?
5. Сформулюйте і доведіть критерій кратного кореня.
6. Запишіть формули Вієта для многочлена *n*-го степеня.

Розділ ІІ. МНОГОЧЛЕНИ ВІД КІЛЬКОХ ЗМІННИХ

Тема 6. Кільце многочленів від *n* змінних над областю цілісності

Означення 1. Кільцем многочленів $R[x_1, x_2, \cdots, x_{n-1}, x_n]$ від n змінних $x_1, x_2, \cdots, x_{n-1}, x_n$ над областю цілісності R називається кільце многочленів від змінної x_n над кільцем $R[x_1, x_2, \cdots, x_{n-1}]$, тобто

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

Це означення має індуктивний характер. При $n=1$ воно зводиться до означення кільця многочленів від однієї змінної x_1 над областю цілісності R.

Теорема 1. Кільце многочленів $R[x_1, x_2, \cdots, x_{n-1}, x_n]$ над областю цілісності R є областю цілісності.

Д о в е д е н н я. Доводимо методом математичної індукції. При $n=1$ твердження правильне.

Припускаємо, що твердження правильне при $n=k$. Розглядаємо кільце $R[x_1, x_2, \cdots, x_k, x_{k+1}]$. За означенням 1, $R[x_1, x_2, \cdots, x_k, x_{k+1}]$ є кільце многочленів над $R_k \overset{df}{=} R[x_1, x_2, \cdots, x_k]$. За припущенням індукції, R_k є областю цілісності. Тоді і $R_k[x_{k+1}] = R[x_1, x_2, \cdots, x_k, x_{k+1}]$ є областю цілісності.

Отже, за принципом математичної індукції, $R[x_1, x_2, \cdots, x_n]$ є областю цілісності для $\forall n \in N$. Теорему доведено.

Теорема 2. Кожний елемент $f \in R[x_1, x_2, \cdots, x_n]$ можна подати у вигляді скінченної суми

$$f = \sum_{i=1}^{N} A_i \, x_1^{k_{1i}} \, x_2^{k_{2i}} \cdots x_n^{k_{ni}}, \qquad (1)$$

де $A_i \in R$, $k_{ji} \in Z_+$, $i = 1,...,N$, $j = 1,...,n$, і навпаки, будь-який вираз вигляду (1) є елементом кільця $R[x_1, x_2, \cdots, x_n]$.

Д о в е д е н н я. Доведення проводимо методом математичної індукції за змінною n.

При $n=1$ твердження правильне. Припустимо, що воно правильне при $n=m$ і перевіримо його правильність при $n=m+1$. За означенням 1, кожний елемент $f \in R\left[x_1, \cdots, x_m, x_{m+1}\right]$ є многочлен від x_{m+1} над областю цілісності $R\left[x_1, \cdots, x_m\right]$ і тому його можна подати у вигляді суми

$$f=\sum_{j=0}^{l} a_j\left(x_1, \cdots, x_m\right) x_{m+1}^j, \quad a_j\left(x_1, \cdots, x_m\right) \in R\left[x_1, \cdots, x_m\right], \quad j=0,...,l \qquad (2)$$

За припущенням індукції, кожний многочлен $a_j\left(x_1, \cdots, x_m\right)$ від m змінних можна подати у вигляді скінченної суми

$$a_j\left(x_1, \cdots, x_m\right)=\sum_{i=1}^{N_j} A_i^{(j)}\, x_1^{k_{1i}^{(j)}}\, x_2^{k_{2i}^{(j)}} \cdots x_m^{k_{mi}^{(j)}}, \quad A_i^{(j)} \in R, \qquad (3)$$

$$k_{si}^{(j)} \in \mathrm{Z}_+, i=1,...,N_j, \quad s=1,...,m, \quad j=0,...,l.$$

Підставивши (3) в (2), дістанемо суму вигляду

$$f=\sum_{r=1}^{N} B_r\, x_1^{k_{1r}}\, x_2^{k_{2r}} \cdots x_m^{k_{mr}}\, x_{m+1}^{k_{m+1,r}}, \quad B_r \in R, r=1,...,N. \qquad (4)$$

Навпаки, кожна сума вигляду (4) є елемент кільця $R\left[x_1, x_2, \cdots, x_{m+1}\right]$.

Отже, твердження теореми правильне і при $n=m+1$. Теорему доведено.

Означення 2. Елементи кільця $R\left[x_1, \cdots, x_n\right]$ називають **многочленами від** n **змінних над** R і позначають $f\left(x_1, x_2, \cdots, x_n\right)$, $g\left(x_1, x_2, \cdots, x_n\right)$ і т. д.

Кожен доданок $A_i\, x_1^{k_{1i}} \cdots x_n^{k_{ni}}$ в сумі (1) називають **членом многочлена** $f\left(x_1, \cdots, x_n\right)$, елемент $A_i \in R$ – **коефіцієнтом** цього члена. Два члени, які відрізняються лише коефіцієнтами, називаються **подібними.**

При додаванні двох (або більше) подібних членів дістаємо один член, подібний до кожного з даних:

$$A\, x_1^{k_1}\, x_2^{k_2} \cdots x_n^{k_n}+B\, x_1^{k_1}\, x_2^{k_2} \cdots x_n^{k_n}=\left(A+B\right) x_1^{k_1}\, x_2^{k_2} \cdots x_n^{k_n}\ .$$

Таку заміну кількох подібних членів одним називають **зведенням подібних членів**. Множення членів многочлена здійснюють за правилом

$$\left(A\, x_1^{k_1}\, x_2^{k_2} \cdots x_n^{k_n}\right) \cdot \left(B\, x_1^{l_1}\, x_2^{l_2} \cdots x_n^{l_n}\right) = AB\, x_1^{k_1+l_1}\, x_2^{k_2+l_2} \cdots x_n^{k_n+l_n} .$$

Надалі вважатимемо, що в сумі (1) подібних членів немає. Така форма запису многочлена називається **канонічною** або **нормальною**.

Теорема 3. Будь-який многочлен $f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$ можна подати в канонічній формі лише одним способом (з точністю до порядку членів).

Д о в е д е н н я. Нехай многочлени $f(x_1, \cdots, x_n)$ і $g(x_1, \cdots, x_n)$ подано в канонічній формі і

$$f(x_1, \cdots, x_n) = g(x_1, \cdots, x_n);$$

тоді $f(x_1, \cdots, x_n) - g(x_1, \cdots, x_n) = 0$. Це означає, що всі коефіцієнти многочлена $f - g$ дорівнюють нулю. Оскільки подібних членів у записі кожного з цих многочленів немає, а нуль може утворитись лише при відніманні подібних членів з однаковими коефіцієнтами, то кожний член многочлена f є членом многочлена g, і навпаки, тобто $f = g$. Теорему доведено.

Означення 3. **Степенем члена** $A\, x_1^{k_1}\, x_2^{k_2} \cdots x_n^{k_n}$ многочлена називають суму $k_1 + k_2 + \cdots + k_n$. Число k_i, $i = 1,...,n$, називають **степенем даного члена відносно** x_i. Найбільший із степенів членів називають **степенем многочлена**, а член з найбільшим степенем називають **старшим членом многочлена**.

Многочлен може мати декілька різних старших членів, наприклад:

$$f(x_1, x_2, x_3) = 2x_1\, x_2^3\, x_3^2 + x_1^4\, x_2\, x_3 - 2\, x_1^3 + 4.$$

Тут старшими членами є $2x_1\, x_2^3\, x_3^2$ і $x_1^4\, x_2\, x_3$.

Якщо всі члени многочлена мають той самий степінь l, то многочлен називається **однорідним многочленом** або **формою степеня** l. Будь-який многочлен можна подати як суму скінченного числа однорідних многочленів різних степенів.

У кільці $R[x_1, \cdots, x_n]$ (як і в кільці $R[x]$), степінь суми двох многочленів не перевищує степінь кожного з них, а степінь добутку

двох відмінних від нуля многочленів дорівнює сумі степенів цих многочленів, тобто

$$\deg(f+g) \le \max\{\deg f, \deg g\},$$

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

У кільці $R[x_1, \cdots, x_n]$ дільниками одиниці можуть бути лише відмінні від нуля константи.

Як було показано, многочлен може мати декілька старших членів. У якому порядку їх розмістити? Члени многочлена від однієї змінної ми розміщували за спадними степенями змінної. Для многочленів від багатьох змінних використовується **лексикографічний** принцип упорядкування членів многочлена. Цей термін походить від грецького слова «лексикон», що означає словник, і цей принцип упорядкування членів многочлена аналогічний принципу упорядкування слів у словнику, тобто за алфавітом. А саме: з усіх членів многочлена вибирають спочатку той, в якому x_1 є в найвищому степені і записують його першим. Якщо є кілька членів, в яких x_1 входить в цьому найвищому степені, то вибирають той член, в якому x_2 є в найвищому степені і т. д. Наприклад, члени многочлена

$$f(x_1, x_2, x_3, x_4) = x_1^4 + 3x_1^2\, x_2^3\, x_3 - x_1^2\, x_2^3\, x_4^2 + 5\, x_1\, x_3\, x_4^2 + 2x_2 + x_3^3 x_4 - 4 \quad (5)$$

розміщені в лексикографічному порядку.

Якщо $A\, x_1^{k_1}\, x_2^{k_2} \cdots x_n^{k_n}$ і $B\, x_1^{l_1}\, x_2^{l_2} \cdots x_n^{l_n}$ – два члени многочлена $f(x_1, \cdots, x_n)$, то перший член вважають **вищим** від другого, якщо $k_1 = l_1,\ k_2 = l_2, \cdots, k_{i-1} = l_{i-1}$ і $k_i > l_i$.

В окремих випадках використовують упорядкування членів многочлена за спадними степенями однієї із змінних, наприклад, многочлен (5) можна записати за спадними степенями змінної x_4 наступним чином:

$$f(x_1, x_2, x_3, x_4) = \left(-x_1^2\, x_2^3 + 5x_1\, x_3\right) x_4^2 + x_3^3\, x_4 + \left(x_1^4 + 3x_1^2\, x_2^3\, x_3 + 2x_2 - 4\right)$$

Перший по порядку член многочлена при лексикографічному розміщенні називається **вищим членом** многочлена.

Лема. Вищий член добутку двох многочленів дорівнює добутку вищих членів цих многочленів.

Д о в е д е н н я. Нехай перемножуємо многочлени $f\,(x_1,\ \cdots,\ x_n)$ і $g\,(x_1,\ \cdots,\ x_n)$. Якщо

$$A\,x_1^{k_1}\ x_2^{k_2}\cdots x_n^{k_n} \tag{6}$$

– вищий член многочлена $f\,(x_1,\cdots,x_n)$, а

$$A'\,x_1^{s_1}\ x_2^{s_2}\cdots x_n^{s_n} \tag{7}$$

– будь-який інший член цього многочлена, то існує таке $i,\ \ 1\le i\le n$, що

$$k_1=s_1,\cdots,\ k_{i-1}=s_{i-1},\quad k_i>s_i.$$

Якщо, з іншого боку,

$$B\,x_1^{l_1}\ x_2^{l_2}\cdots x_n^{l_n}, \tag{8}$$

$$B'\,x_1^{t_1}\ x_2^{t_2}\cdots x_n^{t_n} \tag{9}$$

– вищий і довільний інший члени многочлена $g\,(x_1,\cdots,x_n)$, то $\exists\ j,\ \ 1\le j\le n$, що

$$l_1=t_1,\cdots,\ l_{j-1}=t_{j-1},\quad l_j>t_j\ .$$

Перемножуючи (6) і (8) , а також (7) і (9), отримуємо:

$$AB x_1^{k_1+l_1}\ x_2^{k_2+l_2}\cdots x_n^{k_n+l_n}\ , \tag{10}$$

$$A'B' x_1^{s_1+t_1}\ x_2^{s_2+t_2}\cdots x_n^{s_n+t_n}\ . \tag{11}$$

Очевидно, член (10) вищий за член (11); якщо, наприклад $i\le j$, то $k_1+l_1=s_1+t_1,\cdots,k_{i-1}+l_{i-1}=s_{i-1}+t_{i-1},$ але $k_i+l_i>s_i+t_i,$ бо $k_i>s_i,\quad l_i\ge t_i$. Аналогічно перевіряється, що член (10) буде вищим від добутку членів (6) і (9), а також (7) і (8). Таким чином, член (10) буде вищим всіх інших в добутку $f\cdot g$, тобто буде вищим членом многочлена $f\cdot g$.

Лему доведено.

Зауважимо, що означення подільності многочленів, дільника, загальні властивості відношення подільності, поняття та властивості звідних і незвідних многочленів у кільці $P\left[x_1,\ \cdots,x_n\right]$ залишаються тими самими, що й у кільці многочленів від однієї

змінної $P[x]$. При цьому, як і у випадку многочлена від однієї змінної, вважатимемо, що основна область цілісності R є поле. При цьому треба зазначити, що кільце $P[x_1, \cdots, x_n]$ при $n \geq 2$ не є кільцем головних ідеалів і тому не може бути й евклідовим кільцем. Проте один з основних результатів теорії подільності в кільці $P[x]$, а саме – можливість і єдиність розкладу многочленів у добуток незвідних множників – залишається в силі і в кільці $P[x_1, \cdots, x_n]$ при $n \geq 2$. Тобто будь-який многочлен $f(x_1, \cdots, x_n)$ над полем P ненульового степеня можна подати у вигляді добутку многочленів, незвідних у полі P і при тому єдиним способом з точністю до сталих множників і порядку множників.

Питання для самоконтролю

1. Дайте означення кільця многочленів від *n* змінних.
2. Яка форма запису многочлена від *n* змінних називається канонічною або нормальною?
3. Дайте означення степеня многочлена від *n* змінних, старшого члена многочлена.
4. Який многочлен називається однорідним або формою степеня *l*?
5. У чому полягає лексикографічний принцип упорядкування членів многочлена?
6. Дайте означення вищого члена многочлена від *n* змінних.
7. Як знайти вищий член добутку двох многочленів?

Тема 7. Симетричні многочлени

Означення. Многочлен $f(x_1, x_2, \cdots, x_n)$ називається **симетричним** відносно змінних $x_1, x_2, \cdots, x_n$, якщо внаслідок довільної перестановки змінних $x_1, x_2, \cdots, x_n$ утворюється многочлен, який дорівнює даному.

Приклад. Многочлен $f_1(x_1, x_2) = x_1^2 + x_2^2$ симетричний відносно x_1, x_2, многочлен $f_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3$ не симетричний відносно x_1, x_2, x_3.

З прикладами симетричних многочленів ми вже зустрічались у формулах Вієта. Нехай $x_1, x_2, \cdots, x_n$ – корені многочлена

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Тоді, за формулами Вієта:

$$\sigma_1(x) \overset{df}{=} x_1 + x_2 + \cdots + x_n = -a_{n-1},$$

$$\sigma_2(x) \overset{df}{=} x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n = a_{n-2},$$

$$\sigma_n(x) \overset{df}{=} x_1 x_2 \cdots x_n = (-1)^n a_0.$$

Якщо під $x_1, x_2, \cdots, x_n$ розуміти незалежні змінні, то $\sigma_1, \sigma_2, \cdots, \sigma_n$ є многочлени, симетричні відносно цих змінних. Многочлени $\sigma_1, \sigma_2, \cdots, \sigma_n$ називаються **основними симетричними функціями.**

Встановимо деякі ***властивості симетричних многочленів***.

1. Сума, різниця і добуток симетричних многочленів над деяким полем P є знову симетричними многочленами над цим полем.

Наслідок. Множина всіх симетричних многочленів над полем P утворює область цілісності з одиницею відносно дій додавання і віднімання.

2. Якщо симетричний многочлен $f(x_1, x_2, \cdots, x_n)$ містить деякий член

$$M\, x_1^{l_1} x_2^{l_2} \cdots x_i^{l_i} \cdots x_j^{l_j} \ldots x_n^{l_n}, \qquad (1)$$

то він містить і член, утворений із заданого внаслідок будь-якої перестановки показників $l_1, l_2, \cdots, l_n$.

Д о в е д е н н я. Відомо, що від довільної перестановки $l_1, l_2, \cdots, l_n$ до іншої перестановки можна перейти за допомогою скінченного числа транспозицій. Тому досить показати, що при

транспозиції довільних двох показників у члені (1) ми знову дістаємо деякий член симетричного многочлена $f(x_1, x_2, \cdots, x_n)$. Виконаємо, наприклад, транспозицію показників l_i та l_j, отримаємо член:

$$M\ x_1^{l_1}\ x_2^{l_2} \cdots x_i^{l_j} \cdots x_j^{l_i} \ldots x_n^{l_n}. \qquad (2)$$

За означенням симетричного многочлена

$$f(x_1, x_2, \cdots, x_i, \cdots, x_j, \cdots, x_n) = f(x_1, x_2, \cdots, x_j, \cdots, x_i, \cdots, x_n).$$

Другий з цих многочленів повинен містити член (2), бо його дістаємо з члена (1) заміною x_i на x_j і навпаки. Внаслідок єдиності канонічної форми і заданий многочлен повинен містити член (2).

Наслідок. Якщо

$$A\ x_1^{l_1}\ x_2^{l_2} \cdots x_i^{l_i}\ x_{i+1}^{l_{i+1}} \cdots x_n^{l_n} \qquad (3)$$

є вищий член симетричного многочлена, то $l_1 \geq l_2 \geq l_3 \geq \cdots \geq l_n$.

Д о в е д е н н я. Припустимо, що при деякому $l_i < l_{i+1}$. За властивістю (2), даний многочлен разом з (3) містить і член

$$A\ x_1^{l_1}\ x_2^{l_2} \cdots x_i^{l_{i+1}}\ x_{i+1}^{l_i} \cdots x_n^{l_n}. \qquad (4)$$

Але з умови $l_{i+1} > l_i$ випливає, що член (4) вищий за член (3), що суперечить умові.

Теорема (основна теорема теорії симетричних многочленів).

Всякий симетричний многочлен $f(x_1, x_2, \cdots, x_n)$ від n змінних над полем P можна подати у вигляді многочлена від основних симетричних функцій $\sigma_1, \sigma_2, \cdots, \sigma_n$ цих змінних, коефіцієнти якого належать тому самому полю P.

Д о в е д е н н я. Зробимо спочатку такі зауваження.

1. Усіх членів певного степеня l, утворених із змінних $x_1, x_2, \cdots, x_n$, може бути лише скінченне число.

Наприклад, при $l=5$, $n=2$ маємо 6 членів:

$$x_1^5 x_2^0,\ x_1^4 x_2^1,\ x_1^3 x_2^2,\ x_1^2 x_2^3,\ x_1^1 x_2^4,\ x_1^0 x_2^5.$$

2. Теорему досить довести для однорідних симетричних многочленів, бо всякий симетричний многочлен можна подати як суму однорідних симетричних многочленів.

Наприклад, многочлен

$$f(x_1,\ x_2,\ x_3)=x_1^2+x_2^2+x_3^2+\ x_1\,x_2+x_1x_3+x_2x_3+x_1+x_2+x_3$$

можна подати як суму однорідних симетричних многочленів

$$f_1(x_1,\ x_2,\ x_3)=x_1^2+x_2^2+x_3^2+\ x_1\,x_2+x_1x_3+x_2x_3\ ,\quad f_2(x_1,\ x_2,\ x_3)=\ x_1+x_2+x_3.$$

3. Вищий член $x_1^{l_1}\ x_2^{l_2}\cdots x_n^{l_n}$ будь-якого симетричного многочлена можна подати як вищий член деякого добутку основних симетричних функцій $\sigma_1,\sigma_2,\cdots,\sigma_n$. Покажемо це.

Розглянемо добуток

$$\sigma_1^{l_1-l_2}\ \sigma_2^{l_2-l_3}\cdots\ \sigma_{n-1}^{l_{n-1}-l_n}\ \sigma_n^{l_n}\ . \tag{5}$$

За наслідком із властивості 2 $l_1\ge l_2\ge l_3\ge\cdots\ge l_n$, тому $l_1-l_2\ge 0$, $l_2-l_3\ge 0,\cdots,\ l_{n-1}-l_n\ge 0$, тому (5) є многочленом від $x_1,\ x_2,\cdots,\ x_n$. За доведеною лемою у темі 6 (вищий член добутку двох многочленів дорівнює добутку вищих членів цих многочленів), вищий член цього многочлена дорівнює добутку вищих членів многочленів $\sigma_1,\sigma_2,\cdots,\sigma_n$. Оскільки вищі члени многочленів $\sigma_1,\sigma_2,\cdots,\sigma_{n-1},\sigma_n$ дорівнюють відповідно $x_1;\ x_1x_2;\cdots;\ x_1\ x_2\cdots x_{n-1};\ x_1x_2\cdots\ x_{n-1}x_n$, то вищий член добутку (5) дорівнює

$$(x_1)^{l_1-l_2}\ (x_1\ x_2)^{l_2-l_3}\cdots(x_1\ x_2\cdots x_{n-1})^{l_{n-1}-l_n}\ (x_1\ x_2\cdots x_{n-1}\ x_n)^{l_n}\ =\ x_1^{l_1}\ x_2^{l_2}\cdots x_n^{l_n}.$$

Перейдемо тепер до доведення теореми.

Нехай вищий член симетричного многочлена $f(x_1,\ x_2,\cdots,\ x_n)$, який у результаті зауваження 2 можна вважати однорідним многочленом степеня N, дорівнює

$$A\ x_1^{l_1}\ x_2^{l_2}\cdots x_n^{l_n}\ . \tag{6}$$

Побудуємо симетричний многочлен

$$g(x_1\ x_2\cdots x_n)\overset{df}{=}A\sigma_1^{l_1-l_2}\ \sigma_2^{l_2-l_3}\cdots\sigma_{n-1}^{l_{n-1}-l_n}\ \sigma_n^{l_n}\ .$$

Згідно із зауваженням 3, вищий член цього многочлена дорівнює (6). Крім того, він однорідний, бо однорідними є многочлени $\sigma_1,\sigma_2,\cdots,\sigma_n$, а тому і їхній добуток. Оскільки в f і g однакові вищі члени, то $\deg f=\deg g$.

Візьмемо

$$f_1(x_1,x_2,\cdots,x_n)\overset{df}{=}f(x_1,x_2,\cdots,x_n)-g(x_1,x_2,\cdots,x_n)\ .$$

Очевидно, що $f_1(x_1, x_2, \cdots, x_n)$ – також однорідний симетричний многочлен степеня N. Але $f_1(x_1, x_2, \cdots, x_n)$ вже не містить деяких членів степеня N. Справді, він не містить вищого члена (6), який у цій різниці знищується. Крім того, в цій різниці знищуються всі $n!$ членів, які дістаємо з вищого члена перестановкою показників $l_1, l_2, \cdots, l_n$, бо ці члени, за властивістю 2, входять в обидва симетричні многочлени.

Отже, $f_1(x_1, x_2, \cdots, x_n)$ може містити лише члени, нижчі за (6). Застосуємо до цього многочлена той самий метод. Нехай вищий член многочлена $f_1(x_1, x_2, \cdots, x_n)$ має вигляд

$$B\, x_1^{m_1}\, x_2^{m_2} \cdots x_n^{m_n}. \qquad (7)$$

Побудуємо симетричний многочлен

$$g_1(x_1, x_2, \cdots, x_n) \overset{df}{=} B\sigma_1^{m_1-m_2}\, \sigma_2^{m_2-m_3} \cdots \sigma_{n-1}^{m_{n-1}-m_n}\, \sigma_n^{m_n}$$

і утворимо різницю

$$f_2(x_1, x_2, \cdots, x_n) = f_1(x_1, x_2, \cdots, x_n) - g_1(x_1, x_2, \cdots, x_n).$$

Очевидно, $f_2(x_1, x_2, \cdots, x_n)$ є симетричний і однорідний многочлен степеня N, який не містить ні члена (6), ні члена (7), а тільки члени, нижчі за них. Оскільки різних членів степеня N може бути лише скінченне число (зауваження 1), то, продовжуючи цей процес, на якомусь кроці дістанемо, що різниця

$$f_{k+1}(x_1, x_2, \cdots, x_n) = f_k(x_1, x_2, \cdots, x_n) - g_k(x_1, x_2, \cdots, x_n)$$

не може містити жодного члена степеня N, тобто дорівнює 0.

Тоді з рівностей

$$\begin{gathered} f_1 = f - g\ , \\ f_2 = f_1 - g_1\ , \\ \text{–––––––} \\ f_k = f_{k-1} - g_{k-1}\ , \\ 0 = f_k - g_k \end{gathered}$$

випливає, що $f = g + g_1 + \cdots + g_{k-1} + g_k$. А оскільки всі g_i виражені через добутки $\sigma_1, \sigma_2, \cdots, \sigma_n$, то многочлен $f(x_1, x_2, \cdots, x_n)$ подано як многочлен від основних симетричних функцій

$$f\ (x_1, x_2, \cdots, x_n) = \varphi(\sigma_1, \sigma_2, \cdots, \sigma_n),$$

коефіцієнти якого (як видно з правила побудови g_i) знайдено з коефіцієнтів многочлена f за допомогою операцій додавання, віднімання, і тому належать полю P. Теорему доведено.

Приклад.

$$x_1^2 + x_2^2 + \cdots + x_n^2 = (x_1 + x_2 + \cdots + x_n)^2 - 2(x_1 x_2 + \cdots + x_{n-1} x_n) = \sigma_1^2 - 2\sigma_2.$$

Справедлива також теорема про єдиність многочлена $\varphi\ (\sigma_1, \sigma_2, \cdots, \sigma_n)$:

Теорема. Зображення симетричного многочлена у вигляді многочлена від основних симетричних функцій єдине.

Доведення цієї теореми тут не наводимо.

З основної теореми теорії симетричних многочленів випливає важливий наслідок.

Наслідок. Якщо $f(x)$ – многочлен від однієї змінної над полем P з коренями $\alpha_1, \alpha_2, \cdots, \alpha_n$ (які можуть не належати P), то будь-який симетричний многочлен $g(x_1, x_2, \cdots, x_n)$ над полем P при $x_1 = \alpha_1,\ x_2 = \alpha_2, \cdots, x_n = \alpha_n$ набуває значення, яке є елементом поля P.

Д о в е д е н н я. Нехай дано якийсь многочлен *n*-го степеня від однієї змінної над полем P:

$$f(x) = x^n + a_{n-1} x^{n+1} + \cdots + a_1 x + a_0,$$

$\alpha_1, \alpha_2, \cdots, \alpha_n$ – його корені, які можуть і не належати P. Візьмемо довільний симетричний многочлен $g(x_1, x_2, \cdots, x_n)$ над P від n змінних.

За основною теоремою теорії симетричних многочленів,

$$g(x_1, x_2, \cdots, x_n) = \varphi(\sigma_1, \sigma_2, \cdots, \sigma_n),$$

причому коефіцієнти многочлена φ належать полю P. Візьмемо тут $x_1 = \alpha_1,\ x_2 = \alpha_2, \cdots, x_n = \alpha_n$. Тоді за формулами Вієта всі основні симетричні функції дорівнюватимуть відповідним коефіцієнтам многочлена $f(x)$ з належним знаком:

$$\sigma_1(\alpha_1, \alpha_2, \cdots, \alpha_n) = \alpha_1 + \alpha_2 + \cdots + \alpha_n = -a_{n-1},$$
$$\sigma_2(\alpha_1, \alpha_2, \cdots, \alpha_n) = \alpha_1\,\alpha_2 + \alpha_1\,\alpha_3 + \cdots + \alpha_{n-1}\,\alpha_n = a_{n-2},$$
$$\text{----------}$$
$$\sigma_n(\alpha_1, \alpha_2, \cdots, \alpha_n) = \alpha_1\,\alpha_2 \cdots \alpha_n = (-1)^n\, a_0.$$

У зв'язку з цим

$$g(\alpha_1, \alpha_2, \cdots, \alpha_n) = \varphi\left(-\alpha_{n-1}, \alpha_{n-2}, \cdots, (-1)^n\, a_0\right).$$

Але тоді $\varphi\left(-a_{n-1}, \alpha_{n-2}, \cdots, (-1)^n\, a_0\right)$ є елемент поля P як результат виконання операції додавання і множення над елементами з поля P. Таким чином, $g(\alpha_1, \alpha_2, \cdots, \alpha_n) \in P$. Теорему доведено.

Розглянутий метод доведення основної теореми можна використати для практичного зображення симетричних многочленів через основні симетричні функції.

Приклад. Подати симетричний многочлен над полем Q

$$f(x_1,\, x_2,\, x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 - 4\left(x_1^2 + x_2^2 + x_3^2\right) + 5$$

через основні симетричні функції.

Запишемо цей многочлен як суму однорідних многочленів:

$$f(x_1,\, x_2,\, x_3) = \varphi_1(x_1,\, x_2,\, x_3) - 4\,\varphi_2(x_1,\, x_2,\, x_3) + 5,$$

де

$$\varphi_1(x_1,\, x_2,\, x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2,$$
$$\varphi_2(x_1,\, x_2,\, x_3) = x_1^2 + x_2^2 + x_3^2\ .$$

Спочатку $\varphi_1(x_1,\, x_2,\, x_3)$ подамо через основні симетричні многочлени. Його вищий член $x_1^2x_2 = x_1^2x_2^1x_3^0$, тобто $l_1 = 2,\ l_2 = 1,\ l_3 = 0$. Побудуємо многочлен

$$g(x_1,\, x_2,\, x_3) = \sigma_1^{2-1}\,\sigma_2^{1-0}\,\sigma_3^0 = \sigma_1\,\sigma_2$$

і знаходимо різницю $\varphi_1 - g$. У цій різниці знищаться всі члени вигляду $A\,x_1^{l_1}\,x_2^{l_2}\,x_3^{l_3}$ з довільною перестановкою показників 2,1,0. Проте одночасно можуть з'явитися члени того самого степеня 3, але з іншою, нижчою системою показників, а саме: 1, 1, 1. Отже, потім треба буде відняти симетричний многочлен

$$g_1(x_1,\, x_2,\, x_3) = a\sigma_1^{1-1}\,\sigma_2^{1-1}\,\sigma_3^1 = a\sigma_3\ ,$$

де a – невизначений поки що коефіцієнт. Тому можна записати:

$$\varphi_1(x_1,\ x_2,\ x_3)=\sigma_1\sigma_2+a\sigma_3\ ,$$

тобто

$$x_1^2x_2\ +\ x_1^2x_3+x_1x_2^2+x_1x_3^2+x_2^2x_3+x_2x_3^2=$$
$$=(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)+ax_1x_2x_3.$$

Щоб знайти a, досить надати деяких числових значень змінним $x_1,\ x_2,\ x_3$, наприклад $x_1=x_2=x_3=1$. Тоді $6=9+a\ \Rightarrow\ a=-3.$

Таким чином, $\varphi_1(x_1,\ x_2,\ x_3)=\sigma_1\sigma_2-3\sigma_3$.

Аналогічно міркуємо відносно многочлена

$$\varphi_2(x_1,\ x_2,\ x_3)=x_1^2\ +\ x_2^2\ +\ x_3^2\ .$$

Можливі системи показників тут будуть 2, 0, 0 і 1, 1, 0. Отже, відніматимемо такі многочлени:

$$g_2(x_1,\ x_2,\ x_3)=\sigma_1^{2-0}\ \sigma_2^{0-0}\ \sigma_3^0\ =\sigma_1^2\ \ ,$$
$$g_3(x_1,\ x_2,\ x_3)=b\sigma_1^{1-1}\ \sigma_2^{1-0}\ \sigma_3^0\ =b\sigma_2\ \ ,$$

і далі, аналогічно до попереднього,

$$\varphi_2(x_1,\ x_2,\ x_3)=\sigma_1^2+b\sigma_2\ .$$

При $x_1=x_2=x_3=1$ маємо $3=3^2+b\cdot3$, тобто $b=-2$, і тому

$$\varphi_2(x_1,\ x_2,\ x_3)=\sigma_1^2-2\sigma_2\ .$$

Остаточно дістанемо

$$f(x_1,\ x_2,\ x_3)=\sigma_1\sigma_2-3\sigma_3-4\left(\sigma_1^2-2\sigma_2\right)+5.$$

Питання для самоконтролю

1. Дайте означення симетричного многочлена від n змінних. Наведіть приклади таких многочленів.
2. Які многочлени називаються основними симетричними функціями?
3. Які властивості мають симетричні многочлени?
4. Сформулюйте основну теорему теорії симетричних многочленів та наслідок з неї.

Тема 8. Результант двох многочленів. Виключення невідомих із системи двох рівнянь з двома невідомими

Нехай дано два многочлени над полем P:

$$f(x)=a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

$$g(x)=b_m x^m + b_{m-1}x^{m-1} + b_1 x + b_0, \quad a_n \neq 0 \ \vee \ b_m \neq 0$$

(хоч би один із старших коефіцієнтів відмінний від 0).

Дамо відповідь на питання: коли ці многочлени мають спільні корені. Для цього знайдемо умови, при яких ці многочлени мають спільний дільник додатного степеня. (Якщо f і g не мають спільного дільника додатного степеня, тобто кожен їхній спільний дільник є многочленом нульового степеня, то f і g є взаємно простими, і, очевидно, не мають спільних коренів).

Теорема 1. Многочлени $f(x)$ і $g(x)$ мають спільний дільник додатного степеня в $P[x]$ тоді і тільки тоді, коли в $P[x]$ існують многочлени $c(x)$ і $d(x)$, що задовольняють умови:

$$f(x)\cdot c(x)=g(x)\cdot d(x), \tag{1}$$

$$c(x)=c_{m-1}x^{m-1} + \cdots + c_0, \quad d(x)=d_{n-1}x^{n-1} + \cdots + d_0, \tag{2}$$

$$c(x)\neq 0 \ \textit{або} \ d(x)\neq 0 \tag{3}$$

(тобто хоч один із многочленів $c(x)$ і $d(x)$ відмінний від нуля).

Д о в е д е н н я. *Необхідність*. Припустимо, що многочлени $f(x)$ і $g(x)$ мають в $P[x]$ спільний дільник $u(x)$ додатного степеня. Тоді існують многочлени $c(x)$ і $d(x)$ такі, що

$$f(x)=d(x)\cdot u(x), \quad g(x)=c(x)\cdot u(x).$$

Домножимо першу рівність на $c(x)$, другу на $d(x)$ і віднімемо почленно:

$$f(x)\cdot c(x)-g(x)\cdot d(x)=0 \quad \Rightarrow \quad f(x)\cdot c(x)=g(x)\cdot d(x),$$

тобто (1) виконується. Очевидно, многочлен $d(x)$ є многочлен степеня не вище $n-1$, бо $\deg f = n$, $\deg u \geq 1$. Аналогічно доводиться для $c(x)$, тобто умова (2) виконується.

Далі, якщо б $c(x)=0$ і $d(x)=0$, то з рівностей $f=du$, $g=cu$ випливало б, що $f(x)=0$ і $g(x)=0$, а це суперечить умові (бо хоч

один з многочленів f або g відмінний від 0), тобто умова (3) виконується.

Достатність. Нехай існують многочлени $c(x)$ і $d(x)$, що задовольняють умови (1) – (3).

Припустимо, що $\deg f = n$, тобто $a_n \neq 0$. Нехай $\varphi(x)$ – найбільший спільний дільник $c(x)$ і $d(x)$: $\varphi=(c,d)$. Тоді в $P[x]$ існують такі многочлени $c_1(x)$ і $d_1(x)$, що

$$c(x)=c_1(x)\varphi(x), \quad d(x)=d_1(x)\varphi(x), \quad (c_1,d_1)=1. \tag{4}$$

Очевидно, що $d_1(x)\neq 0$, бо в протилежному випадку $d(x)=0$ і, за умовою (1), $c(x)=0$, що суперечить умові (3). З (4) і (1) випливає, що

$$f(x)\cdot c_1(x)\cdot\varphi(x)=g(x)\cdot d_1(x)\cdot\varphi(x),$$

звідки

$$f(x)\cdot c_1(x)=g(x)\cdot d_1(x), \tag{5}$$

З (5) випливає, що $f \; c_1 \vdots d_1$; але $(c_1,d_1)=1$, тому $f \vdots d_1$, тобто

$$f(x)=d_1(x)\cdot t(x), \tag{6}$$

де $t(x)$ – многочлен додатного степеня, оскільки $\deg d_1 \le \deg d$, а $\deg d < \deg f$ за умовою (2).

Із (5) і (6) отримаємо

$$d_1(x)\cdot t(x)\cdot c_1(x)=g(x)d_1(x),$$
$$g(x)=c_1(x)\cdot t(x). \tag{7}$$

Отже, з рівностей (6) і (7) випливає, що $f(x)$ і $g(x)$ мають спільний дільник $t(x)$ додатного степеня, що й треба було довести.

Теорему доведено.

Розпишемо умову (1) більш детально, використовуючи (2):

$$\left(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0\right)\left(c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + \ldots + c_1 x + c_0\right) =$$
$$= \left(b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0\right)\left(d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \ldots + d_1 x + d_0\right).$$

Виконавши множення в обидвох частинах рівності і, прирівнюючи коефіцієнти при однакових степенях *x,* отримаємо систему лінійних рівнянь:

$$\begin{cases} a_n\, c_{m-1} = b_m\, d_{n-1}, \\ a_{n-1}\, c_{m-1} + a_n\, c_{m-2} = b_{m-1}\, d_{n-1} + b_m\, d_{n-2}, \\ a_{n-2}\, c_{m-1} + a_{n-1}\, c_{m-2} + a_n\, c_{m-3} = b_{m-2}\, d_{n-1} + b_{m-1}\, d_{n-2} + b_m\, d_{n-3}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0\, c_2 + a_1\, c_1 + a_2\, c_0 = b_0\, d_2 + b_1\, d_1 + b_2\, d_0, \\ a_0\, c_1 + a_1\, c_0 = b_0\, d_1 + b_1\, d_0, \\ a_0\, c_0 = b_0\, d_0. \end{cases} \tag{8}$$

Це є система $n+m$ однорідних рівнянь з $n+m$ невідомими $c_{m-1}, c_{m-2}, \ldots, c_1, c_0, d_{n-1}, d_{n-2}, \ldots, d_1, d_0$. Вона має ненульові розв'язки тоді і тільки тоді, коли визначник цієї системи дорівнює нулю. Перенесемо праві частини рівнянь вліво, і, щоб не писати перед елементами визначника знаки мінус, вважатимемо, що невідомими є

$$c_{m-1}, c_{m-2}, \ldots, c_1, c_0, -d_{n-1}, -d_{n-2}, \ldots, -d_1, -d_0.$$

Якщо, крім цього, транспонувати матрицю визначника, то визначник системи набуде вигляду:

$$R = \begin{vmatrix} a_n & a_{n-1} & \ldots & a_0 & 0 & \ldots & 0 \\ 0 & a_n & \ldots & a_1 & a_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & a_n & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & b_0 & 0 & \cdots & 0 \\ 0 & b_m & \ldots & b_1 & b_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & b_m & \ldots & b_0 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ рядків} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ рядків} \end{matrix}$$

Означення 1. Результантом многочленів $f(x)$ і $g(x)$ називається визначник R.

З теореми 1 випливає, що многочлени $f(x)$ і $g(x)$ (в яких $a_n \neq 0$ або $b_m \neq 0$) мають спільний дільник додатного степеня тоді і тільки тоді, коли система лінійних рівнянь (8) має ненульові розв'язки, тобто коли $R = 0$. Отже, ми довели теорему:

Теорема 2. Нехай $f(x)$ і $g(x)$ – многочлени над полем P, і хоча б один з коефіцієнтів a_n і b_m відмінний від нуля. Многочлени

$f(x)$ і $g(x)$ мають спільний дільник додатного степеня тоді і тільки тоді, коли результант цих многочленів дорівнює нулю.

Наслідок. Якщо результант многочленів f і g дорівнює нулю, то або многочлени мають спільний дільник додатного степеня, або коефіцієнти a_n і b_m рівні нулю, і навпаки.

Результант можна означити і по-іншому.

***Означення* 2**. Результантом многочленів $f(x)$ і $g(x)$ $(a_n \neq 0)$ називається вираз

$$R(f,g) \overset{df}{=} a_n^m\, g(\alpha_1) g(\alpha_2) \cdots g(\alpha_n),$$

де $\alpha_1, \alpha_2, \cdots, \alpha_n$ – корені многочлена $f(x)$.

Аналогічно можна означити $R(g,f)$ (але при цьому слід вимагати, щоб $b_m \neq 0$).

З цього означення випливають такі ***властивості результанта***.

1. $R(f,g) = a_n^m\, b_m^n \prod\limits_{\substack{1 \le i \le n \\ 1 \le j \le m}} (\alpha_i - \gamma_j)$, де γ_j, $j = 1,...,m$, – корені $g(x)$.

Д о в е д е н н я. $g(x) = b_m (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_m)$. Тоді

$$g(\alpha_i) = b_m (\alpha_i - \gamma_1)(\alpha_i - \gamma_2) \cdots (\alpha_i - \gamma_m) = b_m \prod_{1 \le j \le m} (\alpha_i - \gamma_j),$$

звідки

$$R(f,g) = a_n^m\, g(\alpha_1) g(\alpha_2) \cdots g(\alpha_n) = a_n^m \left[b_m \prod_{1 \le j \le m} (\alpha_1 - \gamma_j) \right] \left[b_m \prod_{1 \le j \le m} (\alpha_2 - \gamma_j) \right] \times \cdots \times$$

$$\times \left[b_m \prod_{1 \le j \le m} (\alpha_n - \gamma_j) \right] = a_n^m\, b_m^n \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (\alpha_i - \gamma_j).$$

2. $R(g,f) = (-1)^{mn} R(f,g)$.

Д о в е д е н н я. Використаємо властивість 1 для $R(g,f)$:

$$R(g,f) = b_m^n\, a_n^m \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (\gamma_j - \alpha_i).$$

Винесемо в кожному множнику (а їх є mn) за дужки число (-1), отримаємо:

$$R(g,f) = (-1)^{mn} b_m^n\, a_n^m \prod_{\substack{1 \le i \le n \\ 1 \le j \le m}} (\alpha_i - \gamma_j) = (-1)^{mn} R(f,g).$$

Поняття результанта можна застосувати до розв'язання питання про наявність кратних коренів многочлена. Кратний корінь многочлена $f(x)$ повинен бути спільним коренем многочлена $f(x)$ і його похідної $f'(x)$, а $f(x)$ і $f'(x)$ матимуть спільний корінь, якщо $R(f, f') = 0$.

Означення 3. **Дискримінантом** $D(f)$ многочлена $f(x)$ називається вираз

$$D(f) \overset{df}{=} (-1)^{\frac{n(n-1)}{2}} a_n^{-1} R(f, f'),$$

де $R(f, f')$ – результант многочлена $f(x)$ і його похідної $f'(x)$.

При цьому справджується рівність

$$D(f) = a_n^{2n-2} \prod_{1 \le j < i \le n} (\alpha_i - \alpha_j)^2.$$

З теореми 2 дістаємо таке твердження:

Теорема 3. Многочлен $f(x)$ має кратний корінь тоді і тільки тоді, коли його дискримінант дорівнює нулю.

Дійсно, якщо f має спільний корінь з f', то $R(f, f') = 0 \Rightarrow D(f) = 0$. Навпаки аналогічно.

Приклад. При яких значеннях λ многочлени

$$f(x) = x^3 - \lambda x^2 + \lambda x - 1 \quad i \quad g(x) = x^2 + \lambda$$

мають спільні корені?

Обчислимо результант ($n = 3$, $m = 2$):

$$R(f, g) = \begin{vmatrix} 1 & -\lambda & \lambda & -1 & 0 \\ 0 & 1 & -\lambda & \lambda & -1 \\ 1 & 0 & \lambda & 0 & 0 \\ 0 & 1 & 0 & \lambda & 0 \\ 0 & 0 & 1 & 0 & \lambda \end{vmatrix} = (\lambda^2 - 1)^2.$$

$(\lambda^2 - 1)^2 = 0 \Leftrightarrow \lambda = \pm 1$. Отже, f і g мають спільні корені, якщо $\lambda = \pm 1$.

Перевірка. Якщо $\lambda = 1$, то многочлени

$$f(x) = x^3 - x^2 + x - 1 = (x^2 + 1)(x - 1) \quad \text{і} \quad g(x) = x^2 + 1$$

мають спільні корені $\pm i$.

Якщо $\lambda = -1$, то многочлени

$$f(x) = x^3 + x^2 - x - 1 = \left(x^2 - 1\right)(x+1) \quad \text{і} \quad g(x) = x^2 - 1$$

мають спільні корені ± 1.

Результант 2-х многочленів можна використовувати для розв'язання системи двох рівнянь з двома невідомими, хоча б одне з яких є нелінійне.

Нехай задано систему рівнянь

$$\begin{cases} f(x, y) = 0, \\ g(x, y) = 0, \end{cases} \tag{9}$$

де f і g – многочлени над полем P. Запишемо ці многочлени за спадними степенями змінної x:

$$f(x, y) = a_n(y)x^n + a_{n-1}(y)x^{n-1} + \cdots + a_0(y),$$
$$g(x, y) = b_m(y)x^m + b_{m-1}(y)x^{m-1} + b_0(y),$$

де $a_i(y),\ b_j(y) \in P[y]$. Знайдемо результант f і g, розглядаючи їх як многочлени від x, і позначимо його $R(y)$.

Припустимо, що система (9) має в полі P розв'язок (α, β), тоді многочлени

$$f(x, \beta) = a_n(\beta)x^n + a_{n-1}(\beta)x^{n-1} + \cdots + a_0(\beta),$$
$$g(x, \beta) = b_m(\beta)x^m + b_{m-1}(\beta)x^{m-1} + \cdots + b_0(\beta)$$

мають спільний корінь α, тобто мають спільний дільник додатного степеня. За теоремою 2 їхній результант $R(\beta) = 0$. Навпаки: якщо β – корінь результанта $R(y)$, тобто $R(\beta) = 0$, то за наслідком з теореми 2, многочлени $f(x, \beta)$ і $g(x, \beta)$ або мають спільний корінь, або їхні коефіцієнти $a_n(\beta)$ і $b_m(\beta)$ обидва дорівнюють нулю.

Отже, розв'язання системи рівнянь (9) з двома невідомими зводиться до розв'язання рівняння

$$R(y) = 0 \tag{10}$$

з однією змінною y. Говорять, що рівняння (10) є результант виключення x із системи рівнянь (9).

Схема виключення невідомих із системи (9) така:

1) упорядковуємо многочлени $f(x,y)$ і $g(x,y)$ за спадними степенями однієї із змінних, наприклад, x;

2) складаємо результант $R(f,g)$, розглядаючи змінну y як параметр;

3) знаходимо всі корені результанта $\beta_1, \beta_2, \cdots, \beta_l$;

4) підставляємо в задану систему замість змінної y значення $\beta_1, \beta_2, \cdots, \beta_l$; дістаємо сукупність l систем двох рівнянь з одним невідомим x;

5) розв'язуємо цю сукупність систем рівнянь і складаємо відповідні пари розв'язків.

Приклад. Розв'язати систему рівнянь:

$$\begin{cases} x^2y^2 + x^2y + y + x = 0, \\ xy^2 + 2xy + 1 = 0. \end{cases}$$

Розв'язання.

$$\begin{cases} (y^2 + y)x^2 + x + y = 0, \\ (y^2 + 2y)x + 1 = 0. \end{cases}$$

$$R(y) = \begin{vmatrix} y^2+y & 1 & y \\ y^2+2y & 1 & 0 \\ 0 & y^2+2y & 1 \end{vmatrix} = y^2 + y + y(y^2+2y)^2 - y^2 - 2y = y\left[(y^2+2y)^2 - 1\right]$$

Знаходимо корені рівняння $R(y)=0$.

$$y\left[\left(y^2+2y\right)^2 - 1\right] = y\left(y^2+2y-1\right)\times\left(y^2+2y+1\right) = y(y+1)^2\left(y^2+2y-1\right) = 0$$

$$y_1 = 0, \quad y_{2,3} = -1, \quad y_{4,5} = \frac{-2 \pm 2\sqrt{2}}{2} = -1 \pm \sqrt{2}.$$

При $y = 0$ система $\begin{cases} x = 0, \\ 1 = 0 \end{cases}$ несумісна.

При $y = -1$ $\begin{cases} x - 1 = 0 \\ -x + 1 = 0 \end{cases}$ $\begin{cases} x = 1 \\ x = 1 \end{cases}$. Отже, $(1;-1)$ – перший розв'язок системи.

При

$y=-1-\sqrt{2}$ $\begin{cases}\left(3+2\sqrt{2}-1-\sqrt{2}\right)x^2+x-1-\sqrt{2}=0\\ \left(3+2\sqrt{2}-2-\sqrt{2}\right)x+1=0\end{cases}$ $\begin{cases}\left(2+2\sqrt{2}\right)x^2+x-1-\sqrt{2}=0\\ x+1=0\end{cases}$

$x=-1$ $\left(-1;-1-\sqrt{2}\right)$ – другий розв'язок системи.

При

$y=-1+\sqrt{2}$ $\begin{cases}\left(3-2\sqrt{2}-1+\sqrt{2}\right)x^2+x-1+\sqrt{2}=0\\ \left(3-2\sqrt{2}-2+2\sqrt{2}\right)x+1=0\end{cases}$ $\begin{cases}\left(2-\sqrt{2}\right)x^2+x-1+\sqrt{2}=0\\ x+1=0\end{cases}$

$x=-1$ $\left(-1;-1+\sqrt{2}\right)$ – третій розв'язок системи.

Відповідь: $(1;-1)$, $\left(-1;-1-\sqrt{2}\right)$, $\left(-1;-1+\sqrt{2}\right)$.

Питання для самоконтролю

1. Дайте різні означення результанта двох многочленів.
2. Які властивості має результант?
3. При якій умові многочлени $f(x)$ і $g(x)$ мають спільні корені?
4. Дайте означення дискримінанта многочлена *n*-го степеня.
5. Сформулюйте необхідну і достатню умову наявності кратного кореня у многочлена *n*-го степеня.
6. Опишіть схему виключення невідомих із системи двох рівнянь з двома невідомими, хоча б одне з яких є нелінійне.

Розділ ІІІ. МНОГОЧЛЕНИ НАД ПОЛЕМ КОМПЛЕКСНИХ ЧИСЕЛ І НАД ПОЛЕМ ДІЙСНИХ ЧИСЕЛ

Тема 9. Многочлени над полем комплексних чисел. Алгебраїчна замкненість поля комплексних чисел

Відомо, що для многочленів над числовими полями алгебраїчне та функціональне тлумачення цілком рівноправні. У цьому розділі будемо дотримуватись функціонального погляду на многочлени, причому комплексну змінну позначатимемо буквою z.

Означення. Поле P називається ***алгебраїчно замкненим,*** якщо довільний многочлен $f(x) \in P[x]$ додатного степеня має в полі P хоча б один корінь.

Або, інакше кажучи, поле P називається алгебраїчно замкненим, якщо будь-який многочлен $f(x) \in P[x], \deg f \geq 1$ розкладається на лінійні множники.

Виявляється, що єдиним числовим полем, яке має цю властивість, є поле комплексних чисел C.

Теорема (основна теорема теорії многочленів).

Поле комплексних чисел алгебраїчно замкнене, тобто довільний многочлен ненульового степеня з комплексними коефіцієнтами

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 \qquad (1)$$

має хоча б один комплексний корінь.

Щоб довести цю теорему, сформулюємо та доведемо ряд лем.

Лема 1 (про модуль старшого члена).

Якщо дано многочлен (1), де $n \geq 1$, і якщо $k \in R^+$ – довільне число, то для достатньо великих $|z|$ справджується нерівність

$$\left|a_n z^n\right| > k\left|a_{n-1} z^{n-1} + \ldots + a_1 z + a_0\right|, \qquad (2)$$

тобто модуль старшого члена більший за модуль суми всіх інших членів, причому у скільки завгодно разів.

Д о в е д е н н я. Нехай $A = \max\left\{|a_{n-1}|,...,|a_1|,|a_0|\right\}$. Тоді, використавши властивості модуля комплексного числа, маємо:

$$\left|a_{n-1}z^{n-1} + ... + a_1 z + a_0\right| \le |a_{n-1}||z|^{n-1} + ... + |a_1||z| + |a_0| \le$$

$$\le A\left(|z|^{n-1} + ... + |z| + 1\right) = A\frac{|z|^n - 1}{|z| - 1}.$$

Покладаючи $|z| > 1$, отримаємо: $\dfrac{|z|^n - 1}{|z| - 1} < \dfrac{|z|^n}{|z| - 1}$,

звідки

$$\left|a_{n-1}z^{n-1} + ... + a_1 z + a_0\right| < A\frac{|z|^n}{|z| - 1},$$

$$k\left|a_{n-1}z^{n-1} + ... + a_1 z + a_0\right| < kA\frac{|z|^n}{|z| - 1}.$$

Таким чином, нерівність (2) буде виконуватися, якщо z задовольняє, крім умови $|z| > 1$, ще нерівність

$$kA\frac{|z|^n}{|z| - 1} \le \left|a_n z^n\right| = |a_n||z|^n,$$

тобто якщо $\dfrac{kA}{|z| - 1} \le |a_n|$, або $\dfrac{|z| - 1}{kA} \ge \dfrac{1}{|a_n|}$, або $|z| \ge \dfrac{kA}{|a_n|} + 1$.

Оскільки права частина останньої нерівності більша за 1, то можна стверджувати, що для значень z, що задовольняють цю нерівність, виконується нерівність (2), що і доводить лему.

Лема 2 (про зростання модуля многочлена).

Якщо $f(z) \in C[z]$ – многочлен ненульового степеня, то для довільного додатного числа M можна знайти таке число N, що при $|z| > N$ виконується нерівність $|f(z)| > M$.

Д о в е д е н н я. Використовуючи властивості модуля комплексного числа, маємо:

$$|f(z)| = \left|a_n z^n + \left(a_{n-1}z^{n-1} + ... + a_1 z + a_0\right)\right| \ge \left|a_n z^n\right| - \left|a_{n-1}z^{n-1} + ... + a_1 z + a_0\right|. \quad (3)$$

Використаємо лему 1, поклавши $k = 2$; тоді існує таке число $N_1 = \dfrac{2A}{|a_n|} + 1$, що при $|z| \geq N_1$

$$|a_n z^n| > 2|a_{n-1} z^{n-1} + \ldots + a_1 z + a_0|.$$

Звідси

$$|a_{n-1} z^{n-1} + \ldots + a_1 z + a_0| < \frac{1}{2}|a_n z^n| \ .$$

Тоді, підсилюючи нерівність (3),

$$|f(z)| > |a_n z^n| - \frac{1}{2}|a_n z^n| = \frac{1}{2}|a_n z^n|. \qquad (4)$$

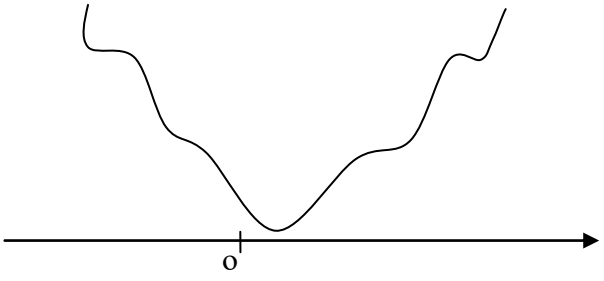
Права частина цієї нерівності буде більша за M, якщо

$$\frac{1}{2}|a_n z^n| > M \Rightarrow |a_n||z|^n > 2M \Rightarrow |z| > \sqrt[n]{\frac{2M}{|a_n|}} \ ,$$

тобто при $|z| > N_2 = \sqrt[n]{\dfrac{2M}{|a_n|}}$.

Отже, при $|z| > N = \max\{N_1, N_2\}$ отримаємо, що $|f(z)| > M$.

Дамо геометричну ілюстрацію цієї леми. Припустимо, що в кожній точці z_0 комплексної площини поставлено перпендикуляр до цієї площини, довжина якого дорівнює $|f(z_0)|$. Унаслідок неперервності модуля многочлена кінці цих перпендикулярів утворюють неперервну криву поверхню, розміщену над комплексною площиною. Лема 2 говорить про те, що при $|z_0| \to \infty$ ця поверхня все більше і більше віддаляється від комплексної площини. На мал. 1 схематично зображено лінію перетину цієї поверхні з площиною, яка проходить через т.О і перпендикулярна до комплексної площини.



Мал. 1.

Наслідок. Многочлен $f(z)$ може мати тільки такі корені, модуль яких менший від числа $N_0 = 1 + \dfrac{A}{|a_n|}$, де $A = \max\{|a_{n-1}|,...,|a_1|,|a_0|\}$.

Якщо z – довільне число, причому $|z| \geq N_0$, тобто

$$|z| \geq 1 + \frac{A}{|a_n|} \Rightarrow |a_n||z| \geq |a_n| + A \Rightarrow |a_n| \geq \frac{|a_n| + A}{|z|}.$$

Тоді з нерівності (4)

$$|f(z)| > \frac{1}{2}|a_n z^n| = \frac{1}{2}|a_n||z|^n \geq \frac{1}{2}\frac{|a_n| + A}{|z|}|z|^n = \frac{1}{2}(|a_n| + A)|z|^{n-1} > 0,$$

тобто $|f(z)| > 0$, а це означає, що z не є коренем $f(z)$.

Лема 3 (Даламбера).
Якщо для деякого $a \in C$ $f(a) \neq 0$, то $\exists c \in C$ таке, що $|f(c)| < |f(a)|$.

Д о в е д е н н я цієї леми не наводимо.

Д о в е д е н н я основної теореми.

Нехай $f(z) \in C[z]$. Якщо $f(0) = 0$ (тобто многочлен $f(z)$ не має вільного члена), то нуль є коренем многочлена $f(z)$, тобто теорема справджується.

Припустимо, що $f(0) \neq 0$, і покладемо, що $M = |f(0)|$. За лемою 2 (про зростання модуля многочлена), існує таке N, що при $|z| > N$ виконується нерівність $|f(z)| > |f(0)|$.

Використаємо тепер теорему, що узагальнює відому теорему Вейєрштрасса:

Якщо дійсна функція $g(z)$ комплексної змінної z неперервна у всіх точках замкнутого круга K, то в крузі K існує така точка z_0, що $\forall z \in K \quad g(z) \geq g(z_0)$. Точка z_0 є точкою мінімуму для $g(z)$ в крузі K.

Дійсна функція комплексної змінної – це функція комплексної змінної, що набуває лише дійсних значень. Очевидно, що модуль многочлена над полем C є дійсною функцією комплексної змінної,

причому можна показати, що ця функція (тобто $|f(z)|$) є неперервною.

Нехай $K = \{ z \in C \ : \ |z| \le N \}$, тобто K – замкнутий круг комплексної площини радіуса N з центром у точці O. Тоді функція $|f(z)|$ досягає на множині K свого мінімуму, тобто $\exists a \in K$, що $\forall z \in K$ $(|z| \le N)$

$$|f(a)| \le |f(z)|;$$

зокрема

$$|f(a)| \le |f(0)|.$$

Легко бачити, що a буде точкою мінімуму для $|f(z)|$ на всій комплексній площині: якщо точка z' лежить поза кругом K, то $|z'| > N$ і тому

$$|f(z')| > |f(0)| \ge |f(a)|.$$

Якщо б $f(a) \ne 0$, то за лемою Даламбера, $\exists c \in C$ таке, що

$$|f(c)| < |f(a)|,$$

а це суперечить тому, що a – точка мінімуму. Тому $f(a) = 0$, тобто комплексне число a є коренем многочлена $f(z)$. Теорему доведено.

З основної теореми теорії многочленів випливає низка важливих наслідків.

Наслідок 1. Кожний многочлен з кільця $C[z]$, степінь якого більший за одиницю, звідний у полі комплексних чисел.

Д о в е д е н н я. Нехай $f(z) \in C[z]$, $\deg f > 1$. За основною теоремою, існує хоча б один корінь $z = a$ цього многочлена, тобто $f(a) = 0$. Тоді $f(z)$ ділиться на $z - a$, тобто $\exists g(z) \in C[z]$ такий, що $f(z) = (z - a)g(z)$. При цьому $\deg g > 0$, бо $\deg f > 1$. Отже, многочлен $f(z)$ звідний у полі C.

З цього наслідку випливає, що для того, щоб многочлен був незвідним у полі комплексних чисел, необхідно і достатньо, щоб його степінь дорівнював одиниці.

Наслідок 2. Кожний многочлен додатного степеня над полем комплексних чисел єдиним способом (з точністю до порядку множників) розкладається на лінійні множники в цьому полі

$$f(z) = a_n(z - z_1)(z - z_2)...(z - z_n),$$

де $z_1, z_2, ..., z_n$ – корені, а a_n – старший коефіцієнт многочлена $f(z)$.

Цей наслідок випливає з попереднього і теореми 2 теми 4.

Якщо в розкладі $f(z) = a_n(z - z_1)(z - z_2)...(z - z_n)$

$z_1, z_2, ..., z_m$ є всі різні корені многочлена $f(z)$, то цей розклад можна подати у вигляді

$$f(z) = a_n(z - z_1)^{k_1}(z - z_2)^{k_2}...(z - z_m)^{k_m}, \quad k_1 + k_2 + ... + k_m = n.$$

Розклад

$$f(z) = a_n(z - z_1)^{k_1}(z - z_2)^{k_2}...(z - z_m)^{k_m}$$

називається ***канонічним розкладом*** $f(z)$ на незвідні множники. Число k_s називається ***показником кратності*** кореня z_s.

Наслідок 3. Кожний многочлен $f(z)$ додатного степеня n із кільця $C[z]$ має точно n комплексних коренів, якщо кожний корінь враховувати стільки разів, яка його кратність.

Питання для самоконтролю

1. Дайте означення алгебраїчно замкненого поля.
2. Сформулюйте основну теорему теорії многочленів.
3. Сформулюйте лему про модуль старшого члена многочлена.
4. Сформулюйте лему про зростання модуля многочлена та наслідок з неї.
5. Сформулюйте лему Даламбера.
6. Сформулюйте твердження про звідність у полі комплексних чисел многочлена з кільця $C[z]$, степінь якого більший за одиницю.
7. Сформулюйте твердження про розклад многочлена додатного степеня над полем комплексних чисел на лінійні множники.

Тема 10. Многочлени над полем дійсних чисел

Оскільки поле дійсних чисел R є підполем поля комплексних чисел C, то всі результати, отримані для многочленів над полем C, залишаються справедливими і для многочленів над полем R, зокрема: будь-який многочлен n-го степеня з дійсними коефіцієнтами має точно n комплексних коренів. Але в багатьох випадках особливий інтерес становлять саме дійсні корені рівнянь з дійсними коефіцієнтами.

Нехай маємо многочлен з дійсними коефіцієнтами:

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0,\ a_i \in R,\ i = 0,\ldots,n. \qquad (1)$$

Теорема 1 (*про спряженість уявних коренів многочлена з дійсними коефіцієнтами*). Якщо комплексне число $z_0 = a + bi$ є коренем многочлена (1) з дійсними коефіцієнтами, то спряжене комплексне число $\overline{z_0} = a - bi$ також є коренем цього многочлена.

Нагадаємо, що комплексне число $a + bi$ називається *уявним*, якщо $b \neq 0$.

Д о в е д е н н я. Оскільки z_0 – корінь многочлена (1), то

$$f(z_0) = a_n z_0^n + a_{n-1} z_0^{n-1} + \ldots + a_1 z_0 + a_0 = 0.$$

Використовуючи властивості спряжених комплексних чисел і враховуючи те, що спряженими до дійсних чисел $a_i,\ i = 0,\ldots,n$, є ті самі дійсні числа a_i, отримаємо, що

$$\begin{aligned} f(\overline{z_0}) &= a_n \overline{z_0}^n + a_{n-1} \overline{z_0}^{n-1} + \ldots + a_1 \overline{z_0} + a_0 = \\ &= \overline{a_n}\,\overline{z_0}^n + \overline{a_{n-1}}\,\overline{z_0}^{n-1} + \ldots + \overline{a_1}\,\overline{z_0} + \overline{a_0} = \\ &= \overline{a_n z_0^n + a_{n-1} z_0^{n-1} + \ldots + a_1 z_0 + a_0} = \overline{f(z_0)} = \overline{0} = 0, \end{aligned}$$

тобто $f(\overline{z_0}) = 0$. А це означає, що $\overline{z_0}$ є коренем многочлена (1).

Теорему доведено.

Теорема 2. Якщо комплексне число z_0 є коренем k-ої кратності (k>1) многочлена (1) з дійсними коефіцієнтами, то спряжене комплексне число $\overline{z_0}$ є коренем многочлена (1) тієї ж кратності k.

Д о в е д е н н я. Оскільки z_0 – корінь $f(z)$ кратності k, то

$$f(z_0) = f'(z_0) = f''(z_0) = \ldots = f^{(k-1)}(z_0) = 0, \quad f^{(k)}(z_0) \neq 0. \qquad (2)$$

Але всі похідні від $f(z)$ мають також дійсні коефіцієнти. Тому, за теоремою 1,

$$f(\overline{z_0}) = f'(\overline{z_0}) = f''(\overline{z_0}) = \ldots = f^{(k-1)}(\overline{z_0}) = 0.$$

З іншого боку, $f^{(k)}(\overline{z_0}) \neq 0$, бо в протилежному випадку (тобто якщо б $f^{(k)}(\overline{z_0}) = 0$) за теоремою 1, число z_0, спряжене з $\overline{z_0}$, було б коренем $f^{(k)}(z)$, тобто $f^{(k)}(z_0) = 0$, що суперечить (2).

Отже,

$$f(\overline{z_0}) = f'(\overline{z_0}) = f''(\overline{z_0}) = \ldots = f^{(k-1)}(\overline{z_0}) = 0, \quad f^{(k)}(\overline{z_0}) \neq 0.$$

Це означає, що $\overline{z_0}$ є коренем многочлена $f(z)$ кратності *k*. Теорему доведено.

Теорема 3. Кожний многочлен над полем *R*, степінь якого перевищує 2, є звідним у цьому полі.

Д о в е д е н н я. Нехай $\deg f > 2$ і z_0 – якийсь корінь $f(z)$.

Якщо z_0 – дійсне число, то за теоремою Безу в полі *R* можливий розклад $f(z) = (z - z_0) f_1(z)$, причому $f_1(z) \in R[z]$ і є многочленом ненульового степеня, бо $\deg f > 2$. Отже, в цьому випадку $f(z)$ звідний у полі *R*.

Якщо ж z_0 – комплексний корінь многочлена $f(z)$, то, за теоремою 1, $\overline{z_0}$ теж є коренем $f(z)$. Тому $f(z) \vdots (z - z_0) \wedge f(z) \vdots (z - \overline{z_0})$, а тому $f(z) \vdots (z - z_0)(z - \overline{z_0})$, тобто $f(z)$ ділиться на добуток

$$\varphi(z) = (z - z_0)(z - \overline{z_0}) = z^2 - (z_0 + \overline{z_0})z + z_0\overline{z_0}.$$

Оскільки сума $z_0 + \overline{z_0}$ і добуток $z_0\overline{z_0}$ двох спряжених чисел є дійсні числа, то многочлен $\varphi(z)$ має дійсні коефіцієнти. Отже, многочлен $f(z) \in R[z]$ ділиться на многочлен $\varphi(z) \in R[z]$:

$$f(z) = \varphi(z) \cdot f_1(z).$$

Тому їхня частка $f_1(z)$ теж є многочленом над полем *R*. Оскільки $\deg \varphi = 2$, $\deg f > 2$, то $f_1(z)$ є многочлен ненульового степеня. Звідність $f(z)$ у полі *R* доведено.

Щодо многочленів другого степеня над полем R, то вони можуть бути незвідні в цьому полі (якщо мають комплексні корені). Отже, якщо в полі C незвідними були лише многочлени першого степеня, то в полі R незвідними є многочлени першого степеня і деякі многочлени другого степеня.

Теорема 4. Кожний многочлен $f(z)$ над полем дійсних чисел допускає єдиний розклад на незвідні множники в цьому полі вигляду:

$$f(z) = a_n(z - z_1)^{k_1}(z - z_2)^{k_2}...(z - z_l)^{k_l}(z^2 + p_{l+1}z + q_{l+1})^{k_{l+1}}...(z^2 + p_m z + q_m)^{k_m}.$$

Д о в е д е н н я. Відомо, що для многочлена $f(z)$ у полі R можливий розклад вигляду

$$f(z) = \left(f_1(z)\right)^{k_1}\left(f_2(z)\right)^{k_2}...\left(f_m(z)\right)^{k_m}, \qquad (3)$$

де $f_1(z), f_2(z),..., f_m(z)$ – незвідні у полі R многочлени, які визначаються з точністю до сталого множника. Якщо поставити вимогу, щоб старші коефіцієнти цих многочленів дорівнювали 1, то вони визначатимуться однозначно. З теореми 3 випливає, що $f_k(z)$ є многочленами не вище другого степеня. Припустимо, що $f_1(z), f_2(z),..., f_l(z)$ є множники першого степеня, а $f_{l+1}(z), f_{l+2}(z),..., f_m(z)$ – незвідні множники другого степеня (може бути, що $l = 0$ або $l = m$). Тоді (3) матиме вигляд:

$$f(z) = A(z + \alpha_1)^{k_1}(z + \alpha_2)^{k_2}...(z + \alpha_l)^{k_l}(z^2 + p_{l+1}z + q_{l+1})^{k_{l+1}}...(z^2 + p_m z + q_m)^{k_m}.$$

Легко бачити, що $A = a_n$, а $-\alpha_1, -\alpha_2,..., -\alpha_l$ – дійсні корені $f(z)$, тобто $z_1, z_2,..., z_l$. Отже, цей розклад збігається з (3). Теорему доведено.

Наслідок 1. Довільний многочлен з дійсними коефіцієнтами має парне число комплексних коренів.

Наслідок 2. Многочлен непарного степеня з дійсними коефіцієнтами має хоча б один дійсний корінь.

Наслідок 3. Нехай $f(z)$ – многочлен степеня n з дійсними коефіцієнтами. Парність числа дійсних коренів многочлена $f(z)$ збігається з парністю числа n.

Приклади. 1. Знайти многочлен найменшого степеня з дійсними коефіцієнтами, якщо цей многочлен має корені $i-1, \pi, -1+i\sqrt{3}$ і старший коефіцієнт 1.

Розклад шуканого многочлена $f(z)$ на незвідні множники над полем C має вигляд:

$$f(z)=1\cdot(z-(-1+i))(z-(-1-i))(z-(-1+i\sqrt{3}))(z-(-1-i\sqrt{3}))(z-\pi)=$$

$$=(z+1-i)(z+1+i)(z+1-i\sqrt{3})(z+1+i\sqrt{3})(z-\pi)=$$

$$=\left((z+1)^2-i^2\right)\left((z+1)^2-(i\sqrt{3})^2\right)(z-\pi)=(z^2+2z+2)(z^2+2z+4)(z-\pi).$$

2. Розкласти многочлен $f(z)=z^4+4$ на незвідні множники над полями *C*, *R*, *Q*.

$$z^4+4=(z^2+2)^2-4z^2=(z^2-2z+2)(z^2+2z+2).$$

Розклад у полях *R* і *Q*: $f(z)=(z^2-2z+2)(z^2+2z+2)$, а в полі *C*: $f(z)=(z-1-i)(z-1+i)(z+1-i)(z+1+i)$.

Теорема 4 має істотне значення для розкладання дробово-раціональних функцій на елементарні дроби в полі дійсних чисел, що використовується у курсі математичного аналізу.

Питання для самоконтролю

1. Сформулюйте і доведіть теорему про спряженість уявних коренів многочлена з дійсними коефіцієнтами.
2. Сформулюйте теорему про звідність у полі *R* кожного многочлена, степінь якого перевищує 2.
3. Сформулюйте теорему про розклад многочлена над полем дійсних чисел на незвідні множники.
4. Яку кількість комплексних коренів має многочлен з дійсними коефіцієнтами?
5. Яку кількість дійсних коренів має многочлен непарного степеня з дійсними коефіцієнтами?

Тема 11. Рівняння третього і четвертого степенів

1. Кубічні рівняння.

Загальний вигляд кубічного рівняння такий:

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \quad (a_3 \neq 0).$$

Якщо $a_3 \neq 1$, то, поділивши обидві частини рівняння на a_3, отримаємо рівняння:

$$x^3 + \frac{a_2}{a_3}x^2 + \frac{a_1}{a_3}x + \frac{a_0}{a_3} = 0 \quad (a_3 \neq 0),$$

рівносильне даному, але в якого старший коефіцієнт дорівнює 1. Тому обмежимось розглядом кубічного рівняння, старший коефіцієнт якого дорівнює 1.

Нехай дано кубічне рівняння

$$x^3 + ax^2 + bx + c = 0 \qquad (1)$$

з довільними комплексними коефіцієнтами. Зробимо заміну $x = y - \frac{a}{3}$.

Отримаємо:

$$\left(y - \frac{a}{3}\right)^3 + a\left(y - \frac{a}{3}\right)^2 + b\left(y - \frac{a}{3}\right) + c = y^3 + \left(-\frac{a^2}{3} + b\right)y + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) = 0.$$

(*Перетворення пропонуємо читачеві провести самостійно.*)

Отже, щоб розв'язати рівняння (1), досить уміти розв'язувати рівняння

$$x^3 + px + q = 0 \qquad (2)$$

з будь-якими комплексними коефіцієнтами. Рівняння (2) називається **неповним кубічним рівнянням**.

Розв'язок рівняння (2) шукаємо у вигляді суми $x = u + v$, де u і v – нові невідомі. Підставимо його в рівняння (2):

$$(u+v)^3 + p(u+v) + q = 0,$$

або $$u^3 + 3u^2v + 3uv^2 + v^3 + pu + pv + q = 0,$$

тобто $$(u^3 + v^3 + q) + (3uv + p)(u + v) = 0.$$

Якщо u і v вибрати так, щоб

$$u^3 + v^3 + q = 0$$
$$3uv + p = 0$$

тобто

$$\begin{aligned} u^3 + v^3 &= -q \\ uv &= -\frac{p}{3}, \end{aligned} \tag{3}$$

тоді $x = u + v$ буде коренем рівняння (2).

Але якщо для u і v виконуються рівності (3), то виконуються також рівності

$$\begin{aligned} u^3 + v^3 &= -q \\ u^3 v^3 &= -\left(\frac{p}{3}\right)^3, \end{aligned} \tag{4}$$

і тому u^3 і v^3 за формулами Вієта для коренів квадратного рівняння будуть коренями квадратного рівняння

$$z^2 + qz - \left(\frac{p}{3}\right)^3 = 0. \tag{5}$$

Його дискримінант позначимо Δ:

$$\Delta = q^2 + 4\left(\frac{p}{3}\right)^3 = 4\left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right).$$

Число $D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$ називають **дискримінантом рівняння** (2).

Корені z_1, z_2 рівняння (5) матимуть вигляд:

$$z_1 = u^3 = \frac{-q + \sqrt{\Delta}}{2} = \frac{-q + 2\sqrt{D}}{2} = -\frac{q}{2} + \sqrt{D} = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},$$

$$z_2 = v^3 = \frac{-q - \sqrt{\Delta}}{2} = \frac{-q - 2\sqrt{D}}{2} = -\frac{q}{2} - \sqrt{D} = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},$$

звідки

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}. \tag{6}$$

Тоді

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}. \qquad (7)$$

Ця формула коренів кубічного рівняння (2) називається **формулою Кардано**.

Кубічний корінь з будь-якого комплексного числа, відмінного від нуля, має в полі C три значення. Отже, u і v мають по три значення. Звідси знаходимо дев'ять розв'язків системи (4). Вибираючи з них тільки ті, що задовольняють умову

$$u\,v = -\frac{p}{3} \qquad (8)$$

(бо система (4) є наслідком системи (3), а не рівносильною їй), отримаємо всі розв'язки системи (3).

Застосовуючи формулу Кардано, знаходять значення одного з радикалів, а відповідні їм значення другого радикала визначають, користуючись співвідношенням (8), і, у такий спосіб, знаходять усі три корені рівняння (2).

Нехай u_0 – будь-яке одне з трьох значень u. Тоді два інші значення u можна отримати множенням u_0 на кубічні корені ε і ε^2 з одиниці:

$$u_1 = u_0\varepsilon, \quad u_2 = u_0\varepsilon^2,$$

де $\varepsilon = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\varepsilon^2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.

Позначимо через v_0 те з трьох значень радикала v, яке відповідає значенню u_0 радикала u, тобто

$$v_0 = -\frac{p}{3u_0}.$$

Двома іншими значеннями v будуть $v_0\varepsilon$, $v_0\varepsilon^2$. Значенню $u_0\varepsilon$ радикала u відповідатиме значення $v_0\varepsilon^2$ радикала v, бо

$$(u_0\varepsilon)(v_0\varepsilon^2) = (u_0v_0)\varepsilon^3 = u_0v_0 = -\frac{p}{3}.$$

Аналогічно, значенню $u_0\varepsilon^2$ радикала u відповідає значення $v_0\varepsilon$ радикала v. Додаючи відповідні значення u і v, отримаємо три корені рівняння (2):

$$\begin{cases} x_0 = u_0 + v_0, \\ x_1 = u_0\varepsilon + v_0\varepsilon^2, \\ x_2 = u_0\varepsilon^2 + v_0\varepsilon. \end{cases} \qquad (9)$$

Приклад 1. Розв'язати рівняння: $x^3 - 9x^2 + 21x - 5 = 0$.

Зробимо заміну $x = y - \frac{a}{3} = y - \frac{-9}{3} = y + 3$; отримаємо рівняння

$$(y+3)^3 - 9(y+3)^2 + 21(y+3) - 5 =$$

$$= y^3 + 9y^2 + 27y + 27 - 9y^2 - 54y - 81 + 21y + 63 - 5 = 0,$$

тобто

$$y^3 - 6y + 4 = 0.$$

Тут $p = -6, q = 4$.

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} = \sqrt[3]{-2 + \sqrt{4-8}} = \sqrt[3]{-2+2i} =$$

$$= \sqrt[3]{2\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)} = \sqrt{2}\left(\cos\frac{\frac{3\pi}{4} + 2\pi k}{3} + i\sin\frac{\frac{3\pi}{4} + 2\pi k}{3}\right).$$

Позначимо через u_0 значення u, яке отримується при $k = 0$, тобто

$$u_0 = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = 1 + i.$$

Із співвідношення (8) отримаємо:

$$v_0 = -\frac{p}{3u_0} = -\frac{-6}{3u_0} = \frac{2}{u_0} = \frac{2}{1+i} = \frac{2}{1+i}\cdot\frac{1-i}{1-i} = 1 - i.$$

Тоді за формулами (9)

$$\begin{cases} y_0 = u_0 + v_0 = (1+i) + (1-i) = 2, \\ y_1 = u_0\varepsilon + v_0\varepsilon^2 = (1+i)\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) + (1-i)\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = -1 - \sqrt{3}, \\ y_2 = u_0\varepsilon^2 + v_0\varepsilon = (1+i)\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) + (1-i)\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = -1 + \sqrt{3}. \end{cases}$$

Оскільки $x = y + 3$, то можна знайти корені заданого рівняння:

$$x_0 = y_0 + 3 = 5,$$
$$x_1 = y_1 + 3 = 2 - \sqrt{3},$$
$$x_2 = y_2 + 3 = 2 + \sqrt{3}.$$

2. Дослідження коренів кубічного рівняння з дійсними коефіцієнтами.

Нехай дано неповне кубічне рівняння

$$x^3 + px + q = 0 \qquad (2)$$

з дійсними коефіцієнтами. З'ясуємо, що можна сказати про корені цього рівняння. У цьому випадку вираз $D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$, що стоїть у формулі Кардано під знаком квадратного кореня, є дійсне число. Воно може бути додатним, дорівнювати нулю або бути від'ємним. Наступна теорема дає можливість визначити число дійсних і уявних коренів рівняння (2) залежно від знаку *D*.

Теорема. Нехай (2) – рівняння з дійсними коефіцієнтами і $D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$. Тоді:

1) якщо $D > 0$, то рівняння (2) має один дійсний корінь і два комплексні спряжені;

2) якщо $D = 0$, то всі корені рівняння дійсні, причому два з них рівні між собою;

3) якщо $D < 0$, то всі корені рівняння дійсні та різні.

Д о в е д е н н я. 1. Нехай $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 > 0$. Тоді – число дійсне, і в формулі Кардано під знаком кожного з кубічних коренів стоятиме дійсне число. Однак відомо, що кубічний корінь з дійсного числа має одне дійсне і два спряжені комплексні значення. Позначимо через u_0 дійсне значення радикала u. Тоді відповідне йому значення $v_0 = -\frac{p}{3u_0}$ теж буде дійсне, бо $p \in R$. Таким чином,

корінь $x_0 = u_0 + v_0$ рівняння (2) буде дійсним числом. Два інші корені цього рівняння знайдемо за формулами (9):

$$x_1 = u_0\varepsilon + u_0\varepsilon^2 = u_0\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) + v_0\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = -\frac{u_0 + v_0}{2} + i\sqrt{3}\,\frac{u_0 - v_0}{2},$$

$$x_2 = u_0\varepsilon^2 + v_0\varepsilon = u_0\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) + v_0\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = -\frac{u_0 + v_0}{2} - i\sqrt{3}\,\frac{u_0 - v_0}{2}.$$

Оскільки u_0 і v_0 є дійсні значення різних кубічних радикалів, то $u_0 \neq v_0$, тобто $\frac{u_0 - v_0}{2} \neq 0$ і, таким чином, корені x_1 і x_2 є спряженими комплексними числами.

Отже, якщо $D > 0$, то рівняння (2) має один дійсний і два комплексні спряжені корені.

2. Нехай $D = 0$. У цьому випадку

$$u = \sqrt[3]{-\frac{q}{2}} \quad \text{і} \quad v = \sqrt[3]{-\frac{q}{2}}.$$

Нехай u_0 – дійсне значення радикала u. Відповідне йому значення v_0 радикала v теж є дійсним числом, бо $u_0 v_0 = -\frac{p}{3}$. Оскільки $\sqrt[3]{-\frac{q}{2}}$ має лише одне дійсне значення, то $u_0 = v_0$. Тому

$x_0 = u_0 + v_0 = 2u_0$,

$$x_1 = u_0\varepsilon + v_0\varepsilon^2 = u_0\varepsilon + u_0\varepsilon^2 = u_0\left(\varepsilon + \varepsilon^2\right) = u_0\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i - \frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = -u_0,$$

$$x_2 = u_0\varepsilon^2 + v_0\varepsilon = u_0\varepsilon^2 + u_0\varepsilon = u_0\left(\varepsilon^2 + \varepsilon\right) = -u_0.$$

Отже, в цьому випадку всі корені рівняння (2) дійсні, причому два з них рівні між собою.

3. Нехай $D < 0$. Тоді $\sqrt{D}$ – число суто уявне, і у формулі Кардано під знаком кожного з кубічних коренів стоятимуть комплексні числа, а тому всі значення радикалів u і v будуть комплексними числами.

Покажемо, що в цьому випадку у формулі Кардано значення радикала v повинно бути спряжене відповідному значенню радикала u. Справді, нехай $u_0 = a + bi$ – будь-яке зі значень

радикала u, а v_0 – відповідне йому значення радикала v. Тоді відповідно до правила добування кореня n-го степеня

$$|u_0| = \left|\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}\right| = \sqrt[3]{\left|-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right|} =$$

$$= \sqrt[3]{\left|-\frac{q}{2}+i\sqrt{-\left(\frac{q}{2}\right)^2-\left(\frac{p}{3}\right)^3}\right|} = \sqrt[3]{\sqrt{\left(\frac{q}{2}\right)^2-\left(\frac{q}{2}\right)^2-\left(\frac{p}{3}\right)^3}} = \sqrt[3]{\sqrt{-\left(\frac{p}{3}\right)^3}} = \sqrt{-\frac{p}{3}}.$$

Зауважимо, що оскільки за умовою $\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3<0$, то коефіцієнт p повинен бути від'ємним.

Тому маємо:

$$v_0 = -\frac{p}{3u_0} = -\frac{p\overline{u_0}}{3u_0\overline{u_0}} = -\frac{p\overline{u_0}}{3|u_0|^2} = -\frac{p\overline{u_0}}{3\left(-\frac{p}{3}\right)} = \overline{u_0}, \text{ тобто } v_0 = a-bi.$$

Таким чином, за формулами (9)

$$x_0 = u_0+v_0 = (a+bi)+(a-bi) = 2a,$$

$$x_1 = u_0\varepsilon+v_0\varepsilon^2 = (a+bi)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)+(a-bi)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) = -a-b\sqrt{3},$$

$$x_2 = u_0\varepsilon^2+v_0\varepsilon = (a+bi)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)+(a-bi)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) = -a+b\sqrt{3}.$$

Отже, у цьому випадку рівняння (2) має три різні дійсні корені. Тим часом формула Кардано виражає ці корені через корені з комплексних чисел, причому можна довести, що їх ніяким способом не можна виразити через коефіцієнти за допомогою радикалів із дійсними підкореневими виразами. Тому розглядуваний випадок дістав назву ***незвідного***.

Останній випадок $(D<0)$ переконливо доводить, що практична цінність формули Кардано невелика. Бо хоч у цьому випадку всі корені рівняння з дійсними коефіцієнтами дійсні, проте відшукання їх за формулою Кардано вимагає добування кубічного кореня з комплексних чисел, для чого ці числа треба записувати в

тригонометричній формі. Отже, запис коренів кубічного рівняння за допомогою радикалів втрачає практичне значення.

Приклад 2. В прикладі 1 ми розглядали рівняння

$$y^3 - 6y + 4 = 0.$$

$D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = \left(\frac{4}{2}\right)^2 + \left(\frac{-6}{3}\right)^3 = 2^2 + (-2)^3 = 4 - 8 = -4 < 0$, тому ми мали незвідний випадок. Його корені $2, -1-\sqrt{3}, -1+\sqrt{3}$, тобто дійсні і різні.

Розглянемо рівняння $x^3 - 6x - 9 = 0$. Тут $p = -6, q = -9$, тому

$$D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = \left(\frac{9}{2}\right)^2 + (-2)^3 = \frac{81}{4} - \frac{32}{4} = \frac{49}{4} > 0,$$

тобто рівняння має один дійсний корінь і два спряжені комплексні корені. Тоді

$u = \sqrt[3]{\frac{9}{2} + \frac{7}{2}} = \sqrt[3]{8}$, $u_0 = 2$, $v_0 = -\frac{p}{3u_0} = -\frac{-6}{3 \cdot 2} = 1$. Тому коренями є:

$x_0 = u_0 + v_0 = 2 + 1 = 3;$

$x_1 = -\frac{u_0 + v_0}{2} + i\sqrt{3}\frac{u_0 - v_0}{2} = -\frac{3}{2} + \frac{\sqrt{3}}{2}i;$

$x_2 = -\frac{u_0 + v_0}{2} - i\sqrt{3}\frac{u_0 - v_0}{2} = -\frac{3}{2} - \frac{\sqrt{3}}{2}i.$

Розглянемо рівняння $x^3 - 12x + 16 = 0$. Тут $p = -12$, $q = 16$, тому $D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{2}\right)^3 = 8^2 + (-4)^3 = 2^6 - 2^6 = 0$, тобто корені дійсні, причому два з них рівні між собою. Тоді $u = \sqrt[3]{-\frac{q}{2}} = \sqrt[3]{-\frac{16}{2}} = \sqrt[3]{-8}$; $u_0 = -2$. Тому коренями є:

$x_0 = 2u_0 = -4;$

$x_1 = x_2 = -u_0 = 2.$

3. Рівняння четвертого степеня.

Перейдемо до розгляду рівняння четвертого степеня

$$a_4x^4+a_3x^3+a_2x^2+a_1x+a_0=0.$$

Якщо старший коефіцієнт a_4 даного рівняння відмінний від одиниці, то, поділивши обидві частини цього рівняння на a_4, отримаємо рівняння вигляду

$$x^4+ax^3+bx^2+cx+d=0, \qquad (10)$$

еквівалентне даному. Тут a,b,c,d – довільні комплексні числа. Найбільш ранній метод розв'язання рівняння (10) належить учневі Кардано Феррарі. Тому він і має назву **метод Феррарі**. Викладемо його.

Запишемо рівняння (10) у вигляді

$$x^4+ax^3=-bx^2-cx-d.$$

Виділимо у лівій частині повний квадрат. Для цього додамо до обидвох частин рівняння $\frac{a^2x^2}{4}$:

$$x^4+ax^3+\frac{a^2x^2}{4}=\frac{a^2x^2}{4}-bx^2-cx-d;$$

$$\left(x^2+\frac{ax}{2}\right)^2=\left(\frac{a^2}{4}-b\right)x^2-cx-d.$$

Додамо до обидвох частин суму $2\left(x^2+\frac{ax}{2}\right)\frac{y}{2}+\frac{y^2}{4}$, в лівій частині отримаємо повний квадрат:

$$\left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(x^2+\frac{ax}{2}\right)y+\frac{y^2}{4}+\left(\frac{a^2}{4}-b\right)x^2-cx-d;$$

$$\left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\left(\frac{y^2}{4}-d\right); \qquad (11)$$

$$\left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=Ax^2+Bx+C,$$

де $A=\frac{a^2}{4}-b+y,\quad B=\frac{ay}{2}-c,\ C=\frac{y^2}{4}-d.$

Тричлен справа залежить від параметра y. Підберемо параметр y так, щоб цей тричлен був повним квадратом. Для того, щоб

тричлен Ax^2+Bx+C був повним квадратом, достатньо, щоб $D=B^2-4AC=0$. При цьому отримаємо

$$Ax^2+Bx+C=Ax^2+2\sqrt{AC}x+C=\left(\sqrt{A}x+\sqrt{C}\right)^2.$$

Значить, у правій частині (11) треба підібрати y так, щоб виконувалася умова

$$\left(\frac{ay}{2}-c\right)^2-4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=0.$$

Розкриємо дужки і перегрупуємо доданки:

$$\frac{a^2y^2}{4}-acy+c^2-4\left(\frac{a^2y^2}{16}-\frac{b}{4}y^2+\frac{y^3}{4}-\frac{a^2d}{4}+bd-dy\right)=0;$$

$$\frac{a^2y^2}{4}-acy+c^2-\frac{a^2y^2}{4}+by^2-y^3+a^2d-4bd+4dy=0,\text{ тобто}$$

$$y^3-by^2+(ac-4d)y-\left(c^2+d\left(a^2-4b\right)\right)=0. \qquad (12)$$

Отже, при виконанні умови (12) права частина рівняння (11) буде повним квадратом, точніше квадратом деякого лінійного двочлена від x.

Допоміжне кубічне рівняння (12) називається **кубічною резольвентою** рівняння (10). Розв'язуючи його, знайдемо один з коренів y_0, і підставимо це значення y_0 в (11). Отримаємо:

$$\left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)^2=(mx+n)^2, \qquad (13)$$

де $$m=\sqrt{A}=\sqrt{\frac{a^2}{4}-b+y_0},\quad n=\sqrt{C}=\sqrt{\frac{y_0^2}{4}-d}\,.$$

Розв'язування рівняння (13) зводиться до розв'язування сукупності двох квадратних рівнянь:

$$\left[\begin{array}{l} x^2+\dfrac{ax}{2}+\dfrac{y_0}{2}=mx+n, \\ x^2+\dfrac{ax}{2}+\dfrac{y_0}{2}=-mx-n. \end{array}\right.$$

Розв'язавши ці рівняння, отримаємо всі чотири корені рівняння (10).

Приклад. Розв'язати рівняння: $x^4-2x^3+6x^2-2x+5=0$.

$$x^4 - 2x^3 = -6x^2 + 2x - 5;$$
$$\left(x^2 - x\right)^2 = -5x^2 + 2x - 5.$$

Доповнимо ліву частину цього рівняння до повного квадрата, ввівши параметр y:

$$\left(x^2 - x\right)^2 + 2y\left(x^2 - x\right) + y^2 = 2y\left(x^2 - x\right) - 5x^2 + 2x + y^2 - 5;$$
$$\left(x^2 - x + y\right)^2 = (2y - 5)x^2 + (2 - 2y)x + \left(y^2 - 5\right).$$

Виберемо y так, щоб у правій частині теж був повний квадрат. Для цього дискримінант повинен дорівнювати нулю:

$$(2 - 2y)^2 - 4(2y - 5)\left(y^2 - 5\right) = 0;$$
$$(1 - y)^2 - (2y - 5)\left(y^2 - 5\right) = 0;$$
$$1 - 2y + y^2 - 2y^3 + 5y^2 + 10y - 25 = 0;$$
$$y^3 - 3y^2 - 4y + 12 = 0;$$
$$y^2(y - 3) - 4(y - 3) = 0;$$
$$(y - 3)\left(y^2 - 4\right) = 0.$$

Одним з коренів останнього рівняння є $y = 3$. Маємо:

$$\left(x^2 - x + 3\right)^2 = x^2 - 4x + 4;$$
$$\left(x^2 - x + 3\right)^2 = (x - 2)^2.$$

$$\left[\begin{array}{l} x^2 - x + 3 = x - 2, \\ x^2 - x + 3 = -x + 2 \end{array}\right. \Rightarrow \left[\begin{array}{l} x^2 - 2x + 5 = 0, \\ x^2 + 1 = 0 \end{array}\right. \Rightarrow \left[\begin{array}{l} x_{1,2} = 1 \pm 2i, \\ x_{3,4} = \pm i. \end{array}\right.$$

Питання для самоконтролю

1. Яку заміну змінної треба виконати, щоб звести кубічне рівняння до неповного кубічного рівняння?
5. Виведіть формулу Кардано для коренів неповного кубічного рівняння.
6. Які корені має неповне кубічне рівняння з дійсними коефіцієнтами залежно від знаку дискримінанта?
7. У чому полягає метод Феррарі розв’язування рівнянь четвертого степеня?

Розділ IV. МНОГОЧЛЕНИ НАД ПОЛЕМ РАЦІОНАЛЬНИХ ЧИСЕЛ І АЛГЕБРАЇЧНІ ЧИСЛА

Тема 12. Цілі і раціональні корені многочлена з цілими коефіцієнтами. Критерій незвідності Ейзенштейна

Якщо многочлен $f(x)$ над полем Q або, що те саме, рівняння

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \qquad (1)$$

з раціональними коефіцієнтами має раціональні корені, то в багатьох випадках ці корені можна знайти за допомогою цілком елементарних способів. Зокрема, знаючи один його корінь α, можна спростити дане рівняння, звівши його до рівняння $(n-1)$-го степеня діленням на $x-\alpha$. Діючи аналогічно, можна далі понизити степінь многочлена $f(x)$.

Зауважимо також, що будь-яке алгебраїчне рівняння з раціональними коефіцієнтами множенням на спільний знаменник усіх коефіцієнтів можна звести до рівняння з цілими коефіцієнтами. Тому вважатимемо коефіцієнти рівняння (1) цілими числами.

Розглянемо елементарні способи знаходження раціональних коренів рівняння (1). Основне практичне значення для цього питання має така теорема.

Теорема 1. Для того, щоб число $\frac{p}{q}$, де $(p,q)=1$, було коренем рівняння (1) з цілими коефіцієнтами, необхідно, щоб p було дільником вільного члена a_0, а q – дільником старшого коефіцієнта a_n цього рівняння.

Д о в е д е н н я. Нехай $\frac{p}{q}$ є коренем рівняння (1). Тоді

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0 \quad \Big| \times q^n$$

або

$$a_n p^n + a_{n-1} q p^{n-1} + \ldots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Усі доданки, крім останнього, діляться на p, $0 \vdots p$, тому і $a_0 q^n \vdots p$. Але $(p,q)=1$, тому $(p,q^n)=1$, отже, $a_0 \vdots p$. Аналогічно, всі доданки, крім першого, діляться на q, тому $a_n p^n : q$, звідки $a_n \vdots q$. Теорему доведено.

Наслідок. Якщо старший коефіцієнт рівняння з цілими коефіцієнтами дорівнює 1, то всі раціональні корені цього рівняння є цілі числа і дільники вільного члена.

Приклад 1. Рівняння $2x^3+3x^2+6x-4=0$ може мати раціональними коренями лише такі числа:

$$\pm 1,\ \pm 2,\ \pm 4,\ \pm\frac{1}{2}.$$

Підставляючи їх у рівняння, визначаємо, які з них є коренями. При цьому зручно користуватися схемою Горнера, наприклад:

	2	3	6	–4
1	2	5	11	7
…	…	…	…	…
$\frac{1}{2}$	2	4	8	0

Отже, $\frac{1}{2}$ є коренем, тобто $2x^3+3x^2+6x-4=(x-\frac{1}{2})(2x^2+4x+8)=0$.

На практиці частіше користуються наслідком з теореми 1. Бо кожне рівняння з цілими коефіцієнтами можна звести до рівняння з цілими коефіцієнтами, в якому старший коефіцієнт дорівнює 1, тобто до зведеного рівняння. Для цього треба помножити рівняння (1) на a_n^{n-1} і зробити заміну $a_n x = y$.

Приклад 2. Домножимо рівняння з прикладу 1 на 2^2:

$$(2x)^3+3(2x)^2+12(2x)-16=0;$$

заміна $2x=y$:

$$y^3+3y^2+12y-16=0.$$

За наслідком з теореми 1, раціональними коренями цього рівняння можуть бути лише цілі числа – дільники вільного члена $\pm 1,\ \pm 2,\ \pm 4,\ \pm 8,\ \pm 16$.

З цього прикладу видно, що при збільшенні степеня рівняння значно збільшується число перевірок – підставлянь у рівняння. Щоб зменшити число цих проб, використовують такі твердження.

Теорема 2. Для того, щоб $\frac{p}{q}$, де $(p,q)=1$, було раціональним коренем многочлена $f(x)$ з цілими коефіцієнтами, необхідно, щоб при довільному цілому k число $f(k)$ ділилося на $p-qk$ (якщо $p-qk\neq 0$).

Д о в е д е н н я. Поділимо $f(x)$ на $x-k$. За теоремою Безу:

$$f(x)=(x-k)(b_{n-1}x^{n-1}+\ldots+b_1x+b_0)+f(k), \qquad (2)$$

де усі коефіцієнти частки $b_{n-1},\ldots,b_1,b_0$ є цілими числами. За умовою теореми, $x=\frac{p}{q}$ – корінь $f(x)$, тому $f(\frac{p}{q})=0$. Підставимо в (2) $x=\frac{p}{q}$:

$$f\left(\frac{p}{q}\right)=\left(\frac{p}{q}-k\right)\left(b_{n-1}\left(\frac{p}{q}\right)^{n-1}+\ldots+b_1\left(\frac{p}{q}\right)+b_0\right)+f(k)=0,$$

звідси

$$-f(k)=\left(\frac{p}{q}-k\right)\left(b_{n-1}\left(\frac{p}{q}\right)^{n-1}+\ldots+b_1\left(\frac{p}{q}\right)+b_0\right).$$

Домножимо обидві частини на q^n:

$$-q^n f(k)=(p-qk)(b_{n-1}p^{n-1}+\ldots+b_1pq^{n-2}+b_0q^{n-1}).$$

Звідси видно, що $q^n f(k)$ ділиться на $p-qk$, якщо $p-qk\neq 0$.

Покажемо тепер, що $(q,p-qk)=1$. Якби q і $p-qk$ мали б спільний дільник α, $|\alpha|\neq 1$, то і $p=qk+(p-qk)$ мало б цей дільник, що неможливо, бо $(p,q)=1$. Отже, $(q,p-qk)=1$, тоді і $(q^n,p-qk)=1$. Оскільки $q^n f(k)\vdots(p-qk)$, то $f(x)$ ділиться на $p-qk$, що й треба було довести.

Наслідок. Якщо старший коефіцієнт a_n даного многочлена $f(x)$ з цілими коефіцієнтами дорівнює 1, то його раціональними коренями можуть бути лише такі цілі числа p, для яких $f(k)\vdots(p-k)$ для будь-якого цілого k $(p-k\neq 0)$.

На практиці теорема 2 найчастіше використовується для $k = \pm 1$, бо вирази $f(1)$ і $f(-1)$ легко обчислити. Тобто, щоб число $\frac{p}{q}$ було раціональним коренем многочлена з цілими коефіцієнтами, необхідно, щоб $\frac{f(1)}{p-q}$ і $\frac{f(-1)}{p+q}$ були цілими числами.

Перейдемо тепер до питання звідності і незвідності многочленів у полі раціональних чисел.

Відомо, що в кільці $C[x]$ звідним є довільний многочлен, степінь якого більший від одиниці; в кільці $R[x]$ – кожний многочлен, степінь якого перевищує 2. Основна відмінність многочленів над полем Q раціональних чисел від многочленів над полем R або полем C полягає в тому, що існують многочлени з раціональними коефіцієнтами як завгодно високого степеня, незвідні у полі раціональних чисел.

Означення. Многочлен $p(x)$ з цілими коефіцієнтами називається **примітивним**, якщо його коефіцієнти не мають спільних дільників, відмінних від ± 1 (тобто якщо НСД всіх його коефіцієнтів дорівнює 1).

Наприклад, многочлен з прикладу 1 є примітивним, а многочлен $2x^4 + 4x^3 - 6x^2 - 12$ не є примітивним.

Справедливе таке твердження.

Лема. Добуток двох примітивних многочленів є примітивним многочленом.

Розглянемо тепер питання про звідність многочлена з цілими коефіцієнтами в полі раціональних чисел.

Теорема 3. Для того, щоб многочлен $f(x)$ з цілими коефіцієнтами був звідним у полі Q, необхідно і досить, щоб він був звідним у кільці Z цілих чисел, тобто щоб існували многочлени $f_1(x)$ і $f_2(x)$ ненульового степеня з цілими коефіцієнтами такі, що $f(x) = f_1(x) \cdot f_2(x)$.

Д о в е д е н н я. *Необхідність.* Нехай дано многочлен з цілими коефіцієнтами $f(x)$, звідний у полі Q, то $f(x)=g_1(x)\cdot g_2(x)$, де $g_1(x)$, $g_2(x)$ – многочлени ненульового степеня з раціональними коефіцієнтами. Потрібно довести, що існують многочлени ненульового степеня f_1 і f_1 з цілими коефіцієнтами, добуток яких дорівнює $f(x)$.

Зведемо коефіцієнти многочлена $g_1(x)$ до спільного знаменника і винесемо цей знаменник за дужки, отримаємо:

$$g_1(x)=\frac{\alpha}{\beta}S_1(x),$$

де $S_1(x)$ – многочлен з цілими коефіцієнтами, β – спільний знаменник коефіцієнтів $g_1(x)$, а α – НСД чисельників коефіцієнтів многочлена, що утворюється з $g_1(x)$ після зведення до спільного знаменника (наприклад, $\frac{2}{3}x+\frac{4}{5}=\frac{10}{15}x+\frac{12}{15}=\frac{2}{15}(5x+6)$). Очевидно, що $S_1(x)$ – примітивний многочлен. Вважатимемо, що дріб $\frac{\alpha}{\beta}$ нескоротний, тобто $(\alpha,\beta)=1$. Аналогічно для $g_2(x)$ маємо:

$$g_2(x)=\frac{\gamma}{\delta}S_2(x),$$

де $S_2(x)$ – примітивний многочлен, а $(\gamma,\delta)=1$. Отже,

$$f(x)=\frac{\alpha\gamma}{\beta\delta}S_1(x)S_2(x)=\frac{\alpha\gamma}{\beta\delta}S(x),\quad S(x)=S_1(x)S_2(x).$$

Доведемо, що $\frac{\alpha\gamma}{\beta\delta}=m$ є ціле число. Від супротивного: припустимо, що $\frac{\alpha\gamma}{\beta\delta}=\frac{p}{q}$, де $(p,q)=1$. Многочлен $S(x)$, за сформульованою лемою, є примітивним. Нехай C_k – якийсь коефіцієнт $S(x)$. Оскільки $f(x)=\frac{p}{q}S(x)$ має цілі коефіцієнти, то добуток $\frac{p}{q}C_k$ має бути цілим числом при будь-якому k. Але $(p,q)=1$, тоді $C_k \vdots q$. Оскільки те саме повинно справджуватись для

всіх коефіцієнтів C_k, дістанемо суперечність з тим, що $S(x)$ примітивний многочлен. Отже, $\frac{\alpha\gamma}{\beta\delta} = m \in Z$.

Візьмемо $f_1(x) = mS_1(x)$, $f_2(x) = S_2(x)$, отримаємо $f(x) = f_1(x) \cdot f_2(x)$, де f_1, f_2 – многочлен ненульового степеня з цілими коефіцієнтами.

Достатність. Якщо $f(x)$ звідний у кільці $Z[x]$, то він тим більше звідний у кільці $Q[x]$, бо $Z \subset Q$, тобто кожний многочлен з цілими коефіцієнтами є многочленом над полем раціональних чисел.

Теорему доведено.

Отже, теорема 3 повністю зводить питання про звідність многочленів у полі Q до звідності многочленів у кільці Z.

Теорема 4 (Критерій незвідності Ейзенштейна). Якщо в многочлені з цілими коефіцієнтами

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

коефіцієнти $a_0, a_1, \ldots, a_{n-1}$ діляться на деяке просте число p, причому a_0 не ділиться на p^2, а старший коефіцієнт a_n не ділиться на p, то многочлен $f(x)$ незвідний у полі раціональних чисел.

Д о в е д е н н я. Згідно з теоремою 3, досить показати, що $f(x)$ при цих умовах не може бути добутком двох многочленів ненульового степеня з цілими коефіцієнтами. Припустимо супротивне, тобто що

$$f(x) = (b_r x^r + b_{r-1} x^{r-1} + \ldots + b_1 x + b_0)(c_s x^s + c_{s-1} x^{s-1} + \ldots + c_1 x + c_0) \quad (r + s = n).$$

Припустивши, що $r \geq s$ і використавши умову рівності двох многочленів, отримаємо:

$$\begin{aligned} a_0 &= b_0 c_0 \\ a_1 &= b_1 c_0 + b_0 c_1 \\ a_2 &= b_2 c_0 + b_1 c_1 + b_0 c_2 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ a_n &= b_r c_s . \end{aligned} \qquad (3)$$

За умовою, $a_0 \vdots p$, але $\overline{a_0 \vdots p^2}$, тобто $b_0 c_0 \vdots p$, але $\overline{b_0 c_0 \vdots p^2}$. Отже, на p ділиться лише одне з чисел b_0 або c_0. Нехай, наприклад, $b_0 \vdots p$, $\overline{c_0 \vdots p}$. Тоді з другої рівності системи (3) отримаємо, що $b_1 \vdots p$ (бо $a_1 \vdots p$ за умовою, а $\overline{c_0 \vdots p}$). З третьої рівності видно, що $b_2 \vdots p$. Так можна показати, що всі коефіцієнти $b_0, b_1, b_2, ..., b_r$ діляться на p. А це неможливо, бо тоді й $a_n \vdots p$ (це випливає з останньої рівності (3)), що суперечить умові теореми. Теорему доведено.

Приклад. Многочлен $f(x) = 3x^4 + 2x^3 - 4x^2 + 2x + 6$ незвідний у полі Q, бо коефіцієнти 2,–4,2,6 діляться на 2, $\overline{6 \vdots 2^2}$, $\overline{3 \vdots 2}$. Тут $p = 2$.

З теореми 4 випливає важливий **наслідок:**

У кільці многочленів над полем раціональних чисел є многочлени довільного степеня, незвідні у полі Q.

Зокрема, при $\forall n \in N$ і простому p многочлен $f(x) = x^n + p$ незвідний у полі Q. Такі многочлени можна побудувати багатьма способами.

Теорема 4 дає *достатню* умову незвідності многочлена в полі Q. Можна дати і *необхідну* умову звідності многочлена у полі Q, а саме:

Теорема 5. Якщо многочлен $f(x)$ з раціональними коефіцієнтами, степінь якого більший за одиницю, має хоча б один раціональний корінь r, то $f(x)$ звідний у полі раціональних чисел.

Д о в е д е н н я. За наслідком з теореми Безу, $f(x) \vdots (x - r)$, тобто $f(x) = (x - r) f_1(x)$, причому $f_1(x)$ – многочлен ненульового степеня над тим самим полем Q. Теорему доведено.

Твердження, обернене до теореми 5, неправильне: многочлен $f(x)$ може не мати жодного раціонального кореня, але бути звідним у полі Q. Наприклад, $f(x) = x^4 - 4$ звідний у полі Q, бо $f(x) = (x^2 - 2)(x^2 + 2)$, але раціональних коренів не має.

Проте у випадку многочлена третього степеня обернена теорема справедлива:

Теорема 6. Якщо многочлен $f(x)$ третього степеня з раціональними коефіцієнтами звідний у полі Q, то він має хоча б один раціональний корінь.

Д о в е д е н н я. Припустимо, що $f(x)$ – звідний, тобто $f(x) = f_1(x) f_2(x)$, де $f_1(x), f_2(x) \in Q[x]$ – многочлени ненульового степеня. Оскільки $\deg f_1 + \deg f_2 = 3$, то $\deg f_1 = 1$, $\deg f_2 = 2$ або навпаки. Нехай $f_1(x) = ax + b$. Але тоді число $x_0 = -\frac{b}{a}$ є раціональним коренем многочлена $f_1(x)$, а тому й многочлена $f(x)$. Отже, $f(x)$ має хоча б один раціональний корінь. Теорему доведено.

Теорему 6 можна сформулювати і так: якщо многочлен $f(x)$ третього степеня з раціональними коефіцієнтами не має раціональних коренів, то він незвідний у полі Q.

Питання для самоконтролю

1. Як алгебраїчне рівняння з раціональними коефіцієнтами звести до рівняння з цілими коефіцієнтами?
2. Сформулюйте необхідні умови того, щоб число $\frac{p}{q}$, де $(p,q)=1$, було коренем алгебраїчного рівняння з цілими коефіцієнтами.
3. Сформулюйте необхідну і достатню умову того, щоб многочлен $f(x)$ з цілими коефіцієнтами був звідним у полі раціональних чисел.
4. Сформулюйте критерій незвідності Ейзенштейна.
5. Сформулюйте необхідну умову звідності многочлена у полі раціональних чисел.

Тема 13. Алгебраїчні і трансцендентні числа. Просте алгебраїчне розширення поля. Знищення алгебраїчної ірраціональності в знаменнику дробу

Означення. Число називається **алгебраїчним**, якщо воно є коренем деякого многочлена з раціональними коефіцієнтами.

Очевидно, кожне раціональне число r алгебраїчне, бо його можна розглядати як корінь многочлена $f(x) = x - r$ з раціональними коефіцієнтами. Ірраціональні числа теж можуть бути алгебраїчними, наприклад, $\sqrt{2}$ – алгебраїчне, бо є коренем многочлена $x^2 - 2$, $\sqrt[3]{7}$ – алгебраїчне, бо є коренем многочлена $x^3 - 7$ над полем Q.

Але не всі ірраціональні числа алгебраїчні. Існує безліч ірраціональних чисел, які не є коренями жодного многочлена над полем Q. Такі числа називаються **трансцендентними**. Наприклад, числа $\pi, \lg 2, 2^{\sqrt{2}}$ – **трансцендентні**.

Узагальнимо дані означення.

Означення. Число α називається **алгебраїчним** відносно числового поля P, якщо воно є коренем деякого многочлена над полем P. Число, яке не є алгебраїчним відносно поля P, називають **трансцендентним** відносно P.

Якщо α є алгебраїчним числом відносно поля P, то в кільці $P[x]$ існує єдиний незвідний зведений многочлен

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

який має α своїм коренем, а його степінь n є найменшим серед степенів усіх многочленів з коренем α. При цьому многочлен $f(x)$ називають **мінімальним многочленом** числа α, а його степінь n – **степенем алгебраїчного числа** α відносно поля P.

Означення. Мінімальне розширення поля P, яке містить число $\alpha \notin P$, називають **простим розширенням поля** P, утвореним приєднанням числа α, і позначають через $P(\alpha)$.

Простими розширеннями називають розширення, утворені приєднанням одного числа.

Якщо α є алгебраїчним числом відносно поля P, то поле $P(\alpha)$, утворене приєднанням до поля P числа α, називається **простим алгебраїчним розширенням** поля P.

Наприклад, поле чисел вигляду $a+b\sqrt{2}, a,b \in Q$, є простим алгебраїчним розширенням поля раціональних чисел, утвореним приєднанням числа $\sqrt{2} \notin Q$.

Будова простого алгебраїчного розширення характеризується такою теоремою.

Теорема (про будову простого алгебраїчного розширення поля).

Поле $P(\alpha)$, утворене з поля P приєднанням кореня α незвідного у полі P многочлена n-го степеня

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \qquad (1)$$

складається з усіх чисел вигляду

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}, \qquad (2)$$

де $c_0, c_1, c_2, \ldots, c_{n-1}$ – довільні числа з поля P.

Д о в е д е н н я. Позначимо через P_1 множину чисел вигляду (2) і покажемо, що P_1 – поле. Очевидно, що сума і різниця чисел вигляду (2) належать до P_1. Розглянемо добуток і частку таких чисел.

Число вигляду (2) можна розглядати як результат підстановки α замість x у деякий многочлен $q(x)$ над полем P не вище (n-1)-го степеня:

$$\beta = q(\alpha).$$

Нехай маємо два числа $\beta_1 = q_1(\alpha)$, $\beta_2 = q_2(\alpha)$. Тоді добуток $\beta_1 \cdot \beta_2 = q_1(\alpha) \cdot q_2(\alpha) = q(\alpha)$, де $q(x)$ – многочлен, степінь якого вже може перевищувати n–1. Поділимо $q(x)$ на $f(x)$ з остачею:

$$q(x) = f(x)\varphi(x) + r(x), \qquad (3)$$

де степінь остачі $r(x)$ менший за степінь многочлена $f(x)$, тобто не перевищує n–1. Підставимо α в тотожність (3):

$$q(\alpha) = f(\alpha)\varphi(\alpha) + r(\alpha) = r(\alpha),$$

оскільки α – корінь $f(x)$, і тому $f(\alpha) = 0$. Отже, маємо:

$$\beta_1 \cdot \beta_2 = r(\alpha),$$

тобто добуток чисел β_1 і β_2 є числом вигляду (2), бо $r(x)$ – многочлен, степінь якого не перевищує n–1.

Перейдемо до розгляду частки. Досить показати, що для будь-якого числа $\beta = q(\alpha) \neq 0$ вигляду (2) $\frac{1}{\beta}$ теж буде числом вигляду (2). Оскільки $f(x)$ – незвідний у полі P многочлен, то многочлен $q(x)$ або взаємно простий з $f(x)$, або ділиться на $f(x)$. Але $\deg q < \deg f$, тому $\overline{q \vdots f}$, і тому многочлени $f(x)$ і $q(x)$ взаємно прості. Отже, існує єдина пара многочленів $\varphi_1(x)$ і $\varphi_2(x)$ таких, що справджується рівність $f(x) \cdot \varphi_1(x) + q(x) \cdot \varphi_2(x) = 1$.

Покладемо в останній рівності $x = \alpha$ і, враховуючи, що $f(\alpha) = 0$, отримаємо $q(\alpha) \cdot \varphi_2(\alpha) = 1$, тобто $\beta \cdot \varphi_2(\alpha) = 1$. Отже, $\frac{1}{\beta} = \varphi_2(\alpha)$. Якщо многочлен $\varphi_2(x)$ має степінь, менший за n, то твердження доведено. Якщо ж $\varphi_2(x)$ має степінь, не менший за n, то ділимо $\varphi_2(x)$ на многочлен $f(x)$ з остачею, тобто $\varphi_2(x) = f(x) \cdot \varphi(x) + r(x)$, звідки $\varphi_2(\alpha) = r(\alpha) = \frac{1}{\beta}$, причому степінь $r(x)$ менший за степінь $f(x)$. Отже, $\frac{1}{\beta}$ є числом вигляду (2), тобто належить до P_1.

Таким чином, P_1 утворює поле.

Залишається довести, що $P_1 = P(\alpha)$. Оскільки P_1 містить як поле P, так і число α, то воно містить і $P(\alpha)$, тобто $P_1 \supseteq P(\alpha)$. З іншого боку, будь-яке поле, яке включає α і поле P, повинно включати і всі числа вигляду (2), які утворюються з чисел поля P і числа α за допомогою дій множення і додавання, тобто $P(\alpha) \supseteq P_1$. Із встановлених співвідношень випливає, що $P_1 = P(\alpha)$. Теорему доведено.

Наслідок. Якщо α – корінь многочлена другого степеня над полем P

$$f(x) = x^2 + px + q,$$

причому $\alpha \notin P$, то просте алгебраїчне розширення $P(\alpha)$ поля P, утворене приєднанням числа α, складається з усіх чисел вигляду $a + b\alpha$, де $a, b \in P$.

Приклади.

1. Поле $Q(\sqrt{2})$ утворюється приєднанням до поля Q кореня $\sqrt{2}$ незвідного у полі Q многочлена другого степеня $f(x) = x^2 - 2$. Елементи поля $Q(\sqrt{2})$ мають вигляд $a + b\sqrt{2}$, де $a, b \in Q$.

2. Поле $Q(\sqrt[3]{2})$ утворюється приєднанням до поля Q кореня $\sqrt[3]{2}$ незвідного у полі Q многочлена третього степеня $f(x) = x^3 - 2$. Елементи поля $Q(\sqrt[3]{2})$ мають вигляд $c_0 + c_1\sqrt[3]{2} + c_2\sqrt[3]{2^2}$, де $c_0, c_1, c_2 \in Q$.

3. Поле C утворюється приєднанням до поля R кореня i незвідного у полі R многочлена $f(x) = x^2 + 1$. З доведеної теореми випливає, що всі елементи поля C мають вигляд $a + bi$, де $a, b \in R$.

Означення. Якщо корінь α квадратного тричлена над полем P не належить полю P, то просте алгебраїчне розширення $P(\alpha)$, утворене з поля P приєднанням до нього числа α, називається **квадратичним розширенням** поля P.

Поле $Q(\sqrt{2})$ є, очевидно, квадратичним розширенням поля Q.

Перейдемо до питання знищення ірраціональності в знаменнику дробу.

Нехай дано дріб $\frac{p(\alpha)}{q(\alpha)}$, де $p(x), q(x)$ – многочлени над полем Q, а α – ірраціональний корінь незвідного многочлена $f(x)$ вигляду (1) з раціональними коефіцієнтами. При цьому, звичайно, $q(\alpha) \neq 0$. Щоб позбутися ірраціональності в знаменнику, використаємо доведення теореми про будову простого алгебраїчного розширення поля.

Якщо $\deg q \geq n$, то ділимо $q(x)$ на $f(x)$ з остачею:

$$q(x) = f(x)s(x) + r(x).$$

Підставимо значення $x = \alpha$:

$$q(\alpha) = r(\alpha).$$

Тому $\frac{p(\alpha)}{q(\alpha)} = \frac{p(\alpha)}{r(\alpha)}$, де $\deg r < \deg f$. Отже, завжди можна вважати степінь знаменника заданого дробу меншим за n. Але тоді зрозуміло, що $q(x)$ і $f(x)-$ взаємно прості, бо $f(x)$ – незвідний многочлен.

Нехай $\varphi_1(x)$ і $\varphi_2(x)$ – такі многочлени над Q, що справджується рівність

$$f(x)\cdot\varphi_1(x)+q(x)\cdot\varphi_2(x)=1. \qquad (4)$$

Тоді $\frac{1}{q(\alpha)} = \varphi_2(\alpha)$ і

$$\frac{p(\alpha)}{q(\alpha)} = p(\alpha)\varphi_2(\alpha). \qquad (5)$$

Таким чином, щоб знищити ірраціональність у знаменнику дробу $\frac{p(\alpha)}{q(\alpha)}$, де α – корінь незвідного многочлена $f(x)$, потрібно виконати такі дії:

1. Якщо $\deg q \ge n$, то замінити $q(\alpha)$ числом $r(\alpha)$, де $r(x)$ – остача від ділення $q(x)$ на $f(x)$.

2. Знайти многочлени $\varphi_1(x)$ і $\varphi_2(x)$, які задовольняють рівність (4).

3. Обчислити $\varphi_2(\alpha)$ і записати дріб $\frac{p(\alpha)}{q(\alpha)}$ за формулою (5).

Приклад. Позбутися від ірраціональності в знаменнику дробу $\frac{4+\sqrt[3]{2}}{2-\sqrt[3]{2}}$.

Тут $f(x)=x^3-2$, $p(x)=x+4$, $q(x)=-x+2$, $\deg q < \deg f$. Знаходимо $\varphi_1(x)$ і $\varphi_2(x)$ такі, що

$$\varphi_1(x)(x^3-2)+\varphi_2(x)(-x+2)=1.$$

Для їх знаходження потрібно для многочленів $f(x)=x^3-2$ і $q(x)=-x+2$ записати алгоритм Евкліда:

$$x^3-2=(-x+2)(-x^2-2x-4)+6;$$
$$(x^3-2)-(-x+2)(-x^2-2x-4)=6;$$
$$(x^3-2)+(-x+2)(x^2+2x+4)=6;$$
$$\frac{1}{6}\left(x^3-2\right)+\left(\frac{1}{6}x^2+\frac{1}{3}x+\frac{2}{3}\right)(-x+2)=1.$$

Отримаємо

$$\varphi_1(x)=\frac{1}{6},\quad \varphi_2(x)=\frac{1}{6}x^2+\frac{1}{3}x+\frac{2}{3}.$$

Тоді за формулою (5) маємо:

$$\frac{4+\sqrt[3]{2}}{2-\sqrt[3]{2}}=\left(\sqrt[3]{2}+4\right)\left(\frac{1}{6}\sqrt[3]{2^2}+\frac{1}{3}\sqrt[3]{2}+\frac{2}{3}\right)=\sqrt[3]{4}+2\sqrt[3]{2}+3.$$

Питання для самоконтролю

1. Сформулюйте означення алгебраїчного і трансцендентного чисел.
2. Сформулюйте означення алгебраїчного і трансцендентного чисел відносно числового поля P.
3. Що означає, що многочлен $f(x)$ є мінімальним многочленом алгебраїчного відносно поля P числа α?
4. Дайте означення простого розширенням поля P, утвореного приєднанням числа α.
5. Дайте означення простого алгебраїчного розширенням поля P.
6. Сформулюйте теорему про будову простого алгебраїчного розширення поля.
7. Дайте означення квадратичного розширенням поля P.
8. Як знищити ірраціональність у знаменнику дробу $\frac{p(\alpha)}{q(\alpha)}$, де α – ірраціональний корінь незвідного многочлена $f(x)$ з раціональними коефіцієнтами?

Тема 14. Скінченні розширення полів. Складне алгебраїчне розширення поля. Поле алгебраїчних чисел та його алгебраїчна замкненість

Нехай F – деяке підполе поля P. Тоді P можна розглядати як векторний простір над полем F. Елементами цього простору є числа з поля P, а операціями – додавання елементів поля P і множення їх на числа з поля F.

Означення 1. Розширення P поля F називається **скінченним**, якщо P, як векторний простір над F, має скінченну розмірність.

При цьому розмірність простору P називають **степенем розширення** P над полем F і позначають символом $(P:F)$.

Можна дати інше означення скінченного розширення поля.

Означення 1'. Розширення P поля F називається **скінченним,** якщо в полі P існує така лінійно незалежна система елементів $\alpha_1,\alpha_2,...,\alpha_n$, що будь-який елемент $\beta \in P$ є лінійною комбінацією цих елементів з коефіцієнтами з поля F:

$$\beta = \lambda_1\alpha_1 + \lambda_2\alpha_2 + ... + \lambda_n\alpha_n .$$

Система елементів $\alpha_1,\alpha_2,...,\alpha_n$ називається **базисом** поля P відносно поля F. Кількість елементів базису називається степенем розширення поля P над полем F.

Приклад. Поле $Q(\sqrt{2}) = \{a + b\sqrt{2},\ a,b \in Q\}$ є скінченним розширенням поля Q степеня 2, тобто $(Q(\sqrt{2}):Q) = 2$, бо існує базис поля $Q(\sqrt{2})$ відносно поля Q, який складається з двох елементів. За базис можна взяти числа 1 і $\sqrt{2}$. Система цих елементів є лінійно незалежною. Покажемо це. Нехай $\lambda_1,\lambda_2 \in Q$. Запишемо рівність $\lambda_1 \cdot 1 + \lambda_2 \cdot \sqrt{2} = 0$. Припустимо, що $\lambda_1 \neq 0, \lambda_2 \neq 0$ (випадок, коли одне з λ_1,λ_2 дорівнює, а друге не дорівнює нулю, неможливий, бо тоді і $\lambda_1 = 0$, і $\lambda_2 = 0$). Тоді $\sqrt{2} = -\dfrac{\lambda_1}{\lambda_2}$, тобто $\sqrt{2} \in Q$, що неможливо. Отже, $\lambda_1 = \lambda_2 = 0$, а система елементів 1 і $\sqrt{2}$ лінійно незалежна.

Зауважимо, що не кожне розширення поля є скінченним. Так, поле R є розширенням поля Q, але це розширення не є скінченним.

Означення 2. Розширення P поля F, утворене за допомогою кількох послідовно виконаних простих алгебраїчних розширень, називається **складним алгебраїчним розширенням** поля F.

Означенн 2'. P є складним алгебраїчним розширенням поля F, якщо існує такий ланцюжок розширень

$$F \subseteq F_1 \subseteq F_2 \subseteq ... \subseteq F_k = P,$$

що $F_1 = F(\alpha_1), F_2 = F_1(\alpha_2),...,F_k = F_{k-1}(\alpha_k)$ причому кожне α_i є алгебраїчним числом над полем F_{i-1} (при $i=1$ $F_{i-1} = F$).

Складне алгебраїчне розширення поля F позначатимемо символом $F(\alpha_1)(\alpha_2)...(\alpha_k)$.

Складне алгебраїчне розширення можна розглядати як узагальнення простого алгебраїчного розширення.

Означення 3. Розширення P поля називається **алгебраїчним**, якщо всі його елементи є алгебраїчними відносно поля F.

З'ясуємо співвідношення між різними типами розширень числових полів.

Теорема 1. Просте алгебраїчне розширення $P(\alpha)$, утворене з P приєднанням алгебраїчного відносно P числа α, є скінченним розширенням поля P. Степінь розширення $P(\alpha)$ над полем P дорівнює степеню числа α відносно P.

Д о в е д е н н я. За теоремою про будову простого алгебраїчного розширення поля, довільне число $\beta \in P(\alpha)$ можна подати у вигляді

$$\beta = c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}, \quad c_i \in P, \quad i = 0,...,n-1.$$

Покажемо, що сукупність чисел $1, \alpha, ..., \alpha^{n-1}$ є лінійно незалежною системою елементів відносно поля P. Запишемо рівність

$$\lambda_0 \cdot 1 + \lambda_1 \cdot \alpha + ... + \lambda_{n-1} \cdot \alpha^{n-1} = 0, \quad \lambda_i \in P.$$

Якщо ця рівність справджується, коли не всі λ_i дорівнюють нулю, то це означає, що α є коренем деякого многочлена $\varphi(x) = \lambda_0 + \lambda_1 x + ... + \lambda_{n-1}x^{n-1}$ з коефіцієнтами з поля P, степінь якого не

перевищує $n-1$. Але це неможливо, бо, як відомо, многочлен $f(x)$ степеня n є мінімальним многочленом числа α.

Отже, сукупність елементів $1,\alpha,...,\alpha^{n-1}$ є базисом поля $P(\alpha)$ відносно поля P, і тому $P(\alpha)$ є скінченним розширенням поля P степеня n, тобто $(P(\alpha):P)=n$. Теорему доведено.

Теорема 2. Складне алгебраїчне розширення $P(\alpha_1)(\alpha_2)...(\alpha_k)$ є скінченним розширенням поля P. Степінь цього розширення дорівнює добутку степенів усіх послідовних простих розширень.

Д о в е д е н н я цієї теореми впливає з теореми 1 і такої **леми**: якщо P_2 – скінченне розширення поля P_1, а P_1 – скінченне розширення поля P, то P_2 – скінченне розширення поля P, причому $(P_2:P)=(P_2:P_1)\cdot(P_1:P)$.

Теорема 3. Будь-яке скінченне розширення поля є його алгебраїчним розширенням.

Д о в е д е н н я. Нехай P_1 – скінченне розширення n-го степеня поля P, тобто n – розмірність P_1 над P. Отже, будь-які $n+1$ елементів у полі P_1 є лінійно залежними відносно P, зокрема $1,\alpha,\alpha^2,...,\alpha^n$, де α – довільний елемент з P_1. Це означає, що в P існують такі елементи $\lambda_0,\lambda_1,...,\lambda_n$, не всі рівні нулю, що

$$\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+...+\lambda_n\alpha^n=0.$$

Отже, α є коренем деякого многочлена $f(x)=\lambda_n x^n+...+\lambda_1 x+\lambda_0$ з коефіцієнтами з поля P, тобто є алгебраїчним числом відносно поля P. Теорему доведено.

Теореми 1–3 дають змогу прийти до такого ***висновку***. Кожне просте або складне алгебраїчне розширення числового поля P є алгебраїчним розширенням цього поля.

Справедливі також такі твердження.

Теорема 4. Розширення $P(\alpha_1,\alpha_2,...,\alpha_k)$, утворене з P одночасним приєднанням алгебраїчних відносно P чисел $\alpha_1,\alpha_2,...,\alpha_k$, збігається зі складним алгебраїчним розширенням $P(\alpha_1)(\alpha_2)...(\alpha_k)$.

Теорема 5. Будь-яке скінченне розширення поля P є складним алгебраїчним розширенням цього поля.

Теорема 6. Будь-яке складне алгебраїчне розширення $P(\alpha_1)(\alpha_2)...(\alpha_k)$ поля P є простим розширенням цього поля, тобто існує таке число ω, алгебраїчне відносно P, що $P(\alpha_1)(\alpha_2)...(\alpha_k) = P(\omega)$.

З теорем 5 і 6 випливає, що скінченне розширення поля P є не тільки алгебраїчним, але й простим алгебраїчним розширенням P.

Таким чином, поняття простого і складного алгебраїчних розширень, скінченного розширення, по суті, збігаються. Різні за способом побудови, всі вони становлять ту саму алгебраїчну структуру.

Що ж до алгебраїчних розширень, то виявляється, що існують алгебраїчні розширення, які не є скінченними (а тому й простими або складними). До розгляду цього питання і перейдемо.

Розглянемо сукупність $A(P)$ усіх алгебраїчних чисел відносно поля P, тобто множину коренів усіх многочленів з $P[x]$.

Теорема 7. Сукупність $A(P)$ алгебраїчних чисел відносно поля P є поле.

Д о в е д е н н я. Досить показати, що $\forall \xi, \eta \in A(P)$ $\xi + \eta, \xi \cdot \eta, -\xi, \frac{1}{\xi} \in A(P)$ і що $0 \in A(P)$, $1 \in A(P)$. Останній факт випливає з того, що

$$Q \subseteq P \subseteq A(P).$$

Нехай тепер $\xi \in A(P), \eta \in A(P)$. Розглянемо розширення $P(\xi, \eta)$. За теоремою 4, $P(\xi, \eta) = P(\xi)(\eta)$; а за теоремами 2 і 3, таке розширення є алгебраїчне, а тому кожне число з нього належить $A(P)$. Зокрема, числа $\xi + \eta, \xi \cdot \eta, -\xi, \frac{1}{\xi}$, які належать $P(\xi, \eta)$, належать і $A(P)$. Теорему доведено.

Наслідок. Множина A усіх алгебраїчних чисел (тобто $A = A(Q)$) є поле.

Очевидно, що $A(P)$ є алгебраїчне розширення поля P. Можна показати, що в загальному випадку це розширення не є скінченним. Тобто існують алгебраїчні розширення полів, які не є скінченними. Але це не означає, що будь-яка розширення $A(P)$ є нескінченним.

Як відомо, поле C алгебраїчно замкнуте, тобто всі алгебраїчні числа над ним належать самому полю C: $A(C) = C$. Виявляється, що цю властивість має сукупність $A(P)$ алгебраїчних чисел над довільним числовим полем P: $A[A(P)] = A(P)$.

Теорема 8. Поле алгебраїчних чисел $A(P)$ над довільним числовим полем P алгебраїчно замкнуте.

Д о в е д е н н я. Нехай $A[A(P)] = F$. Потрібно показати, що $F = A(P)$. Оскільки включення $A(P) \subseteq A[A(P)]$ чи $A(P) \subseteq F$ очевидне, то досить показати, що $F \subseteq A(P)$, тобто $\forall \omega \in F \quad \omega \in A(P)$, тобто елемент ω алгебраїчний відносно P.

Якщо

$$g(x) = x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x + \alpha_0 \quad (\alpha_i \in A(P), i = 0,\ldots,n-1)$$

є мінімальний многочлен над $A(P)$ числа ω (такий многочлен існує, бо ω – алгебраїчне число відносно $A(P)$), то розглянемо розширення $P(\alpha_0, \alpha_1,\ldots,\alpha_{n-1})$ поля P. За раніше доведеним, $P(\alpha_0, \alpha_1,\ldots,\alpha_{n-1})$ – алгебраїчне розширення P, тобто будь-який його елемент, зокрема ω, алгебраїчний над P. Звідси $\omega \in A(P)$. Теорему доведено.

Питання для самоконтролю

1. Сформулюйте означення скінченного розширення поля P.
2. Дайте означення складного алгебраїчного розширенням поля P.
3. Яке розширення поля називається алгебраїчним?
4. Які співвідношення є між різними типами розширень числових полів?

Тема 15. Поняття розв'язності рівнянь у радикалах. Умови розв'язності рівняння 3-го степеня в квадратних радикалах. Приклади геометричних задач, що зводяться до рівнянь, нерозв'язних у квадратних радикалах

Означення. Уважається, що алгебраїчне рівняння

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0, \quad (a_n \neq 0) \tag{1}$$

можна розв'язати у квадратних радикалах, якщо кожний з його n коренів можна подати через коефіцієнти $a_0, a_1, \ldots, a_n$ за допомогою скінченного числа дій додавання, віднімання, множення, ділення та добування квадратного кореня.

Оскільки дії додавання, віднімання, множення, ділення називають раціональними операціями, то це означення можна скоротити, а саме: рівняння (1) розв'язне у квадратних радикалах, якщо кожний його корінь можна подати через коефіцієнти a_j, $j = 0,\ldots,n,$ за допомогою скінченного числа раціональних операцій та дій добування квадратного кореня.

Очевидно, будь-яке лінійне рівняння

$$ax + b = 0 \tag{2}$$

та будь-яке квадратне рівняння

$$ax^2 + bx + c = 0 \tag{3}$$

розв'язуються у квадратних радикалах, бо корені цих рівнянь можна подати через коефіцієнти формулами $\alpha = -\frac{b}{a}$; $\alpha_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, де α – корінь рівняння (2), $\alpha_{1,2}$ – корені (3), тобто за допомогою скінченного числа дій додавання, віднімання, множення, ділення та добування квадратного кореня.

Не кожне алгебраїчне рівняння можна розв'язати у радикалах, тобто виразити всі його корені через коефіцієнти за допомогою скінченного числа дій додавання, віднімання, множення, ділення і добування кореня з цілим показником степеня. Зокрема, славнозвісна теорема Руффіні-Абеля (за ім'ям італійського математика П. Руффіні та норвезького математика Н. Абеля)

твердить, що рівняння n-степеня з довільними буквеними коефіцієнтами при $n \geq 5$ не можна розв'язати в радикалах. Водночас існують окремі класи рівнянь вищих степенів, які можна розв'язати у радикалах (зокрема, двочленні рівняння).

Наведемо *приклад*. Розв'язати рівняння $x^5 - 1 = 0$. Запишемо його так:

$$(x-1)(x^4 + x^3 + x^2 + x + 1) = 0.$$

$$\left[\begin{array}{l} x - 1 = 0, \\ x^4 + x^3 + x^2 + x + 1 = 0. \end{array}\right.$$

Розв'язком першого рівняння є $x_1 = 1$. Розглянемо друге рівняння. Поділимо його обидві частини на x^2. Розв'язків при цьому ми не втратимо, бо $x = 0$ не є коренем цього рівняння.

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0.$$

Нехай $x + \frac{1}{x} = y$; $x^2 + 2 + \frac{1}{x^2} = y^2$; тоді отримаємо: $y^2 - 2 + y + 1 = 0$ або

$$y^2 + y - 1 = 0.$$

$$y_1 = \frac{-1-\sqrt{5}}{2}, \quad y_2 = \frac{-1+\sqrt{5}}{2}.$$

$$\left[\begin{array}{l} x + \frac{1}{x} = \frac{-1-\sqrt{5}}{2}, \\ x + \frac{1}{x} = \frac{-1+\sqrt{5}}{2} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x^2 + 1 = \frac{-1-\sqrt{5}}{2}x, \\ x^2 + 1 = \frac{-1+\sqrt{5}}{2}x \end{array}\right. \Leftrightarrow \left[\begin{array}{l} x^2 + \frac{1+\sqrt{5}}{2}x + 1 = 0, \\ x^2 + \frac{1-\sqrt{5}}{2}x + 1 = 0. \end{array}\right.$$

$$x_{2,3} = \frac{-1-\sqrt{5}}{4} \pm \frac{\sqrt{-10+2\sqrt{5}}}{4} = \frac{-1-\sqrt{5}}{4} \pm i\frac{\sqrt{10-2\sqrt{5}}}{4};$$

$$x_{4,5} = \frac{-1+\sqrt{5}}{4} \pm \frac{\sqrt{-10-2\sqrt{5}}}{4} = \frac{-1+\sqrt{5}}{4} \pm i\frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Якщо врахувати, що всі цілі числа, які фігурують у знайдених формулах для $x_{2,3}$, $x_{4,5}$, можна отримати з коефіцієнтів рівняння $x^5 - 1 = 0$ (тобто чисел 1,–1,0) за допомогою скінченного числа раціональних дій, то стає зрозумілим, що задане рівняння 5-го степеня розв'язується у квадратних радикалах.

Загальне дослідження тих класів алгебраїчних рівнянь, які можуть бути розв'язані в радикалах, є предметом важливої галузі сучасної алгебри – теорії Галуа (Галуа – видатний французький математик).

З'ясуємо умови розв'язності в квадратних радикалах рівнянь 3-го степеня:

$$f(x) \equiv x^3 + ax^2 + bx + c = 0. \qquad (4)$$

Теорема. Рівняння 3-го степеня вигляду (4) з раціональними коефіцієнтами розв'язне у квадратних радикалах тоді і тільки тоді, коли воно має хоча б один раціональний корінь.

Д о в е д е н н я. Обмежимось доведенням *достатності.* Якщо рівняння (4) має хоча б один раціональний корінь d, то це рівняння можна записати:

$$(x-d)(x^2 + mx + n) = 0, \text{ де } \ m, n \in Q.$$

Рівняння (4) розпадається на сукупність двох рівнянь не вище 2-го степеня, а тому воно розв'язне у квадратних радикалах.

Наслідок. Рівняння (4) з раціональними коефіцієнтами розв'язне у квадратних радикалах тоді і тільки тоді, коли многочлен $f(x)$ звідний у кільці $Q[x]$.

З даною теоремою тісно пов'язане питання про побудовність чисел за допомогою циркуля і лінійки. У геометрії доводиться, що корені рівняння

$$x^3 + ax^2 + bx + c = 0$$

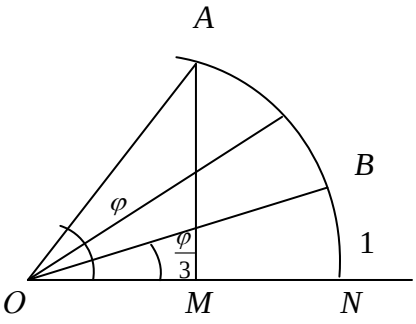
з раціональними коефіцієнтами можуть бути побудовані циркулем і лінійкою тоді і тільки тоді, коли це рівняння розв'язне в квадратних радикалах.

Ще близько двох з половиною тисяч років тому геометри Греції виявили деякі задачі, які неможливо було розв'язати за допомогою циркуля і лінійки (тобто за допомогою проведення кіл і прямих ліній). Найбільш відомим серед них є задача **подвоєння куба**, **трисекції кута** і **квадратури круга**. Розглянемо ці класичні задачі.

Задача подвоєння куба. Побудувати ребро куба, об'єм якого вдвічі більший за об'єм даного куба.

Нехай довжина ребра такого куба дорівнює 1, тоді його об'єм – 1. Довжину ребра куба вдвічі більшого об'єму позначимо x; тоді $x^3 = 2$ або $x^3 - 2 = 0$. Це рівняння раціональних коренів не має, тому нерозв'язне в квадратних радикалах. Таким чином, корені цього рівняння не можуть бути побудовані циркулем і лінійкою, тобто задача подвоєння куба не може бути розв'язана циркулем і лінійкою.

Задача трисекції кута. Поділити даний кут на три рівні частини.



Мал. 1.

Нехай φ – заданий кут (мал. 1). Проведемо дугу одиничного радіуса з центром в точці O. Точку A, а, отже, – відрізок $OM = \cos\varphi = a$ можна вважати заданими разом з кутом φ. Задача буде розв'язана, якщо ми побудуємо точку B або відрізок $ON = \cos\dfrac{\varphi}{3} = x_0$.

Оскільки $\cos\varphi = 4\cos^3\dfrac{\varphi}{3} - 3\cos\dfrac{\varphi}{3}$, то $a = 4x_0^3 - 3x_0$, тобто x_0 є коренем рівняння

$$4x^3 - 3x - a = 0. \qquad (5)$$

Отже, задачу трисекції кута можна розв'язати циркулем і лінійкою тоді і тільки тоді, коли рівняння (5) має раціональні корені. А це залежить від числового значення параметра $a = \cos\varphi$.

Нехай $\varphi = 90°$, тоді $a = \cos 90° = 0$. Матимемо рівняння

$$4x^3 - 3x = 0;$$

$$x(4x^2 - 3) = 0.$$

Це рівняння має раціональний корінь $x = 0$. А тому трисекцію кута $\varphi = 90°$ можна виконати циркулем і лінійкою.

Нехай $\varphi = 60°$, $a = \cos 60° = \frac{1}{2}$. Матимемо рівняння

$$4x^3 - 3x - \frac{1}{2} = 0;$$

$$8x^3 - 6x - 1 = 0.$$

Покладемо $y = 2x$, тоді отримаємо рівняння

$$y^3 - 3y - 1 = 0.$$

Це рівняння раціональних коренів не має, тому трисекція кута $\varphi = 60°$ циркулем і лінійкою неможлива.

Задача квадратури круга полягає у побудові квадрата, рівновеликого даному кругу.

Якщо взяти радіус даного круга 1, то його площа π. Тому треба побудувати квадрат зі стороною $\sqrt{\pi}$. Оскільки π – трансцендентне число, тобто не може бути коренем жодного алгебраїчного рівняння з раціональними коефіцієнтами, то задача квадратури круга не може бути розв'язана циркулем і лінійкою.

Питання для самоконтролю

1. Що означає, що алгебраїчне рівняння можна розв'язати у квадратних радикалах?
2. При якій умові рівняння 3-го степеня з раціональними коефіцієнтами розв'язне у квадратних радикалах?
3. Які класичні задачі неможливо розв'язати за допомогою циркуля і лінійки (тобто за допомогою проведення кіл і прямих ліній)? У чому полягають задачі подвоєння куба, трисекції кута і квадратури круга?

Література

1. Завало С.Т., Костарчук В.М., Хацет Б.І. Алгебра і теорія чисел : у 2-х ч. – К. : «Вища школа», 1976. – Ч. 2. – 384 с.
2. Завало С.Т., Костарчук В.М., Хацет Б.І. Алгебра і теорія чисел : у 2-х ч. – К. : «Вища школа», 1974. – Ч. 1. – 464 с.
3. Требенко Д.Я., Требенко О.О. Алгебра і теорія чисел : у 2 ч. – К. : НПУ імені М.П. Драгоманова, 2009. – Ч. 1. – 420 с.
4. Требенко Д.Я., Требенко О.О. Алгебра і теорія чисел : у 2 ч. – К. : НПУ імені М.П. Драгоманова, 2018. – Ч. 2. – 500 с.
5. Завало С.Т., Левіщенко С.С., Пилаєв В.В., Рокицький І.О. Алгебра і теорія чисел : практикум. – К. : «Вища школа», 1986. – Ч. 2. – 264 с.

Предметний покажчик

Електронне навчальне видання

Леся Комарницька,
Юрій Матурін

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

Частина 2

Дрогобицький державний педагогічний університет
імені Івана Франка

Редактор
Ірина Невмержицька
Технічний редактор
Ольга Лужецька
Коректор
Ірина Артимко

Здано до набору 28.09.2023 р. Формат 60x90/16. Гарнітура Times. Ум. друк. арк. 7,000. Зам. 63.

Дрогобицький державний педагогічний університет імені Івана Франка. (Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників та розповсюджувачів видавничої продукції ДК № 5140 від 01.07.2016 р.). 82100, Дрогобич, вул. Івана Франка, 24, к. 31.