

ЛІНІЙНА

Розділ 9. Поліноми від однієї змінної

Один з основних методів алгебри полягає в тому, що розв'язок якої-небудь задачі для заданого алгебричного об'єкта зводиться до розв'язання більш простої задачі для іншого алгебричного об'єкта, певним чином побудованого з вихідного. Для прикладу, розв'язання системи n лінійних рівнянь від n невідомих над кільцем R зводиться до розв'язання найпростішого рівняння над кільцем матриць $M_n(R)$. У зв'язку з цим, в алгебрі багато уваги приділяється різним способам конструювання з даних алгебричних об'єктів нових об'єктів і вивченю властивостей останніх.

Ми розпочинаємо дослідження ще однієї важливої конструкції подібного типу — кільця поліномів над заданим кільцем. До необхідності використання і вивчення поняття полінома приводять багато різних алгебричні задач. Найпростіша (за формулюванням) і найдавніша з них — задача про розв'язання рівняння вигляду

$$a_n x^n + \dots + a_1 x + a_0 = 0$$

над заданими кільцем. Цим, однак, далеко не вичерpuється область застосувань поліномів в алгебрі. Наприклад, за допомогою поліномів описуються перетворення кілець і полів, вивчаються властивості матриць, з вихідних полів будуються різні нові поля із заданими властивостями і розв'язуються багато інших задач.

Загалом, поняття полінома відоме ще із середньої школи. Однак ми розпочнемо виклад теорії поліномів з їхнього формального визначення, яке, на перший погляд, може здатися неприродним і незручним, але насправді дозволяє найбільш економним способом домогтися потрібної строгості і перейти до загальноприйнятої термінології.

9.1. Кільця поліномів від однієї змінної над кільцями

Нехай R — довільне кільце з одиницею, відмінною від нуля.

Означення 9.1. Розглянемо нескінченну впорядковану послідовність

$$f = (a_0, a_1, a_2, \dots, a_n, \dots) \tag{9.1}$$

елементів $a_0, a_1, a_2, \dots, a_n \in R$, в якій всі a_i , окрім їхньої скінченної кількості, дорівнюють нулю (нескінченні впорядковані послідовності (рядки нескінченної довжини), в яких лише скінчена кількість елементів відмінна від нуля, часто називаються *фінітними*). Елементи a_i називатимемо *коєфіцієнтами послідовності* (9.1). Послідовність $(0, 0, \dots)$, усі елементи якої нульові, називають *нульовою*. Множину всіх послідовностей вигляду (9.1) позначатимемо через R^∞ .

Означення 9.2. Нехай $f = (a_0, a_1, \dots, a_n, \dots)$, $g = (b_0, b_1, \dots, b_n, \dots) \in R^\infty$. Сумою послідовностей f, g називають послідовність

$$f + g = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots). \tag{9.2}$$

Добутком послідовностей f, g називають послідовність

$$fg = (c_0, c_1, \dots, c_n, \dots), \quad \text{де } c_i = \sum_{k=0}^i a_k b_{i-k} \text{ для усіх } i \in \mathbb{N}_0. \quad (9.3)$$

Добутком послідовності f на елемент $r \in R$ зліва або справа називають послідовність

$$rf = (ra_0, ra_1, \dots, ra_n, \dots) \text{ або } fr = (a_0r, a_1r, \dots, a_nr, \dots). \quad (9.4)$$

Сумою елемента $r \in R$ та послідовності f називають послідовність

$$r + f = f + r = (a_0 + r, a_1, \dots, a_n, \dots). \quad (9.5)$$

Зрозуміло, що у послідовностях (9.2)–(9.5), так як і у вихідних послідовностях, всі коефіцієнти, за винятком скінченної кількості, дорівнюють нулю, і тому ці послідовності належать R^∞ .

Зауваження 9.1. Операції додавання вигляду (9.2) і (9.5) різні, хоча її позначаються, для зручності, одним і тим же символом «+». Остання обставина не може призводити до плутанини, оскільки природа елементів, які додаються, зрозуміло вказує на те, яка з операцій мається на увазі. Крім цього, відмінність між цими операціями має, по суті, лише формальний характер, оскільки операція вигляду (9.5) легко виражається через операцію (9.2):

$$r + f = (r, 0, \dots, 0, \dots) + f.$$

Твердження 9.1. Якщо R — кільце з одиницею, то множина R^∞ також є кільцем з одиницею стосовно операції додавання (9.2) та множення (9.3). Кільце R^∞ комутативне тоді і лише тоді, коли комутативне кільце R .

Доведення. Як ми уже наголошували, в результаті додавання та множення елементів з R^∞ знову отримуються елементи з R^∞ , тобто множина R^∞ замкнена стосовно цих операцій.

Очевидно, що множина R^∞ утворює абелеву групу стосовно операції додавання (9.2): асоціативність та комутативність додавання в множині R^∞ випливає з асоціативності та комутативності додавання в самому кільці R ; елемент $(0, 0, \dots, 0, \dots)$ є нейтральним (нульовим) елементом в R^∞ , а протилежним до довільного елемента $f = (a_0, a_1, \dots, a_n, \dots) \in R^\infty$ є елемент $-f = (-a_0, -a_1, \dots, -a_n, \dots)$.

Перевіримо, що операція множення (9.3) асоціативна. Нехай $f = (a_0, a_1, \dots, a_n, \dots)$, $g = (b_0, b_1, \dots, b_n, \dots)$, $h = (c_0, c_1, \dots, c_n, \dots) \in R^\infty$. Тоді на i -му місці в добутку $(fg)h$ знаходитьться елемент

$$\sum_{s+t=i} \left(\sum_{k+l=s} a_k b_l \right) c_t = \sum_{k+l+t=i} a_k b_l c_t,$$

а в добутку $f(gh)$ — елемент

$$\sum_{k+j=i} a_k \left(\sum_{l+t=j} b_l c_t \right) = \sum_{k+l+t=i} a_k b_l c_t,$$

тобто $(fg)h = f(gh)$.

Доведемо дистрибутивність множення щодо додавання. Нехай $f, g, h \in R^\infty$. Тоді на i -му місці в послідовності $(f+g)h$ буде елемент $\sum_{k+l=i} (a_k + b_k)c_l$, а в послідовності $fh + gh$ — елемент $\sum_{k+l=i} a_k c_l + \sum_{k+l=i} b_k c_l$.

Але, оскільки

$$\sum_{k+l=i} (a_k + b_k)c_l = \sum_{k+l=i} a_k c_l + \sum_{k+l=i} b_k c_l,$$

то й $(f+g)h = fh + gh$. Праву дистрибутивність доведено, ліва доводиться аналогічно.

Якщо 1 — одиниця кільця R , то $(1, 0, \dots, 0, \dots)$ — одиничний елемент кільця R^∞ .

Якщо кільце R комутативне, то на i -му місці послідовностей fg і gf буде знаходитись один і той же елемент $\sum_{k+l=i} a_k b_l = \sum_{l+k=i} b_l a_k$, а тому кільце R^∞ також комутативне. Якщо ж $ab \neq ba$ для деяких $a, b \in R$, то в R^∞ не комутують послідовності $(a, 0, \dots)$ і $(b, 0, \dots)$. \square

Використовуючи задані на R^∞ операції, перейдемо до традиційного запису поліномів. Введемо позначення

$$x = (0, 1, 0, \dots) \quad (9.6)$$

і x назовемо *змінною* (або *невідомою*) над R . За співвідношенням (9.3) легко переконатися, що $x^2 = (0, 0, 1, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, \dots)$ і т.д., тобто для довільного $n \in \mathbb{N}_0$ маємо

$$x^n = (\underbrace{0, 0, \dots, 0}_{n \text{ нулів}}, 1, 0, \dots). \quad (9.7)$$

Крім цього, очевидно, $x^k x^t = x^{k+t}$ і $(x^k x^t)x^s = x^k(x^t x^s)$ для довільних $k, t, s \in \mathbb{N}_0$, а також $x^0 = (1, 0, \dots)$.

Таким чином, користуючись співвідношенням (9.4), отримаємо, що для довільних $r \in R$ і $n \in \mathbb{N}_0$ правильні рівності

$$rx^n = (0, \dots, 0, r, 0, \dots) = x^n r,$$

і тому довільний елемент $f = (a_0, a_1, \dots, a_n, 0, \dots) \in R^\infty$ може бути записаний у вигляді суми

$$\begin{aligned} f &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, \dots, 0, a_n, 0, \dots) = \\ &= a_0 x^0 + a_1 x^1 + a_2 x^2 + \dots + a_n x^n = \sum_{i=0}^n a_i x^i. \end{aligned} \quad (9.8)$$

Користуючись зауваженням 9.1 і позначенням (9.6), останній запис можна ще спростити, записавши його у загальноприйнятому вигляді

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n. \quad (9.9)$$

Таке зображення елемента f однозначне, оскільки a_0, \dots, a_n у правій частині співвідношення (9.9) — це коефіцієнти послідовності $(a_0, a_1, \dots, a_n, 0, \dots)$, яка дорівнює нулю тоді і лише тоді, коли $a_0 = \dots = a_n = 0$.

Означення 9.3. При введених вище позначеннях елемент $f(x)$ вигляду (9.9) називають *поліномом* (або *многочленом*) від змінної x над кільцем R , а елементи $a_i \in R$ — його *коефіцієнтами*. Кажуть також, що a_i — *коефіцієнт полінома* $f(x)$ біля змінної x^i , а a_0 — його *вільний член*. Кільце R^∞ називають *кільцем поліномів* від однієї змінної x над кільцем R і позначають через $R[x]$.

Зауваження 9.2. Наголосимо, що поліном $f(x) \in R[x]$ вигляду (9.9) має нескінченно багато коефіцієнтів a_i , $i \in \mathbb{N}_0$, а рівність (9.9) означає, що $a_{n+1} = a_{n+2} = \dots = 0$. При цьому можливо, що й $a_n = 0$. Зокрема, відповідно до означення 9.1 і 9.3, поліном (9.9) дорівнює поліному

$$g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m \quad (9.10)$$

тоді і тільки тоді, коли $a_i = b_i$ для всіх $i \in \mathbb{N}_0$. Зокрема, жоден поліном, в якому хоча б один коефіцієнт відмінний від нуля, не може бути рівним нулю.

Означення 9.4. Степенем ненульового полінома $f(x)$ вигляду (9.9) називають число, яке дорівнює найбільшому з номерів i його ненульових коефіцієнтів a_i . Якщо поліном нульовий, то вважають, що його степінь дорівнює $-\infty$. Степінь полінома $f(x)$ позначатимемо через $\deg f(x)$. Якщо $\deg f(x) = n$, то коефіцієнт a_n полінома $f(x)$ називають його *старшим коефіцієнтом*, а доданок $a_n x^n$ — *старшим членом* полінома $f(x)$. Поліноми степеня 1, 2, 3 називають відповідно *лінійними, квадратичними* (або *квадратними*), *кубічними*.

Приклад 9.1. Якщо $f(x) = 3x^5 + 13x^2 + 2x$, $g(x) = x^3 + 5x^2 + 5$, $h(x) = x + 17$, то $\deg f(x) = 5$, поліном $g(x)$ кубічний, а $h(x)$ — лінійний.

Безпосередньо із означення 9.2 випливає, що сума і добуток поліномів $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ можуть бути записані так:

$$f(x) + g(x) = \sum_{i=0}^k (a_i + b_i)x^i, \quad k = \max\{n, m\},$$

$$f(x) \cdot g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_{n-1}b_m + a_nb_{m-1})x^{n+m-1} + a_nb_mx^{n+m}. \quad (9.11)$$

Звідси легко випливає (перевірте!) таке твердження.

Твердження 9.2. Для довільних поліномів $f(x), g(x) \in R[x]$ виконуються співвідношення:

$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}, \quad (9.12)$$

$$\deg(f(x) \cdot g(x)) \leq \deg f(x) + \deg g(x). \quad (9.13)$$

Як легко бачити із рівності (9.11), співвідношення (9.13) заміняється рівністю

$$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x) \quad (9.14)$$

кожного разу, коли добуток a_nb_m старших коефіцієнтів поліномів $f(x), g(x)$ відмінний від нуля, тобто у кільці R немає дільників нуля. А це означає, що правильне таке твердження.

Твердження 9.3. Кільце $R[x]$ містить дільники нуля тоді і лише тоді, коли R містить дільники нуля.

Надалі нуль і одиницю в кільці $R[x]$ ми, для стисlosti, будемо позначати тими ж символами, які прийняті для їх позначення в кільці R , тобто покладемо

$$0 \cdot x^0 = 0, \quad x^0 = 1.$$

Зауваження 9.3. Остання домовленість дозволяє ототожнити будь-який елемент $r = r \cdot 1$ з кільця R з поліномом $rx^0 = (r, 0, 0, \dots)$. Таке ототожнення велими природне, оскільки очевидно, що множина $\bar{R} = \{rx^0 \mid r \in R\}$ є підкільцем в $R[x]$, яке ізоморфне кільцю R , і ізоморфізм $R \rightarrow \bar{R}$ задається якраз відповідністю $r \mapsto rx^0$. Таким чином, скрізь, де це зручно, можна вважати, що кільце R є підкільцем в кільці $R[x]$.

9.2. Подільність поліномів. Теорема про ділення з остачею

Кажуть, що елемент a кільця R ділиться зліва (справа) на елемент b цього ж кільця, якщо в R існують розв'язки рівняння

$$bx = a \quad (yb = a).$$

Як нам уже відомо, якщо R — кільце з одиницею і b — обертний елемент в R , то кожне з цих рівнянь має єдиний розв'язок: $b^{-1}a$ (ab^{-1} , відповідно). Якщо ж елемент b — необертний, то навіть немає алгоритму, який би дозволяв з'ясувати чи існують розв'язки цих рівнянь у довільному нескінченному кільці R . Однак, у випадку кільця поліномів $R[x]$ над кільцем R з одиницею можна ввести поняття подільності із остачею і запропонувати алгоритм, який у багатьох важливих випадках дозволяє перевірити: ділиться один поліном на інший чи ні.

Означення 9.5. Поліном $f(x) \in R[x]$ ділиться зліва з остачею на поліном $g(x) \in R[x]$, якщо існують такі поліноми $q_l(x), r_l(x) \in R[x]$, що

$$f(x) = g(x) \cdot q_l(x) + r_l(x), \quad \deg r_l(x) < \deg g(x). \quad (9.15)$$

При цьому поліноми $q_l(x)$ і $r_l(x)$ називають, відповідно, *неповною лівою часткою* і *лівою остачею* від ділення $f(x)$ на $g(x)$. Аналогічно, поняття *подільності* $f(x)$ на $g(x)$ справа з остачею і *неповна права частка* $q_r(x)$ та *права остача* $r_r(x)$ визначаються як поліноми, що задовільняють співвідношенням

$$f(x) = q_r(x) \cdot g(x) + r_r(x), \quad \deg r_r(x) < \deg g(x).$$

Іноді, для стисlosti, поліном $q_l(x)$ ($q_r(x)$) називають просто *лівою* (*правою*) *часткою* від ділення з остаточею $f(x)$ на $g(x)$.

Зауваження 9.4. Взагалі кажучи, ділення з остаточею в $R[x]$ не завжди можливе, а коли й можливе, то не завжди однозначне. Наприклад, якщо $R = M_2(F)$ — кільце матриць другого порядку над полем F , то поліном $f(x) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}x + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ можна поділити справа з остаточею на поліном $g(x) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}x + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ принаймні двома способами:

$$f(x) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot g(x) + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad f(x) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot g(x) + \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}.$$

При цьому $f(x)$ не можна поділити на $g(x)$ з остаточею зліва (доведіть!).

Однак зазначеність зникає при деяких обмеженнях на поліном $g(x)$.

Теорема 9.4 (про ділення з остаточею). Якщо старший коефіцієнт полінома $g(x) \in R[x]$ оборотний у кільці R , то будь-який поліном $f(x) \in R[x]$ можна поділити зліва (справа) з остаточею на $g(x)$. При цьому ліві (праві) неповні частки і остаті визначаються однозначно.

Доведення. Виконаємо доведення для лівобічного випадку і спочатку доведемо можливість ділення з остаточею. В кільці $R[x]$ розглянемо довільні поліноми

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 \end{aligned}$$

і нехай старший коефіцієнт b_m полінома $g(x)$ є оборотним.

Якщо $\deg f(x) < \deg g(x)$, то

$$f(x) = g(x) \cdot 0 + f(x),$$

а тому співвідношення (9.15) виконується при $q_l(x) = 0$, $r_l(x) = f(x)$.

Якщо $\deg f(x) \geq \deg g(x)$, то існує поліном $g(x) \cdot b_m^{-1} a_n x^{n-m}$, старший член якого, як легко бачити, дорівнює $a_n x^n$ і тому степінь полінома

$$f_1(x) = f(x) - g(x) b_m^{-1} a_n x^{n-m}$$

менший n . Нехай $\deg f_1(x) = n_1$ і якщо $n_1 < m$, то ділення з остаточею $f(x)$ на $g(x)$ завершується:

$$f(x) = g(x) \cdot (b_m^{-1} a_n x^{n-m}) + f_1(x),$$

$q_l(x) = b_m^{-1} a_n x^{n-m}$, $r_l(x) = f_1(x)$, $\deg r_l(x) = n_1 < m = \deg g(x)$. Якщо ж $n_1 \geq m$ і $a_{n_1}^{[1]} x^{n_1}$ є старшим членом полінома $f_1(x)$, то, зрозуміло, степінь полінома

$$f_2(x) = f_1(x) - g(x) b_m^{-1} a_{n_1}^{[1]} x^{n_1-m}$$

менший n_1 . Нехай $\deg f_2(x) = n_2$ і якщо $n_2 < m$, то співвідношення (9.15) виконується:

$$f(x) = g(x) \cdot (b_m^{-1} a_n x^{n-m} + b_m^{-1} a_{n_1}^{[1]} x^{n_1-m}) + f_2(x),$$

$q_l(x) = b_m^{-1} a_n x^{n-m} + b_m^{-1} a_{n_1}^{[1]} x^{n_1-m}$, $r_l(x) = f_2(x)$, $\deg r_l(x) = n_2 < m = \deg g(x)$. Якщо ж $n_2 \geq m$, то продовжимо аналогічні перетворення. У підсумку, за скінченне число k кроків ми прийдемо до рівності

$$f(x) = g(x) \cdot (b_m^{-1} a_n x^{n-m} + b_m^{-1} a_{n_1}^{[1]} x^{n_1-m} + \dots + b_m^{-1} a_{n_k}^{[k]} x^{n_k-m}) + f_{k+1}(x),$$

в якій $\deg f_{k+1}(x) < m$, що й доводить можливість лівобічного ділення з остаточею в кільці $R[x]$.

Тепер доведемо, що ліві неповні частки і остатча визначені умовами теореми однозначно. Нехай

$$f(x) = g(x) \cdot q_l(x) + r_l(x) = g(x) \cdot \dot{q}_l(x) + \dot{r}_l(x),$$

де

$$\deg r_l(x) < \deg g(x), \quad \deg \dot{r}_l(x) < \deg g(x). \quad (9.16)$$

Припустимо, що $q(x) \neq \dot{q}(x)$. Тоді з рівності

$$r_l(x) - \dot{r}_l(x) = g(x) \cdot (\dot{q}_l(x) - q_l(x))$$

за співвідношенням (9.14) випливає, що

$$\deg(r_l(x) - \dot{r}_l(x)) = \deg g(x) + \deg(\dot{q}_l(x) - q_l(x)) \geq \deg g(x),$$

що, очевидно, неможливо, оскільки степені $r_l(x)$ та $\dot{r}_l(x)$ менші степеня $g(x)$ (див. (9.16)). Отже, $\dot{q}_l(x) = q_l(x)$, а тому й $r_l(x) = \dot{r}_l(x)$.

Доведення теореми для правобічного випадку аналогічне. \square

Запропонований в доведенні теореми 9.4 метод ділення $f(x)$ на $g(x)$ з остачею є добре відомим методом ділення «кутом».

Приклад 9.2. Поділімо «кутом» поліном $f(x) = 3x^3 + 13x^2 + 27x - 3$ на поліном $g(x) = x^2 + 5x + 5$.

Розв'язання. Маємо:

$$\begin{array}{r} 3x^3 + 13x^2 + 27x - 3 \\ 3x^3 + 15x^2 + 15x \\ \hline -2x^2 + 12x - 3 \\ -2x^2 - 10x - 10 \\ \hline 22x + 7 \end{array} \quad \left| \begin{array}{c} x^2 + 5x + 5 \\ 3x - 2 \end{array} \right.$$

Отож, $f(x) = g(x)(3x - 2) + 22x + 7$. \square

Якщо кільце R комутативне, то ліві неповна частка і остача від ділення $f(x)$ на $g(x)$ (у випадку їхнього існування) є також правими неповною часткою і остачею. У цьому випадку говорять просто про ділення $f(x)$ на $g(x)$ із остачею. Очевидно, що якщо R — поле, то ситуація аналогічна. Більше цього, у випадку поля очевидним наслідком теореми 9.4 є таке твердження.

Наслідок 9.5. Якщо F — поле і $g(x)$ — ненульовий поліном із $F[x]$, то будь-який поліном $f(x) \in F[x]$ можна поділити з остачею на $g(x)$, причому єдиним способом.

Доведення. Досить зауважити, що старший коефіцієнт $g(x)$ відмінний від нуля і тому оборотний у F . \square

Аналогічно означеню ?? можна навести таке означення.

Означення 9.6. Поліном $f(x)$ ділиться зліва (справа) на поліном $g(x)$ в кільці $R[x]$, якщо існують такі поліноми $p(x) \in R[x]$ ($h(x) \in R[x]$), що $f(x) = g(x)p(x)$ ($f(x) = h(x)g(x)$). При цьому поліном $g(x)$ називають лівим (правим) дільником полінома $f(x)$.

Наслідок 9.6. Якщо старший коефіцієнт полінома $g(x) \in R[x]$ оборотний у кільці R , то $g(x)$ ділить поліном $f(x) \in R[x]$ зліва (справа) тоді і лише тоді, коли при діленні $f(x)$ на $g(x)$ зліва (справа) остача дорівнює нулю.

Доведення. Якщо у співвідношеннях (9.15) остача $r_l(x) \neq 0$, то за доведеною у теоремі 9.4 єдиністю лівої остачі рівність $f(x) = g(x) \cdot q_l(x) + 0$ неможлива при жодному $q_l(x) \in R[x]$. \square

Наведемо декілька основних властивостей подільності поліномів кільця $R[x]$. Оскільки кільце R передбачається некомутативним, то, для стислоті викладу, сформулюємо та доведемо ці властивості для лівобічного випадку (правобічний формулюється та доводиться аналогічно).

Лема 9.7. Нехай $f(x), g(x), h(x) \in R[x]$. Тоді правильні такі твердження:

- 1) якщо $f(x)$ ділиться зліва на $g(x)$, а $g(x)$ ділиться зліва на $h(x)$, то $f(x)$ ділиться зліва на $h(x)$;
- 2) якщо $f(x)$ і $h(x)$ діляться зліва на $g(x)$, то $f(x) \pm h(x)$ також ділиться зліва на $g(x)$;
- 3) якщо $f(x)$ ділиться зліва на $g(x)$, то для довільного $p(x) \in R[x]$ добуток $f(x)p(x)$ також ділиться зліва на $g(x)$;
- 4) якщо $f(x)$ ділиться зліва на $g(x)$, то $f(x)$ також ділиться зліва на $g(x)c$, де c — довільний оборотний елемент кільця R ;
- 5) поліноми $f(x)c$, де c — оборотний елемент кільця R , і лише вони будуть лівими дільниками полінома $f(x)$, які мають ту ж степінь, що й $f(x)$.

Доведення. 1) За умовою $f(x) = g(x) \cdot q_l(x)$ і $g(x) = h(x) \cdot p_l(x)$ для деяких $q_l(x), p_l(x) \in R[x]$, а тому, підставивши другу рівність у першу, отримаємо $f(x) = h(x) \cdot (q_l(x) \cdot p_l(x))$.

2) Якщо $f(x) = g(x) \cdot q_l(x)$ і $h(x) = g(x) \cdot p_l(x)$, то $f(x) \pm h(x) = g(x) \cdot (q_l(x) \pm p_l(x))$.

3) Дійсно, якщо $f(x) = g(x) \cdot q_l(x)$, то, як легко бачити, $f(x) \cdot p(x) = g(x) \cdot (q_l(x) \cdot p(x))$.

4) Якщо $f(x) = g(x) \cdot q_l(x)$, то $f(x) = (g(x)c) \cdot (c^{-1}q_l(x))$, що й потрібно було довести.

5) З одного боку очевидно, оскільки $f(x) = (f(x)c)c^{-1}$. З іншого боку, якщо $f(x)$ ділиться зліва на $g(x)$, причому степені $f(x)$ і $g(x)$ співпадають, то за співвідношенням (9.13) степінь лівої частки від ділення $f(x)$ на $g(x)$ мусить дорівнювати нулю, тобто $f(x) = g(x)d$, $d \neq 0$. Аналогічно, $g(x) = f(x)c$ для деякого $c \in R \setminus \{0\}$. Звідси отримуємо, що $f(x) = f(x)cd$ і $g(x) = g(x)dc$, а тому $cd = dc = 1$. \square

9.3. Кільця поліномів над полями

У цьому та наступних параграфах ми розглянемо кільця $F[x]$ поліномів над довільним полем F і тому термін подільність поліномів вживатимемо без наголошення з якого саме боку це ділення відбуватиметься.

Для подальшого описання властивостей кільця $F[x]$ введемо до розгляду таке поняття.

Означення 9.7. Елементи a та b комутативного кільця Q з одиницею називають *асоційованими*, якщо $b = ua$ для деякого оборотного елемента $u \in Q$.

Легко перевірити, що відношення асоційованості елементів є відношенням еквівалентності на Q .

Твердження 9.8. У кільці $F[x]$ оборотні всі поліноми нульового степеня і лише вони. Для поліномів $f(x), g(x) \in F[x]$ еквівалентні такі твердження:

- 1) $f(x)$ і $g(x)$ асоційовані;
- 2) $f(x)$ ділить $g(x)$ і $g(x)$ ділить $f(x)$;
- 3) $f(x)$ ділить $g(x)$ і $\deg f(x) = \deg g(x)$.

Доведення. Якщо $u(x) \in F[x]$ і $u(x)v(x) = 1$, то за рівністю (9.14) $\deg u(x) + \deg v(x) = 0$ і $\deg u(x) = 0$. Оборотність $u(x)$ за умови $\deg u(x) = 0$ очевидна.

Іmplікація з 1) у 2) очевидна. Іmplікація з 2) у 3) легко доводиться з використанням рівності (9.14). Нарешті, за умови 3) правильні рівності $g(x) = u(x)f(x)$, $\deg u(x) = 0$. Отже, $u(x) \in F[x]^*$ і з 3) випливає 1). \square

Означення 9.8. Поліном зі старшим коефіцієнтом, рівним одиниці, називають *унітарним* (або *нормалізованим*, або *нормованим*).

Очевидно, що множина усіх унітарних поліномів із $F[x]$ замкнута стосовно операції множення і, оскільки $F[x]^* = F^*$, то з будь-яким ненульовим поліномом $f(x) \in F[x]$ асоційований єдиний унітарний поліном, який ми будемо позначати символом $f^*(x)$.

9.4. Найбільший спільний дільник і найменше спільне кратне

Означення 9.9. Поліном $p(x)$ називають *спільним дільником* поліномів $f(x), g(x) \in F[x]$, якщо кожен з них ділиться на $p(x)$ без остачі, тобто існують такі поліноми $q_1(x), q_2(x) \in F[x]$, що

$$f(x) = p(x) \cdot q_1(x) \quad \text{i} \quad g(x) = p(x) \cdot q_2(x).$$

Означення 9.10. *Найбільшим спільним дільником* (позначатимемо *НСД*) поліномів $f(x), g(x) \in F[x]$ називається такий поліном $d(x) \in F[x]$, що

- (1) $d(x)$ є спільним дільником $f(x)$ і $g(x)$;
- (2) $d(x)$ ділиться на будь-який інший спільний дільник цих поліномів.

Інакше кажучи, *найбільшим спільним дільником* поліномів називається їхній спільний дільник максимального степеня. Сукупність усіх найбільших спільних дільників поліномів $f(x), g(x)$ позначатимемо $\text{НСД}\{f(x), g(x)\}$. Очевидно, що якщо $f(x) = g(x) = 0$, то $\text{НСД}\{f(x), g(x)\} = \{0\}$. Для опису всієї множини $\text{НСД}\{f(x), g(x)\}$ досить знайти один його елемент.

Твердження 9.9. Якщо хоча б один з поліномів $f(x), g(x)$ ненульовий і $\text{НСД}\{f(x), g(x)\} \neq \emptyset$, то для довільного $d(x) \in \text{НСД}\{f(x), g(x)\}$ правильна рівність

$$\text{НСД}\{f(x), g(x)\} = \{u d(x) \mid u \in F^*\},$$

та існує єдиний унітарний НСД поліномів $f(x), g(x)$.

Доведення. З означення 9.10 випливає, що $d(x) \neq 0$ і $ud(x) \in \text{НСД}\{f(x), g(x)\}$ для будь-якого $u \in F^*$. Навпаки, якщо $h(x) \in \text{НСД}\{f(x), g(x)\}$, то за другою властивістю означення 9.10 поліном $h(x)$ ділить $d(x)$ і $d(x)$ ділить $h(x)$, тобто за твердженням 9.8 правильною є рівність $h(x) = ud(x)$ для деякого $u \in F^*$. \square

Означення 9.10 та твердження 9.9 показують, що *найбільший спільний дільник довільних двох поліномів визначається з точністю до множника (полінома) нульового степеня*, проте залишають відкритим питання, чи цей найбільший спільний дільник існує взагалі. Відповідь на це питання є позитивною і для доведення цього факту використаємо метод для практичного знаходження найбільшого спільного дільника — алгоритм Евкліда або, інакше кажучи, *метод послідовного ділення*.

Теорема 9.10. Якщо хоча б один з поліномів $f(x), g(x) \in F[x]$ ненульовий, то для них в $F[x]$ існує єдиний унітарний найбільший спільний дільник.

Доведення. За твердженням 9.9 (2) достатньо показати існування одного НСД розглядуваних поліномів. Якщо $f(x)$ ділиться на $g(x)$, то $g(x) \in \text{НСД}\{f(x), g(x)\}$. Якщо ж $f(x)$ не ділиться на $g(x)$, то поділимо $f(x)$ на $g(x)$ з остачею (позначимо її $r_1(x)$). Далі поділимо $g(x)$ на $r_1(x)$ і отримуємо остачу $r_2(x)$, потім поділимо $r_1(x)$ на $r_2(x)$ з остачею і т.д. Отримаємо ланцюг співвідношень вигляду

$$\begin{aligned} f(x) &= g(x) \cdot q_1(x) + r_1(x), & 0 \leq \deg r_1(x) < \deg g(x), \\ g(x) &= r_1(x) \cdot q_2(x) + r_2(x), & 0 \leq \deg r_2(x) < \deg r_1(x), \\ r_1(x) &= r_2(x) \cdot q_3(x) + r_3(x), & 0 \leq \deg r_3(x) < \deg r_2(x), \\ &\dots & \\ r_{k-3}(x) &= r_{k-2}(x) \cdot q_{k-1}(x) + r_{k-1}(x), & 0 \leq \deg r_{k-1}(x) < \deg r_{k-2}(x), \\ r_{k-2}(x) &= r_{k-1}(x) \cdot q_k(x) + r_k(x), & 0 \leq \deg r_k(x) < \deg r_{k-1}(x). \end{aligned} \tag{9.17}$$

Цей ланцюг при деякому $k \in \mathbb{N}$ обов'язково обривається співвідношенням

$$r_{k-1}(x) = r_k(x) \cdot q_{k+1}(x), \quad r_{k+1}(x) = 0, \tag{9.18}$$

оскільки степені остач (9.17) утворюють строго спадний ряд чисел із \mathbb{N}_0

$$\deg g(x) > \deg r_1(x) > \dots > \deg r_k(x)$$

і цей ряд не може бути нескінченим, а у випадку, коли $r_{k+1}(x) \neq 0$, до цього рядку можна додати справа ще один член.

Покажемо, що остання ненульова остача в ланцюгу (9.17), тобто $r_k(x)$, буде найбільшим спільним дільником поліномів $f(x)$ та $g(x)$. Дійсно, по-перше, з рівності (9.18) випливає, що $r_k(x)$ є дільником $r_{k-1}(x)$, а тому обидві складові правої частини останньої рівності співвідношень (9.17) діляться на $r_k(x)$ і, отже, $r_k(x)$ буде дільником й $r_{k-2}(x)$. Далі, піднімаючись вверх за рівностями (9.17), аналогічно отримаємо, що $r_k(x)$ буде спільним дільником й для $r_{k-3}(x), \dots, r_1(x)$ і, насамкінець, для $g(x)$ та $f(x)$. Тепер, по-друге, візьмемо довільний спільний дільник $p(x)$ поліномів $f(x)$ та $g(x)$. Оскільки ліва частина і перша складова правої частини першої з рівностей (9.17) діляться на $p(x)$, то $r_1(x)$ також мусить ділитися на $p(x)$. Переїшовши до другої і наступних рівностей, ми аналогічно отримаємо, що на $p(x)$ діляться поліноми $r_2(x), \dots, r_{k-1}(x)$ і $r_k(x)$. Отже, $r_k(x) \in \text{НСД}\{f(x), g(x)\}$. \square

Ми довели, що довільні два поліноми володіють найбільшим спільним дільником, і отримали спосіб для його обчислення.

Приклад 9.3. Знайдемо найбільший спільний дільник поліномів

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

Розв'язання. Щоб уникнути дробових коефіцієнтів під час застосування алгоритму Евкліда до поліномів з цілими коефіцієнтами, можна домножити ділене або скоротити дільник на будь-яке ненульове число, причому навіть в процесі самого ділення. Це буде призводити, очевидно, до спотворення частки, але остачі, які нас цікавлять, будуть отримувати лише деякий множник нульового степеня, що, як ми вже знаємо, під час знаходження найбільшого спільного дільника дозволяється. Поділимо $f(x)$ на $g(x)$, попередньо домноживши $f(x)$ на 3:

$$\begin{array}{r} 3x^4 + 9x^3 - 3x^2 - 12x - 9 \\ 3x^4 + 10x^3 + 2x^2 - 3x \\ \hline -x^3 - 5x^2 - 9x - 9 \end{array} \quad \left| \begin{array}{r} 3x^3 + 10x^2 + 2x - 3 \\ x + 1 \\ \hline \end{array} \right.$$

$$\begin{array}{r} 3x^3 + 15x^2 + 27x + 27 \\ 3x^3 + 10x^2 + 2x - 3 \\ \hline 5x^2 + 25x + 30 \end{array}$$

(домножаємо на -3)

Отож, перша остача, після скорочення на 5, буде $r_1(x) = x^2 + 5x + 6$. Поділимо на неї поліном $g(x)$:

$$\begin{array}{r} 3x^3 + 10x^2 + 2x - 3 \\ 3x^3 + 15x^2 + 18x \\ \hline -5x^2 - 16x - 3 \\ -5x^2 - 25x - 30 \\ \hline 9x + 27 \end{array} \quad \left| \begin{array}{r} x^2 + 5x + 6 \\ 3x - 5 \\ \hline \end{array} \right.$$

Таким чином, другою остачею, після скорочення на 9, буде $r_2(x) = x + 3$, а оскільки, $r_1(x) = r_2(x) \cdot (x + 2)$, то $r_2(x)$ буде також і останньою ненульовою остачею в алгоритмі Евкліда ділення $f(x)$ на $g(x)$. Отже, $x + 3 \in \text{НСД}\{f(x), g(x)\}$. \square

Теорема 9.11. Якщо $d(x)$ — найбільший спільний дільник поліномів $f(x)$ та $g(x) \in F[x]$, то існують такі поліноми $u(x)$ та $v(x) \in F[x]$, що

$$d(x) = f(x) \cdot u(x) + g(x) \cdot v(x). \quad (9.19)$$

Доведення. Із останньої рівності співвідношень (9.17) випливає, що $r_k(x) = r_{k-2}(x) \cdot 1 + r_{k-1}(x) \cdot (-q_k(x))$, або, врахувавши, що $d(x) = r_k(x)$, і позначивши $u_1(x) = 1$, $v_1(x) = -q_k(x)$,

$$d(x) = r_{k-2}(x) \cdot u_1(x) + r_{k-1}(x) \cdot v_1(x).$$

Підставляючи сюди вираження $r_{k-1}(x)$ через $r_{k-3}(x)$ і $r_{k-2}(x)$ із передостанньої рівності (9.17), ми отримаємо

$$d(x) = r_{k-3}(x) \cdot u_2(x) + r_{k-2}(x) \cdot v_2(x),$$

де, очевидно, $u_2(x) = v_1(x)$, $v_2(x) = u_1(x) - v_1(x) \cdot q_{k-1}(x)$. Продовжуючи далі підніматися вверх рівностями (9.17), ми прийдемо до (9.19). \square

Зauważення 9.5. З доведення останньої теореми випливає практичний спосіб обчислення поліномів $u(x)$, $g(x)$ з рівності (9.19). Розглянемо його детальніше. Для цього перепишемо (9.19) у вигляді

$$r_m(x) = f(x) \cdot u_m(x) + g(x) \cdot v_m(x),$$

де $r_m(x)$ — m -та остача ($m \in \overline{1, k}$) від ділення $f(x)$ на $g(x)$ у алгоритмі Евкліда (9.17). З доведення теореми 9.11 легко бачити, що ці поліноми визначаються рекурентними формулами

$$u_m(x) = u_{m-2}(x) - u_{m-1}(x)q_m(x), \quad v_m(x) = v_{m-2}(x) - v_{m-1}(x)q_m(x)$$

з початковими умовами

$$u_0(x) = 0, \quad u_1(x) = 1, \quad v_0(x) = 1, \quad v_1(x) = -q_1(x).$$

Процес обчислення поліномів $u_m(x)$, $v_m(x)$ і, зокрема, $u(x)$, $v(x)$ зручно проводити за допомогою такої таблиці.

i	0	1	2	...	m	...	k
$q_i(x)$		$q_1(x)$	$q_2(x)$...	$q_m(x)$...	$q_k(x)$
$u_i(x)$	0	1	$u_2(x) = u_0(x) - u_1(x)q_2(x)$...	$u_m(x) = u_{m-2}(x) - u_{m-1}(x)q_m(x)$...	$u(x) = u_k(x)$
$v_i(x)$	1	$-q_1(x)$	$v_2(x) = v_0(x) - v_1(x)q_2(x)$...	$v_m(x) = v_{m-2}(x) - v_{m-1}(x)q_m(x)$...	$v(x) = v_k(x)$

Приклади 9.4. 1. Знайдемо НСД та поліноми $u(x)$ і $v(x)$, що задовольняють рівність (9.19), для поліномів $f(x) = x^4 + 2x^3 - x^2 - 4x - 2$, $g(x) = x^4 + x^3 - x^2 - 2x - 2 \in \mathbb{R}[x]$. Застосуємо до цих поліномів алгоритм Евкліда (причому тепер під час виконання ділення уже не можна допускати спотворення часток, оскільки ці частки використовуються при знаходженні поліномів $u(x)$ та $v(x)$). Ми отримаємо таку послідовність рівностей:

$$\begin{aligned} f(x) &= g(x) \cdot 1 + x^3 - 2x, \\ g(x) &= (x^3 - 2x) \cdot (x + 1) + x^2 - 2, \\ x^3 - 2x &= (x^2 - 2) \cdot x. \end{aligned}$$

Звідси випливає, що $r_3(x) = x^2 - 2$ є найбільшим спільним дільником заданих поліномів $f(x)$ та $g(x)$ і для знаходження $u(x)$, $v(x)$ побудуємо таблицю

i	0	1	2	3
$q_i(x)$		1	$x + 1$	x
$u_i(x)$	0	1	$-x - 1$	$x^2 + x + 1 = u(x)$
$v_i(x)$	1	-1	$x + 2$	$-x^2 - 2x - 1 = v(x)$

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

2. Нехай $F = \mathbb{Z}_3$ — поле лишків за модулем 3. Знайдемо НСД поліномів $f(x) = x^5 + 2x^4 + 2x^3 + x^2 + x + 2$, $g(x) = x^5 + x^3 + x \in \mathbb{Z}_3[x]$ і зобразимо цей найбільший спільний дільник у вигляді лінійної комбінації $f(x)$ та $g(x)$ над $\mathbb{Z}_3[x]$. Оскільки

$$\begin{aligned} f(x) &= g(x) \cdot 1 + 2x^4 + x^3 + x^2 + 2, \\ g(x) &= (2x^4 + x^3 + x^2 + 2) \cdot (2x + 2) + x^2 + 2, \\ 2x^4 + x^3 + x^2 + 2 &= (x^2 + 2) \cdot (2x^2 + 2) + x + 2, \\ x^2 + 2 &= (x + 2) \cdot (x + 1), \end{aligned}$$

то $r_3(x) = x + 2 \in \text{НСД}\{f(x), g(x)\}$, і для знаходження поліномів $u(x)$, $g(x) \in \mathbb{Z}_3[x]$, які задовольняють співвідношення $x + 2 = f(x)u(x) + g(x)v(x)$, побудуємо таблицю

i	0	1	2	3
$q_i(x)$		1	$2x + 2$	$2x^2 + 2$
$u_i(x)$	0	1	$x + 1$	$x^3 + 2x + 1 = u(x)$
$v_i(x)$	1	-1	$2x$	$x^3 + x^2 + 2 = v(x)$

Звідси випливає, що $x + 2 = f(x)(x^3 + 2x + 1) + g(x)(x^3 + x^2 + 2)$.

Унітарний найбільший спільний дільник поліномів $f(x)$, $g(x) \in F[x]$, хоча б один з яких є ненульовим, позначатимемо через $(f(x), g(x))$. У випадку $f(x) = g(x) = 0$ покладемо $(f(x), g(x)) = 0$.

Означення 9.11. Поліноми $f(x)$, $g(x) \in F[x]$ називають взаємно простими, якщо

$$(f(x), g(x)) = 1.$$

Теорема 9.12. Поліноми $f(x)$, $g(x) \in F[x]$ взаємно прості тоді і лише тоді, коли існують такі поліноми $u(x)$, $v(x) \in F[x]$, що

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1. \quad (9.20)$$

Доведення. Якщо $(f(x), g(x)) = 1$, то шукані поліноми $u(x)$, $v(x) \in F[x]$ існують за теоремою 9.11. Навпаки, якщо для деяких $u(x)$, $v(x) \in F[x]$ виконується рівність (9.20) і деякий поліном $d(x)$ є спільним дільником $f(x)$ та $g(x)$, то $d(x)$ мусить ділити 1. А тому, $(f(x), g(x)) = 1$. \square

Доведемо декілька простих, але важливих властивостей взаємно простих поліномів.

Теорема 9.13. Для довільних поліномів $f(x)$, $g(x)$, $h(x) \in F[x]$ правильні такі твердження:

- 1) якщо $(f(x), g(x)) = 1$ і $(f(x), h(x)) = 1$, то $(f(x), g(x)h(x)) = 1$;
- 2) якщо $(f(x), g(x)) = 1$ і добуток $f(x)h(x)$ ділиться на $g(x)$, то $h(x)$ ділиться на $g(x)$;
- 3) якщо $f(x)$ ділиться на кожен із поліномів $g(x)$ та $h(x)$ і $(g(x), h(x)) = 1$, то $f(x)$ ділиться на добуток $g(x)h(x)$;
- 4) якщо $(f(x), g(x)) = h(x) \neq 0$, то $\left(\frac{f(x)}{h(x)}, \frac{g(x)}{h(x)}\right) = 1$.

Доведення. 1) Дійсно, за співвідношенням (9.20) існують такі поліноми $u(x)$ та $v(x) \in F[x]$, що $f(x)u(x) + g(x)v(x) = 1$. Домножаючи цю рівність на $h(x)$, отримаємо

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

звідки випливає, що кожен спільний дільник $f(x)$ та $g(x)h(x)$ є дільником й $h(x)$; проте, за умовою твердження, $(f(x), h(x)) = 1$.

2) Домноживши рівність (9.20) на $h(x)$, отримаємо

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

Обидві складові лівої частини цієї рівності діляться на $g(x)$, а тому, як наслідок, на нього ділиться й $h(x)$.

3) Дійсно, оскільки $f(x) = g(x)\tilde{g}(x)$ для деякого $\tilde{g}(x) \in F[x]$, то за умовою твердження добуток з правої частини цієї рівності ділиться на $h(x)$. А оскільки $(g(x), h(x)) = 1$, то за попереднім твердженням $\tilde{g}(x)$ мусить ділитися на $h(x)$, тобто $\tilde{g}(x) = h(x)\tilde{h}(x)$ для деякого $\tilde{h}(x) \in F[x]$. Звідси отримаємо, що

$$f(x) = (g(x)h(x))\tilde{h}(x),$$

що й треба було довести.

4) За умовою $f(x) = h(x)\tilde{f}(x)$, $g(x) = h(x)\tilde{g}(x)$ для деяких $\tilde{f}(x)$, $\tilde{g}(x) \in F[x]$, а за теоремою 9.11 існують такі $u(x)$, $v(x) \in F[x]$, що

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

Тоді $h(x)\tilde{f}(x)u(x) + h(x)\tilde{g}(x)v(x) = h(x)$, тобто $h(x)(\tilde{f}(x)u(x) + \tilde{g}(x)v(x)) = h(x)$. Звідси отримуємо

$$h(x)(\tilde{f}(x)u(x) + \tilde{g}(x)v(x) - 1) = 0.$$

Оскільки кільце $F[x]$ не містить дільників нуля і $h(x) \neq 0$, то $\tilde{f}(x)u(x) + \tilde{g}(x)v(x) - 1 = 0$, тобто $\tilde{f}(x)u(x) + \tilde{g}(x)v(x) = 1$. Застосування до поліномів $\tilde{f}(x)$, $\tilde{g}(x)$ теореми 9.12 завершує доведення. \square

Поняття найбільшого спільного дільника може бути поширене на випадок довільної скінченної множини поліномів.

Означення 9.12. *Найбільшим спільним дільником поліномів $f_1(x), f_2(x), \dots, f_s(x) \in F[x]$ називається такий спільний дільник цих поліномів, який ділиться на будь-який інший спільний дільник цих поліномів.*

Існування найбільшого спільного дільника для довільної скінченної множини поліномів випливає із нижченаведеної теореми 9.14, яка також дає спосіб його обчислення.

Теорема 9.14. *Найбільший спільний дільник поліномів $f_1(x), f_2(x), \dots, f_s(x) \in F[x]$ дорівнює найбільшому спільному дільнику полінома $f_s(x)$ і найбільшому спільному дільнику поліномів $f_1(x), f_2(x), \dots, f_{s-1}(x)$.*

Доведення. Дійсно, при $s = 2$ теорема очевидна. Тому припустимо, що вона правильна для випадку $s - 1$ полінома, тобто уже доведено існування найбільшого спільного дільника $d(x)$ поліномів $f_1(x), f_2(x), \dots, f_{s-1}(x)$. Позначимо через $\tilde{d}(x)$ найбільший спільний дільник поліномів $d(x)$ та $f_s(x)$. Він буде, очевидно, спільним дільником для всіх заданих поліномів. З іншого боку, будь-який спільний дільник цих поліномів буде дільником також і для $d(x)$, а тому і для $\tilde{d}(x)$. \square

Означення 9.13. Поліноми $f_1(x), \dots, f_s(x) \in F[x]$ називаються *взаємно простими*, якщо їхній найбільший спільний дільник дорівнює 1.

Якщо $s > 2$, то попарно ці поліноми можуть і не бути взаємно простими.

Приклад 9.5. Поліноми $f(x) = x^3 - 7x^2 + 7x + 15$, $g(x) = x^2 - x - 20$, $h(x) = x^3 + x^2 - 12x$ взаємно прості, але $\text{НСД}(f(x), g(x)) = x - 5$, $\text{НСД}(f(x), h(x)) = x - 3$, $\text{НСД}(g(x), h(x)) = x + 4$.

Пропонуємо читачеві отримати узагальнення вище тверджень про взаємно прості поліноми для випадку довільної скінченної кількості поліномів.

Означення 9.14. *Найменшим спільним кратним (НСК) поліномів $f(x)$, $g(x) \in F[x]$ називають такий поліном $k(x) \in F[x]$, що*

- 1) $k(x)$ — спільне кратне поліномів $f(x)$, $g(x)$, тобто $f(x)$ та $g(x)$ ділять $k(x)$;
- 2) якщо $k_1(x)$ — будь-яке спільне кратне поліномів $f(x)$, $g(x)$, то $k(x)$ ділить $k_1(x)$.

Сукупність усіх описаних поліномів $k(x)$ позначається через $\text{НСК}\{f(x), g(x)\}$. Очевидно, що якщо один з поліномів $f(x)$ чи $g(x)$ нульовий, то $\text{НСК}\{f(x), g(x)\} = \{0\}$. В протилежному випадку правильною є така теорема.

Теорема 9.15. Якщо $f(x)$ та $g(x)$ — ненульові поліноми кільця $F[x]$, то існує єдиний унітарний поліном $k(x) \in \text{НСК}\{f(x), g(x)\}$ і виконується співвідношення

$$\text{НСК}\{f(x), g(x)\} = \{u k(x) \mid u \in F^*\}.$$

Унітарний поліном $k(x)$, який є найменшим спільним кратним ненульових поліномів $f(x), g(x) \in F[x]$, позначатимемо через $k(x) = [f(x), g(x)]$. Тепер результати теореми 9.15 можна коротко записати так

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

Доведення теореми 9.15 і узагальнення поняття НСК поліномів (та його властивостей) для випадку довільної скінченної множини поліномів пропонуємо читачеві провести самостійно.

9.5. Незвідні поліноми. Канонічний розклад полінома

Означення 9.15. Дільник $d(x) \in F[x]$ полінома $f(x) \in F[x]$ називається *власним*, якщо $0 < \deg d(x) < \deg f(x)$, і *невласним* в іншому випадку. Поліном $f(x) \in F[x]$ називається *незвідним над полем F* (або *незвідним в кільці $F[x]$*), якщо $\deg f(x) > 0$ і $f(x)$ не має власних дільників в кільці $F[x]$. Якщо поліном $f(x)$ має власний дільник в кільці $F[x]$, то він називається *звідним*.

Поліноми нульового степеня (тобто оборотні елементи) і нульовий поліном не є ні звідними, ні незвідними поліномами.

Оскільки за рівностю (9.14) степінь добутку будь-яких двох поліномів з $F[x]$ дорівнює сумі їхніх степенів, то очевидно правильним є таке твердження.

Твердження 9.16. Поліном $f(x) \in F[x]$ звідний тоді і тільки тоді, коли його можна зобразити у вигляді добутку двох поліномів, степені яких строго менші, ніж $\deg f(x)$.

Очевидно, що в кільці $F[x]$ незвідні всі поліноми першого степеня, проте можуть існувати поліноми більших степенів.

Зрозуміло, що якщо $f(x)$ — незвідний поліном з $F[x]$ степеня $n \geq 2$, то він не має коренів в F (в іншому випадку за теоремою Безу він має власний дільник степеня 1). Обернене твердження в загальному випадку (при $n \geq 4$) не правильне, однак правильне таке твердження.

Твердження 9.17. Поліном $f(x) \in F[x]$ степеня 2 або 3 незвідний над F тоді і тільки тоді, коли він не має коренів в F .

Доведення. Досить зауважити, що якщо $f(x)$ звідний, то він має унітарний дільник степеня 1, і скористатися теоремою Безу. \square

Приклад 9.6. В $\mathbb{Z}_2[x]$ незвідними є поліноми $x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1$, оскільки вони не мають в полі \mathbb{Z}_2 коренів. Поліном $x^4 + x^2 + 1$ також не має коренів в \mathbb{Z}_2 , але він звідний: $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.

Іноді один і той же поліном доводиться розглядати як поліном над різними полями. Наприклад, поліном $x^2 - 3 \in \mathbb{Q}[x]$ можна розглядати і як поліном над \mathbb{R} . У зв'язку з цим потрібно наголосити, що незвідність полінома це не просто властивість самого полінома, а властивість полінома по відношенню до того поля, над яким він розглядається. Так, поліном $x^2 - 3$ незвідний над \mathbb{Q} , оскільки його корені ірраціональні, але звідний над \mathbb{R} : $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$.

Для опису властивостей поліномів, пов'язаних з їх розкладанням на множники, потрібно спочатку описати властивості незвідних поліномів.

Твердження 9.18. Нехай $f(x) \in F[x]$ — незвідний поліном. Тоді

- 1) якщо $h(x)$ — довільний поліном з $F[x]$, то або $f(x)$ ділить $h(x)$, або $(f(x), h(x)) = 1$;
- 2) якщо $f(x)$ ділить добуток $h(x)p(x)$, де $h(x), p(x)$ — довільні поліноми з $F[x]$, то $f(x)$ ділить або $h(x)$, або $p(x)$;
- 3) якщо $g(x) \in F[x]$ — незвідний поліном, то або $(f(x), g(x)) = 1$, або поліноми $f(x)$ і $g(x)$ — асоційовані.

Доведення. 1) Нехай $f(x)$ не ділить $h(x)$. Тоді оскільки $(h(x), f(x)) = d(x) \in \{1, f(x)\}$ і $d(x)$ ділить $h(x)$, то $d(x) = 1$.

2) Нехай $f(x)$ ділить $h(x)p(x)$. Якщо $f(x)$ не ділить $h(x)$, то за першою властивістю $(h(x), f(x)) = 1$, і тоді за теоремою 9.13 (2) $f(x)$ ділить $p(x)$.

3) Якщо поліном $g(x)$ — незвідний і $g(x), f(x)$ не асоційовані, то за означенням 9.15 поліном $f(x)$ не ділить $g(x)$, а тоді за першою властивістю $(g(x), f(x)) = 1$. \square

Зауваження 9.6. Задача про розкладання довільного полінома з $F[x]$ на множники легко зводиться до аналогічної задачі для унітарного полінома, оскільки для будь-яких ненульових поліномів $f(x), g(x), h(x) \in F[x]$ поліном $f(x)$ незвідний над F тоді і тільки тоді, коли $f^*(x)$ незвідний, а рівність $f(x) = g(x) \cdot h(x)$ тягне рівність $f^*(x) = g^*(x) \cdot h^*(x)$. Перехід до унітарних поліномів виявляється досить зручним, оскільки істотно спрощує формульовання теорем і їхнє доведення. Наприклад, якщо $f(x), g(x)$ — унітарні поліноми, то для них твердження 9.18 (3) має вигляд: або $(f(x), g(x)) = 1$, або $f(x) = g(x)$.

Для поліномів над полем правильний такий аналог основної теореми арифметики.

Теорема 9.19. Будь-який унітарний поліном $f(x) \in F[x]$ ненульового степеня або незвідний над F , або розкладається у добуток унітарних незвідних над F поліномів, причому це розкладання однозначне з точністю до перестановки співмножників.

Доведення. Проведемо доведення методом повної математичної індукції за степенем $n = \deg f(x)$. При $\deg f(x) = 1$ твердження теореми правильне. Припустимо, що воно правильне для усіх унітарних ненульових поліномів степеня $\leq n$ і доведемо його правильність для поліномів степеня $n+1$. Нехай $\deg f(x) = n+1$. Якщо $f(x)$ незвідний над F , то твердження теореми правильне. Якщо ж поліном $f(x)$ — звідний, то він ділиться на деякий поліном $g(x) \in F[x]$, де $1 < \deg g(x) < n+1$. Тому $f(x) = g(x) \cdot h(x)$, де $1 < \deg h(x) < n+1$. За припущенням індукції кожен з поліномів $g(x), h(x)$ або незвідний над F , або розкладається у добуток унітарних незвідних над F поліномів, тобто

$$g(x) = g_1(x) \cdot \dots \cdot g_k(x), \quad h(x) = h_1(x) \cdot \dots \cdot h_l(x),$$

де $g_1(x), \dots, g_k(x), h_1(x), \dots, h_l(x)$ — незвідні унітарні поліноми, $k, l \in \mathbb{N}$. Звідси та з рівності $f(x) = g(x) \cdot h(x)$ отримуємо розкладання полінома $f(x)$ степеня $n+1$ у добуток незвідних унітарних поліномів

$$f(x) = g_1(x) \cdot \dots \cdot g_k(x) \cdot h_1(x) \cdot \dots \cdot h_l(x),$$

Отже, ми довели, що будь-який унітарний поліном $f(x) \in F[x]$ ненульового степеня може бути зображеній у вигляді

$$f(x) = p_1(x) \cdot p_2(x) \cdot \dots \cdot p_s(x), \tag{9.21}$$

де $s \geq 1$, поліноми $p_1(x), \dots, p_s(x)$ — незвідні, унітарні і $\deg p_1(x) \leq \dots \leq \deg p_s(x)$.

Однозначність розкладання (9.21) доведемо індукцією за параметром $s(f)$, де $s(f)$ — найменше значення s з усіх розкладів вигляду (9.21) для полінома $f(x)$. При $s(f) = 1$ це очевидно. Припустимо, що це правильно для всіх $f(x)$ при $s(f) < s$ та будь-якому фіксованому $s > 1$, і доведемо для $f(x)$ при $s(f) = s$. Нехай поряд з (9.21) існує зображення

$$f(x) = q_1(x) \cdot q_2(x) \cdot \dots \cdot q_t(x), \tag{9.22}$$

де $q_1(x), \dots, q_t(x)$ — незвідні унітарні поліноми і $\deg q_1(x) \leq \dots \leq \deg q_t(x)$. Оскільки $p_1(x)$ ділить $f(x)$, то за узагальненням властивості 2) з твердження 9.18 поліном $p_1(x)$ ділить $q_i(x)$ для деякого $i \in \overline{1, t}$, і тоді за властивістю 3) цього ж твердження поліноми $p_1(x) = q_i(x)$. Звідси та з нерівності $\deg q_1(x) \leq \deg q_i(x)$ отримуємо, що $\deg q_1(x) \leq \deg p_1(x)$. За симетрією отримаємо також $\deg p_1(x) \leq \deg q_1(x)$. Отже, поліноми $p_1(x) = q_1(x)$. Тепер з (9.21) і (9.22), враховуючи відсутність дільників нуля в $F[x]$, отримуємо два зображення для полінома $f(x)$

$$f(x) = p_1(x) \cdot (p_2(x) \cdot \dots \cdot p_s(x)) = p_1(x) \cdot (q_2(x) \cdot \dots \cdot q_t(x)).$$

За припущенням індукції добутки $p_2(x) \cdot \dots \cdot p_s(x)$ та $q_2(x) \cdot \dots \cdot q_t(x)$ збігаються, а тому збігаються й розкладання (9.21) і (9.22), що й потрібно було довести. \square

З першого твердження теореми 9.19 випливає, що будь-який поліном $f(x) \in F[x]$ степеня $n > 0$ можна зобразити у вигляді

$$f(x) = a_n \cdot p_1(x)^{k_1} \cdot p_2(x)^{k_2} \cdot \dots \cdot p_r(x)^{k_r}, \quad (9.23)$$

де a_n — старший коефіцієнт $f(x)$; $p_1(x), \dots, p_r(x)$ — унітарні, незвідні, попарно різні (тобто попарно взаємно прості) поліноми із $F[x]$ і $k_1, \dots, k_r \in \mathbb{N}$.

Означення 9.16. Зображення полінома $f(x)$ у вигляді (9.23) називають його *канонічним розкладанням над полем F* . Кожен поліном $p_i(x)$ називають *незвідним дільником $f(x)$* , а показник k_i — *кратністю $p_i(x)$ в канонічному розкладанні $f(x)$* . Поліноми $p_i(x)^{k_i}$ називають *примарними компонентами* полінома $f(x)$.

З другого твердження теореми 9.19 отримуємо такий наслідок.

Наслідок 9.20. Канонічний розклад полінома $f(x) \in F[x]$ степеня $n > 0$ визначено однозначно, з точністю до перестановки примарних компонент: якщо $f(x) = a_n \cdot h_1(x)^{l_1} \cdot \dots \cdot h_t(x)^{l_t}$ — інший канонічний розклад $f(x)$, то $r = t$ і існує така перестановка $(i_1, \dots, i_r) \in S_r$, що для $m = 1, 2, \dots, r$ виконуються рівності $h_m(x)^{l_m} = p_{i_m}(x)^{k_{i_m}}$, тобто $h_m(x) = p_{i_m}(x)$ і $l_m = k_{i_m}$.

Зауважимо, що з використанням понять канонічного розкладання і незвідного полінома часто вдається просто доводити взаємну простоту поліномів. В основі таких доведень лежить таке очевидне твердження.

Твердження 9.21. Поліноми $p_1(x), \dots, p_n(x) \in F[x]$ взаємно прості тоді і тільки тоді, коли вони не мають спільного незвідного дільника.

Як приклад використання цього твердження доведемо таке твердження.

Твердження 9.22. Якщо ненульові поліноми $p_1(x), \dots, p_n(x) \in F[x]$ попарно взаємно прості і $\bar{p}_i(x) = p_1(x) \cdot \dots \cdot p_{i-1}(x) \cdot p_{i+1}(x) \cdot \dots \cdot p_t(x)$ для $i \in \overline{1, t}$, то $(\bar{p}_1(x), \dots, \bar{p}_t(x)) = 1$.

Доведення. Нехай твердження невірне. Тоді за твердженням 9.21 існує незвідний поліном $f(x) \in F[x]$ такий, що $f(x)$ ділить $\bar{p}_i(x)$ для $i \in \overline{1, t}$. Звідси за твердженням 9.18 (2) отримуємо, що $f(x)$ ділить $p_j(x)$ для деякого $j \in \overline{1, t}$. Останнє суперечить твердженням 9.21, оскільки $f(x)$ ділить $\bar{p}_j(x)$, і за теоремою 9.13 (1) отримуємо $(p_j(x), \bar{p}_j(x)) = 1$. \square

З використанням теореми 9.19 доводиться така теорема.

Теорема 9.23. Для будь-якого поля F множина унітарних незвідних поліномів в кільці $F[x]$ нескінчена.

Зрозуміло, що це твердження нетривіальне лише для скінчених полів і в цьому випадку з теореми випливає очевидний наслідок.

Наслідок 9.24. Якщо F — скінченне поле, то для кожного натурального числа m в кільці $F[x]$ існує незвідний поліном степеня $n \geq m$.

Зауважимо, що в сучасній прикладній математиці вельми важливими є задачі розробки алгоритмів, що дозволяють за допомогою комп’ютерів швидко будувати поліноми великих степенів над скінченими полями і розкладати поліноми над такими полями на незвідні множники.

9.6. Значення та корені поліномів. Теорема Безу. Поліном як функція

Означення 9.17. Значенням полінома $f(x) = a_0 + a_1x + \dots + a_nx^n$ із кільця $F[x]$ у точці $c \in F$ називають елемент із F вигляду

$$f(c) = a_0 + a_1c + \dots + a_nc^n.$$

Елемент $c \in F$ називається коренем полінома $f(x) \in F[x]$, якщо $f(c) = 0$.

Важливий зв’язок між поняттями подільності і кореня полінома встановлює така теорема.

Теорема 9.25 (Безу). Остача від ділення полінома $f(x) \in F[x]$ на двочлен $x - c \in F[x]$ дорівнює $f(c)$. Зокрема, елемент c поля F є коренем полінома $f(x)$ тоді і тільки тоді, коли $f(x)$ ділиться на $(x - c)$.

Доведення. За теоремою 9.4 поліном $f(x)$ можна поділити з остачею на $x - c$, тобто для деякого $q(x) \in F[x]$

$$f(x) = (x - c)q(x) + r(x), \quad \text{де } \deg r(x) < 1.$$

Тоді $r(x) = rx^0$, де $r \in F$, і $r(c) = r$. Звідси випливає, що

$$f(c) = (c - c)q(c) + r(c) = 0 + r = r.$$

Зокрема, рівність $f(c) = 0$ еквівалентна рівності $r = 0$, а останнє за твердженням 9.5 еквівалентне тому, що $x - c$ ділить $f(x)$. \square

Зауваження 9.7. Ділення з остачею полінома на двочлен $(x - c)$ здійснюється за простою схемою, яка називається схемою Горнера. Розглянемо її детальніше. Нехай

$$a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - c)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x + b_0) + r.$$

Прирівнюючи коефіцієнти біля відповідних степенів x , отримаємо ланцюг рівностей

$$a_n = b_{n-1}, \quad a_{n-1} = b_{n-2} - cb_{n-1}, \quad \dots, \quad a_1 = b_0 - cb_1, \quad a_0 = r - cb_0,$$

звідки легко знайти рекурентні формулі для $b_{n-1}, b_{n-2}, \dots, b_0$ та r

$$b_{n-1} = a_n, \quad b_{n-2} = cb_{n-1} + a_{n-1}, \quad \dots, \quad b_0 = cb_1 + a_1, \quad r = cb_0 + a_0. \quad (9.24)$$

Вихідні дані і результати обчислень зручно розташовувати у вигляді таблиці

	a_n	a_{n-1}	a_{n-2}	\dots	a_1	a_0	
c	b_{n-1}	b_{n-2}	b_{n-3}	\dots	b_0	r	

або, зважаючи на (9.24), у вигляді

	a_n	a_{n-1}	a_{n-2}	\dots	a_1	a_0	
c	a_n	$cb_{n-1} + a_{n-1}$	$cb_{n-2} + a_{n-2}$	\dots	$cb_1 + a_1$	$cb_0 + a_0$	

Теорема 9.25 та схема Горнера дають дуже ефективний спосіб обчислення значень полінома.

Приклади 9.7. 1. Знайдемо значення полінома $f(x) = 2x^6 - 11x^4 - 19x^3 - 7x^2 + 8x + 5$ у точці $x = 3$. За схемою Горнера отримуємо:

$$\begin{array}{c|ccccccc} & 2 & 0 & -11 & -19 & -7 & 8 & 5 \\ \hline 3 & 2 & 6 & 7 & 2 & -1 & 5 & 20 \end{array}$$

Отже, $f(3) = 20$.

2. Доведемо, що число $x = 2$ є коренем полінома $f(x) = x^5 - 3x^4 + 3x^3 - 4x^2 - 2x + 12$. Для цього поділимо цей поліном на двочлен $x - 2$. Отримаємо

$$\begin{array}{c|cccccc} & 1 & -3 & 3 & -4 & -2 & 12 \\ \hline 2 & 1 & -1 & 1 & -2 & -6 & 0 \end{array}$$

Отже, $f(x) = (x - 2)(x^4 - x^3 + x^2 - 2x - 6)$, тобто поліном $f(x)$ ділиться на двочлен $x - 2$, і тому за теоремою Безу $x = 2$ є коренем цього полінома.

Означення 9.17. дозволяє поставити у відповідність кожному поліному $f(x) \in F[x]$ функцію $f_F: F \rightarrow F$, яка визначається умовою

$$f_F(c) = f(c) \text{ для довільного } c \in F.$$

У загальному випадку поліноми не слід ототожнювати з функціями. Наприклад, різні поліноми x^2 і x з кільця $\mathbb{Z}_2[x]$ визначають одну і ту ж функцію із \mathbb{Z}_2 в \mathbb{Z}_2 . З іншого боку, на довільному кільці R не кожну функцію $\varphi: R \rightarrow R$ можна задати у вигляді $\varphi = f_R$ для відповідного $f(x) \in R[x]$. Проте виявляється, що випадок, коли різні поліноми визначають одну і ту ж функцію, можливий лише тоді, коли поле F скінченне.

Означення 9.18. Відображення φ кільця R в себе називають *поліноміальним*, якщо для деякого $f(x) \in R[x]$ виконується рівність $\varphi = f_R$. У цьому випадку кажуть, що φ задається поліномом $f(x)$.

Теорема 9.26. Якщо у полі F є n попарно різних елементів c_1, \dots, c_n , то для довільних $d_1, \dots, d_n \in F$ існує єдиний поліном $f(x) \in F[x]$ з властивостями

$$f(c_i) = d_i \text{ для } i \in \overline{1, n}, \deg f(x) < n. \quad (9.25)$$

Доведення. Поліном $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in F[x]$ задовольняє умовам (9.25) тоді і тільки тоді, коли вектор $(a_0, a_1, \dots, a_{n-1})$ є розв'язком системи лінійних рівнянь

$$\begin{pmatrix} 1 & c_1 & c_1^2 & \dots & c_1^{n-1} \\ 1 & c_2 & c_2^2 & \dots & c_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & c_n & c_n^2 & \dots & c_n^{n-1} \end{pmatrix} \cdot X = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}. \quad (9.26)$$

Ця система має розв'язок, причому єдиний, оскільки визначник її основної матриці є визначником Вандермонда (див. (3.19)), який відмінний від нуля за умовою. \square

Зауваження 9.8. Для побудови полінома з властивостями (9.25) зовсім не обов'язково розв'язувати систему (9.26), оскільки він, очевидно, описується формулою

$$\begin{aligned} f(x) = \sum_{i \in \overline{1, n}} \frac{d_i}{(c_i - c_1) \cdot \dots \cdot (c_i - c_{i-1}) \cdot (c_i - c_{i+1}) \cdot \dots \cdot (c_i - c_n)} \times \\ \times (x - c_1) \cdot \dots \cdot (x - c_{i-1}) \cdot (x - c_{i+1}) \cdot \dots \cdot (x - c_n), \end{aligned}$$

яка називається *інтерполяційною формuloю Лагранжа*.

Наслідок 9.27. Поліном степеня $n > 0$ над полем F має в цьому полі не більше n різних коренів.

Доведення. у протилежному випадку він приймає нульове значення у $n+1$ точках із F і за теоремою співпадає з поліномом $0 + 0x + \dots + 0x^n$. \square

З цього результату, зокрема, випливає, що для комплексного числа z в полі \mathbb{C} існує не більше n різних коренів степеня n з z , оскільки всі вони є коренями полінома $x^n - z$ (див. рівність (8.16)). Звідси ж випливає, що якщо поле F — нескінченне, то існують не поліноміальні відображення $\varphi: F \rightarrow F$. Наприклад, таким є відображення φ , яке приймає значення 0 на нескінченні множині точок з F , але не рівне тоді нулю. (Доведіть!)

Наслідок 9.28. Якщо F — нескінченне поле, то поліноми $f(x), g(x) \in F[x]$ рівні тоді і тільки тоді, коли рівні функції $f_F(x), g_F(x)$.

9.7. ПОХІДНА ПОЛІНОМА ТА КРАТНІ КОРЕНІ

В алгебрі та її застосуваннях широко використовується така класифікація поліномів.

Означення 9.19. Нехай $k \in \mathbb{N}$. Елемент c поля F називають *k-кратним коренем* полінома $f(x) \in F[x]$, якщо $f(x)$ ділиться в кільці $F[x]$ на $(x - c)^k$ і не ділиться на $(x - c)^{k+1}$. Корені кратності > 1 називають *кратними*, а 1-кратні корені — *простими*. Якщо $k = 2$ або $k = 3$, то c називають *подвійним* або *потрійним коренем* полінома $f(x)$. Інколи зручно вважати, що число, яке не є коренем, — це корінь кратності 0.

Очевидно, що кратність кореня c полінома $f(x)$ співпадає з кратністю двочлена $x - c$ у канонічному розкладі $f(x)$ над F .

Наведемо теорему, яка суттєво підсилює теорему 9.27

Теорема 9.29. Поліном $f(x)$ степеня $n > 0$ над полем F має в цьому полі не більше n коренів з врахуванням їхніх кратностей, тобто якщо c_1, \dots, c_m — різні корені полінома $f(x)$ у полі F і їхні кратності дорівнюють відповідно k_1, \dots, k_m , то $k_1 + \dots + k_m \leq n$.

Доведення. Оскільки за першим твердженням теореми 9.13 поліноми $(x - c_1)^{k_1}, \dots, (x - c_m)^{k_m}$ попарно взаємно прості і кожний з них ділить $f(x)$, то за третім твердженням теореми 9.13 добуток $(x - c_1)^{k_1} \cdot \dots \cdot (x - c_m)^{k_m}$ ділить $f(x)$. Звідси за співвідношенням (9.14) отримуємо, що $n \geq k_1 + \dots + k_m$. \square

Зручний спосіб розрізнення простих і кратних коренів полінома в полі пов'язаний з поняттям похідної полінома. В алгебрі це поняття вводиться формально, за аналогією з відомим з курсу математичного аналізу описом похідної полінома в $\mathbb{R}[x]$.

Означення 9.20. Нехай F — поле. Відображення $\frac{d}{dx}: F[x] \rightarrow F[x]$, для якого

$$\frac{d}{dx}(a_0 + a_1x + \dots + a_nx^n) = a_1 + 2a_2x + \dots + na_nx^{n-1},$$

називають *диференціюванням*.

Якщо $f(x) \in F[x]$, то $\frac{d}{dx}(f(x))$ позначають через $f'(x)$ і називають *похідною* полінома $f(x)$. Якщо до полінома $f(x)$ застосувати відображення $\frac{d}{dx}$ k разів, то одержимо k -ту похідну цього полінома, яку позначають $f^{(k)}(x)$.

Незважаючи на настільки формальне означення, похідна зберігає властивості, відомі з курсу математичного аналізу.

Твердження 9.30. Для довільних поліномів $f(x), g(x) \in F[x]$ правильні такі рівності:

$$(f(x) + g(x))' = f'(x) + g'(x); \quad (9.27)$$

$$(a \cdot f(x))' = a \cdot f'(x), \text{ де } a \in F, \deg f(x) \geq 1; \quad (9.28)$$

$$(f(x)g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x); \quad (9.29)$$

$$(f(x)^s)' = s \cdot f(x)^{s-1} \cdot f'(x). \quad (9.30)$$

Доведення. Співвідношення (9.27) і (9.28) безпосередньо випливають з означень похідної та правила додавання поліномів. Нехай $f(x) = a_0 + a_1x + \dots + a_nx^n$, $g(x) = b_0 + b_1x + \dots + b_mx^m$. Оскільки добуток поліномів є сумою добутків поліномів вигляду $a_i x^i \cdot b_j x^j$, то, беручи до уваги (9.27), співвідношення (9.29) досить довести у випадку $f(x) = a_i x^i$, $g(x) = b_j x^j \in F[x]$. Маємо

$$(a_i x^i \cdot b_j x^j)' = (a_i b_j x^{i+j})' = (i+j)a_i b_j x^{i+j-1},$$

$$(a_i x^i)' b_j x^j + a_i x^i (b_j x^j)' = ia_i b_j x^{i+j-1} + ja_i b_j x^{i+j-1} = (i+j)a_i b_j x^{i+j-1}.$$

З рівності правих частин останніх двох співвідношень випливає рівність їхніх лівих частин, що й треба було довести. Для доведення (9.30) скористаємося методом математичної індукції. Випадок $s = 1$ очевидний. Припустимо, що співвідношення (9.30) виконується для показника s . Використовуючи (9.29) для $g(x) = f(x)^s$, маємо

$$(f(x)^{s+1})' = (f(x) \cdot f(x)^s)' = f'(x)f(x)^s + f(x)s f^{s-1}(x)f'(x) = (s+1)f(x)^s f'(x),$$

що й треба було довести. \square

Зауваження 9.9. Цілком аналогічно похідну можна визначити для поліномів над будь-яким (не обов'язково комутативним) кільцем з одиницею. (Перевірте!)

Твердження 9.31. Корінь $c \in F$ полінома $f(x) \in F[x]$ є простим тоді і тільки тоді, коли c не є коренем його похідної $f'(x)$, тобто $f'(c) \neq 0$.

Доведення. Нехай k — кратність кореня c , тобто $f(x) = (x - c)^k g(x)$, де $g(c) \neq 0$. Звідси за твердженням 9.30 маємо

$$f'(x) = k(x - c)^{k-1}g(x) + (x - c)^k g'(x). \quad (9.31)$$

Якщо $k = 1$, то звідси випливає, що $f'(c) = g(c) \neq 0$. Якщо ж $k > 1$, то $f'(c) = k(c - c)^{k-1}g(c) + (c - c)^k g'(c) = 0$ (тобто з умови $f'(c) \neq 0$ випливає, що $k = 1$). \square

Твердження 9.31 допускає уточнення у випадку, коли поле F має характеристику 0.

Означення 9.21. Кажуть, що кільце з 1 (зокрема, поле) має *характеристику 0*, якщо не існує ненульових натуральних чисел n з властивістю $n \cdot 1 = \underbrace{1 + \dots + 1}_n = 0$.

Наприклад, кільце \mathbb{Z} має характеристику 0, а кільце $\mathbb{Z}/2\mathbb{Z}$ не має цієї властивості, бо $2 \cdot \bar{1} = \bar{0}$ в $\mathbb{Z}/2\mathbb{Z}$.

Твердження 9.32. Нехай F — поле характеристики 0. Якщо елемент $c \in F$ є k -кратним коренем полінома $f(x) \in F[x]$, то c є $(k-1)$ -кратним коренем полінома $f'(x)$.

Доведення. Запишемо (9.31) у вигляді

$$f'(x) = (x - c)^{k-1}(kg(x) + (x - c)g'(x)).$$

Оскільки F має характеристику 0, то поліном $kg(x)$ ненульовий. Звідси випливає, що $x - c$ не ділить $kg(x) + (x - c)g'(x)$, тобто c є $(k-1)$ -кратним коренем полінома $f'(x)$. \square

Приклад 9.8. Розкладемо поліном $f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8 \in \mathbb{R}[x]$ за степенями двочлена $x - 2$. Послідовне ділення з остачею на $x - 2$ будемо проводити за схемою Горнера, використовуючи рядок результатів кожного ділення як рядок вихідних даних для наступного ділення:

	1	-5	7	-2	4	8
2	1	-3	1	0	4	0
2	1	-1	-1	-2	0	
2	1	1	1	0		
2	1	3	7			
2	1	5				
2	1					

Таким чином, число 2 є трикратним коренем полінома $f(x)$ і

$$f(x) = (x - 2)^5 + 5(x - 2)^4 + 7(x - 2)^3.$$

Крім того, $f'''(2) = 3! \cdot 7 = 42$, $f^{(IV)}(2) = 4! \cdot 5 = 120$, $f^{(V)}(2) = 5! \cdot 1 = 120$.

З твердження 9.32 випливає наслідок, який може бути корисним при знаходженні коренів поліномів.

Наслідок 9.33. Нехай $f(x) \in F[x]$ — поліном над полем F характеристики 0. Множина кратних коренів у полі F полінома $f(x)$ співпадає з множиною усіх коренів у полі F полінома $d(x) = (f(x), f'(x))$.

Доведення. Для довільного елемента $c \in F$ рівність $f(c) = f'(c) = 0$ можлива тоді і лише тоді, коли двочлен $x - c$ ділить і $f(x)$, і $f'(x)$. А це у свою чергу рівносильно тому, що $x - a$ ділить $d(x)$, тобто $d(c) = 0$. \square

Означення 9.22. Поле F називається *полем розкладання полінома* $f(x) \in F[x]$ степеня $n > 0$, якщо $f(x)$ розкладається над F у добуток лінійних множників, тобто якщо канонічне розкладання $f(x)$ над F має вигляд

$$f(x) = (x - c_1)^{k_1} \cdots \cdot (x - c_r)^{k_r}.$$

Приклади 9.9. 1. Для полінома $x^2 + 1$ поле \mathbb{C} є полем розкладання, а поле \mathbb{R} — ні.

2. Для будь-якого простого $p \in \mathbb{N}$ поле \mathbb{Z}_p лишків за модулем p є полем розкладання полінома $x^p - x$, тобто

$$x^p - x = x \cdot (x - 1) \cdot \dots \cdot (x - (p - 1)). \text{ (Доведіть!)}$$

Наслідок 9.34. Якщо F — поле розкладання полінома $f(x) \in F[x]$, то $f(x)$ не має кратних коренів у F тоді і тільки тоді, коли $(f(x), f'(x)) = 1$.

Доведення. Поліном $d(x) = (f(x), f'(x))$ ділить $f(x)$, а тому, якщо $\deg d(x) > 0$, то за умовою теореми $d(x)$ розкладається над F на лінійні множники і має в F корінь. В ситуації, яка розглядається, відсутність в $f(x)$ кратних коренів в полі F за наслідком 9.33 рівносильно умові $\deg d(x) = 0$. \square

Зауваження 9.10. Якщо F не є полем розкладання для $f(x)$, то умова $(f(x), f'(x)) = 1$ є достатньою для відсутності кратних коренів полінома $f(x)$ в полі F , але не є необхідною. (Доведіть!)

Отримані результати можна використовувати не тільки для знаходження кратних коренів полінома, а й для розкладання його на множники в випадку наявності у нього таких коренів.

Приклад 9.10. Знайдемо кратні корені в полі \mathbb{Z}_5 полінома $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1 \in \mathbb{Z}_5[x]$. Обчислюючи найбільший спільний дільник $f(x)$ і $f'(x) = 4x^3 - x^2 + 4x - 2$, отримуємо $(f(x), f'(x)) = x - 1$. Отже, 1 є кратним коренем полінома $f(x)$ і $(x - 1)^2$ ділить $f(x)$. Виконуючи ділення, знаходимо $f(x) = (x - 1)^2(x^2 + 1)$. Безпосередньо перевіркою перевірюємося, що поліном $x^2 + 1$ має в полі \mathbb{Z}_5 корені 2 і 3. Таким чином, $f(x) = (x - 1)^2(x - 2)(x - 3)$.

9.8. Формули Віста

Якщо унітарний поліном

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \quad (9.32)$$

розкладається на лінійні множники, то цей розклад може бути записано у вигляді

$$f(x) = (x - c_1)(x - c_2) \dots (x - c_n), \quad (9.33)$$

де c_1, c_2, \dots, c_n — корені полінома $f(x)$, причому кожен із них повторюється стільки разів, яка його кратність. Прирівнюючи у зображеннях (9.32) та (9.33) коефіцієнти при відповідних степенях x , отримаємо, так звані, *формули Віста*:

$$\begin{aligned} a_{n-1} &= -(c_1 + c_2 + \dots + c_n), \\ a_{n-2} &= c_1 c_2 + c_1 c_3 + \dots + c_1 c_n + c_2 c_3 + \dots + c_{n-1} c_n, \\ &\dots \\ a_k &= (-1)^{n-k} \sum_{i_1 < i_2 < \dots < i_k} c_{i_1} c_{i_2} \dots c_{i_k}, \\ &\dots \\ a_1 &= (-1)^{n-1} (c_1 c_2 \dots c_{n-1} + c_1 c_2 \dots c_{n-2} c_n + \dots + c_2 c_3 \dots c_n), \\ a_0 &= (-1)^n c_1 c_2 \dots c_n. \end{aligned} \tag{9.34}$$

Приклад 9.11. Знайдемо унітарний поліном $f(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$, для якого число 1 є 2-кратним коренем, а числа 2 та 3 — простими. За формулами Віста

$$\begin{aligned} a_3 &= -(1 + 1 + 2 + 3) = -7, \\ a_2 &= 1 \cdot 1 + 1 \cdot 2 + 1 \cdot 3 + 1 \cdot 2 + 1 \cdot 3 + 2 \cdot 3 = 17, \\ a_1 &= -(1 \cdot 1 \cdot 2 + 1 \cdot 1 \cdot 3 + 1 \cdot 2 \cdot 3 + 1 \cdot 2 \cdot 3) = -17, \\ a_0 &= 1 \cdot 1 \cdot 2 \cdot 3 = 6. \end{aligned}$$

Таким чином, $f(x) = x^4 - 7x^3 + 17x^2 - 17x + 6$.

9.9. Спільний множник двох поліномів. Результант

Якщо два поліноми $f(x)$ і $g(x)$ над полем F мають спільний корінь $c \in F$, то вони мають спільний множник, який входить $x - c$, і навпаки. Тому варто розглянути таку задачу: коли два поліноми $f(x), g(x) \in F[x]$ мають спільний множник?

Нехай $f(x), g(x) \in F[x]$, де F — поле. *Константами* або *постійними поліномами* будемо називати поліноми нульового степеня і 0.

Теорема 9.35. Поліноми $f(x)$ і $g(x)$ мають спільний множник, відмінний від константи, тоді і тільки тоді, коли існують такі поліноми $f_1(x), g_1(x) \in F[x]$, що $\deg f_1(x) < \deg f(x)$, $\deg g_1(x) < \deg g(x)$ і $f(x)g_1(x) = f_1(x)g(x)$.

Доведення. Якщо поліноми $f(x)$ і $g(x)$ мають спільний множник $h(x)$, то $f(x) = f_1(x)h(x)$, $g(x) = g_1(x)h(x)$, $\deg f_1(x) < \deg f(x)$, $\deg g_1(x) < \deg g(x)$ і $f(x)g_1(x) = f_1(x)g_1(x)h(x) = f_1(x)g(x)$.

Навпаки, нехай $f(x)g_1(x) = f_1(x)g(x)$, $\deg f_1(x) < \deg f(x)$, $\deg g_1(x) < \deg g(x)$. Розкладемо $f(x)$ і $g(x)$ в добуток незвідних поліномів. Не всі незвідні множники полінома $f(x)$ входять в $f_1(x)$, бо $\deg f_1(x) < \deg f(x)$, тому з рівності $f(x)g_1(x) = f_1(x)g(x)$ випливає, що деякі незвідні множники $f(x)$ входять в $g(x)$, а це і означає, що $f(x)$ і $g(x)$ мають спільний множник. \square

Означення 9.23. Нехай $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $g(x) = b_0 + b_1 x + \dots + b_m x^m$ — поліноми з кільця $F[x]$. Визначник

$$\text{Res}(f(x), g(x)) = \left| \begin{array}{cccccc} a_0 & a_1 & \dots & a_n & & \\ & a_0 & a_1 & \dots & a_n & \\ & & \dots & \dots & \dots & \\ b_0 & b_1 & \dots & b_m & & \\ & b_0 & b_1 & \dots & b_m & \\ & & \dots & \dots & \dots & \\ & b_0 & b_1 & \dots & b_m & \end{array} \right|_m^n$$

називають *результантом* поліномів $f(x)$ і $g(x)$.

Теорема 9.36. Поліноми $f(x), g(x) \in F[x]$ мають непостійний спільний множник тоді й лише тоді, коли $\text{Res}(f(x), g(x)) = 0$.

Доведення. Нехай поліноми $f(x)$ і $g(x)$ мають непостійний спільний множник. Тоді за теоремою 9.35 існують ненульові поліноми

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

для яких $f(x)g_1(x) = g(x)f_1(x)$. Порівнюючи відповідні коефіцієнти добутків $f(x)g_1(x)$ і $g(x)f_1(x)$, одержимо

$$\begin{cases} a_0b_0^{(1)} = b_0a_0^{(1)}, \\ a_1b_0^{(1)} + a_0b_1^{(1)} = b_1a_0^{(1)} + b_0a_1^{(1)}, \\ \dots \\ a_nb_m^{(1)} = b_ma_n^{(1)}. \end{cases} \quad (9.35)$$

Цю систему рівностей можна трактувати як систему лінійних однорідних рівнянь стосовно невідомих $b_0^{(1)}, \dots, a_n^{(1)}$. Ця система має $m+n$ рівнянь, $m+n$ невідомих і має ненульовий розв'язок. Отже визначник цієї системи, який з точністю до знаку є $\text{Res}(f(x), g(x))$, дорівнює нулю.

Навпаки, якщо $\text{Res}(f(x), g(x)) = 0$, то система (9.35) має ненульовий розв'язок в полі F . Якщо не всі $a_i^{(1)}$ дорівнюють нулю, то $f_1(x) \neq 0$, отже і $g_1(x) \neq 0$, а оскільки $f(x)g_1(x) = f_1(x)g(x)$, то за теоремою 9.35 поліноми $f(x)$ і $g(x)$ мають непостійний множник. \square

9.10. Основна теорема алгебри

Нехай F — довільне поле. Нагадаємо, що підмножина $P \subset F$ називається підполем поля F , якщо P замкнута щодо операцій додавання і множення на F і є полем щодо цих операцій. У цій ситуації говорять також, що поле F є розширенням поля P . Для будь-якого поля P і будь-якого полінома $f(x) \in P[x]$ існує розширення F поля P , яке є полем розкладання для $f(x)$. Насправді, правильне навіть більш сильне твердження — теорема Штейніца¹.

Означення 9.24. Поле F називається алгебрично замкнутим, якщо воно є полем розкладання для будь-якого полінома $f(x) \in F[x], \deg f(x) > 0$.

Теорема 9.37 (Штейніц). Для будь-якого поля P існує розширення F , яке є алгебрично замкнутим.

Доведення цього результату виходить за рамки нашого курсу. Ми обмежимося тут лише формулюванням одного дуже важливого прикладу.

Теорема 9.38. Будь-який поліном ненульового степеня над полем \mathbb{C} комплексних чисел має в цьому полі хоча б один корінь (іншими словами, поле \mathbb{C} алгебрично замкнute).

Ця теорема, яку довгий час називали «основною теоремою алгебри», не має чисто алгебричного доведення і може бути виведена як простий наслідок з теореми Ліувілля про обмеженість цілих аналітичних функцій при вивченні теорії функцій комплексної змінної.

Зауважимо також, що назва «основна теорема алгебри» — це даніна традиції; вона нагадує про часи, коли основною задачею алгебри була задача знаходження коренів поліномів. Основна теорема алгебри вперше була сформульована (у вигляді, що відрізняється від сучасного) А. Жірапом і Р. Декартом. Пізніше К. Маклорен і Л. Ейлер сформулювали її у вигляді, що еквівалентний сучасному:

¹Ернст Штейніц (нім. Ernst Steinitz; 13 червня 1871 – 29 вересня 1928) — німецький математик. Основні наукові результати з алгебричної теорії чисел, алгебри і геометрії.

кожний поліном з дійсними коефіцієнтами можна розкласти в добуток лінійних та квадратичних поліномів з дійсними коефіцієнтами. Першим, хто опублікував доведення, був Ж. Д'Аламбер (1746р.), після цього в другій половині XVIII ст. з'являються доведення Л. Ейлера, П. Лапласа, Ж. Лагранжа та інших математиків; всі ці доведення мали певні недоліки. Перше строгое доведення основної теореми алгебри запропонував К. Гаус, який у 1808–1817 рр. опублікував декілька різних доведень цієї теореми. Зараз існує багато доведень основної теореми алгебри. Пропонуємо читачеві ознайомитися хоч з одним з них самостійно.

9.11. Поліноми над числовими полями

Хоча ми обмежилися лише формулюванням теореми 9.38, проте уже зараз будемо широко її використовувати. Зокрема, використаємо її для опису незвідних поліномів над полями \mathbb{C} і \mathbb{R} , деяких важливих достатніх умов незвідності поліномів над \mathbb{Q} і способів обчислення раціональних коренів поліномів з $\mathbb{Q}[x]$.

Твердження 9.39. Незвідними поліномами в кільці $\mathbb{C}[x]$ є поліноми першого степеня і тільки вони.

Доведення. Нехай $f(x)$ — ненульовий поліном з кільця $\mathbb{C}[x]$. Міркуємо індукцією за степенем n полінома $f(x)$. Якщо $n = 1$, то доводити нічого. Нехай $n > 1$ і твердження доведено для всіх поліномів степеня, меншого n . За основною теоремою алгебри існує таке $c_1 \in \mathbb{C}$, що $f(c_1) = 0$. Тоді за теоремою Безу $f(x) = (x - c_1)f_1(x)$. Оскільки $\deg f_1(x) < n$, то за припущенням індукції $f_1(x)$ розкладається на лінійні множники, а тому ми одержуємо шукане розкладання полінома $f(x)$. \square

Наслідок 9.40. Будь-який поліном ненульового степеня над полем \mathbb{C} розкладається в $\mathbb{C}[x]$ на лінійні множники.

Тепер можна коротко довести таке твердження (див. теорему 8.11).

Твердження 9.41. Для довільного ненульового $z \in \mathbb{C}$ і довільного $n \in \mathbb{N}$ у полі \mathbb{C} існує рівно n різних коренів степеня n із z .

Доведення. За наслідком 9.40 поліном $x^n - z$ розкладається на лінійні множники над \mathbb{C} , а за наслідком 9.34 він не має кратних коренів в \mathbb{C} , тобто у полі \mathbb{C} у нього є рівно n різних коренів. \square

Нагадаємо, що *дискримінантом полінома* $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$, $a \neq 0$, називається число $D(f) = b^2 - 4ac$, і поліном $f(x)$ не має коренів в \mathbb{R} тоді й лише тоді, коли $D(f) < 0$.

Теорема 9.42. В кільці $\mathbb{R}[x]$ незвідними поліномами є поліноми першого степеня та квадратні тричлени з від'ємними дискримінантами і тільки вони.

Доведення. Незвідність вказаних поліномів очевидна (див. твердження 9.17). Покажемо, що інших незвідних поліномів в $\mathbb{R}[x]$ немає.

Нехай $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{R}[x]$ — незвідний поліном степеня $n > 1$. Тоді він не має коренів в \mathbb{R} , але за основною теоремою алгебри має корінь $z \in \mathbb{C}$. В такому випадку $z \neq \bar{z}$ (оскільки $z \notin \mathbb{R}$), і тому \bar{z} — також є коренем $f(x)$, оскільки за твердженням 8.5 маємо

$$0 = \bar{0} = \overline{a_0 + a_1z + \dots + a_nz^n} = \bar{a}_0 + \bar{a}_1\bar{z} + \dots + \bar{a}_n\bar{z}^n = a_0 + a_1\bar{z} + \dots + a_n\bar{z}^n = f(\bar{z}).$$

Тоді за теоремою Безу поліном $f(x)$ ділиться у кільці $\mathbb{C}[x]$ на два поліноми $x - z$ і $x - \bar{z}$, а оскільки ці поліноми взаємно прості, то за теоремою 9.13 (3) поліном $f(x)$ ділиться на $g(x) = (x - z)(x - \bar{z})$. Оскільки $g(x) = x^2 - (z + \bar{z})x + z\bar{z}$ — також поліном з $\mathbb{R}[x]$, то $g(x)$ ділить $f(x)$ в $\mathbb{R}[x]$. Оскільки у $f(x)$ немає власних дільників в $\mathbb{R}[x]$, то $f(x)$ асоційований з $g(x)$. Як наслідок, $f(x)$ — поліном степеня 2, і оскільки його корені в \mathbb{C} не належать \mathbb{R} , то $D(f) < 0$. \square

Наслідок 9.43. Будь-який поліном непарного степеня із $\mathbb{R}[x]$ має корінь в \mathbb{R} .

Значно більш складніше властивості поліномів в $\mathbb{Q}[x]$. Повного їх опису не існує, але можна вказати деякі чималі класи таких поліномів. Один з основних методів вивчення можливостей розкладання поліномів з $\mathbb{Q}[x]$ на множники полягає в зведенні задачі до розкладання поліномів в кільці $\mathbb{Z}[x]$.

Означення 9.25. Поліном $h(x) = c_0 + c_1x + \dots + c_nx^n$ степеня $n \geq 0$ з цілими коефіцієнтами назовемо примітивним, якщо $c_n > 0$ і $(c_0, c_1, \dots, c_n) = 1$.

Твердження 9.44. Для кожного ненульового полінома $f(x) \in \mathbb{Q}[x]$ в кільці $\mathbb{Z}[x]$ існує єдиний асоційований з ним примітивний поліном $f^*(x)$.

Доведення. Якщо $\deg f(x) = n$, то $f(x)$ можна зобразити у вигляді $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \dots + \frac{a_n}{b_n}x^n$, де $a_i \in \mathbb{Z}$, $b_i \in \mathbb{N}$ для $i \in \overline{0, n}$. Нехай c — найменше спільне кратне елементів b_0, b_1, \dots, b_n . Тоді $c \cdot f(x) = c_0 + c_1x + \dots + c_nx^n$ — поліном з цілими коефіцієнтами, і якщо d — найбільший спільний дільник елементів c_0, c_1, \dots, c_n , то, очевидно, шуканий поліном має вигляд $f^*(x) = \pm \frac{c}{d}f(x)$ (де знак визначається знаком коефіцієнта c_n). Якщо $h(x)$ є один примітивний поліном з $\mathbb{Z}[x]$, асоційований з $f(x)$, то він асоційований із $f^*(x)$ і $h(x) = \frac{u}{v}f^*(x)$, де $u, v \in \mathbb{N}$. Тоді $vh(x) = uf^*(x)$, і, оскільки НСД коефіцієнтів поліномів $uf^*(x)$ і $vh(x)$ рівні, відповідно, u та v , то з останньої рівності випливає, що $u = v$, тобто $h(x) = f^*(x)$. \square

Лема 9.45 (Гаус). Добуток примітивних поліномів $g^*(x)$ і $h^*(x)$ є примітивним поліномом.

Доведення. Нехай $g^*(x) = \sum_{i \geq 0} b_i x^i$, $h^*(x) = \sum_{i \geq 0} c_i x^i$ і $g^*(x) \cdot h^*(x) = \sum_{i \geq 0} d_i x^i$. Досить довести, що для

будь-якого простого $p \in \mathbb{N}$ хоча б один з коефіцієнтів d_i не ділиться на p . Оскільки $g^*(x)$ і $h^*(x)$ — примітивні поліноми, то можна вибрати таке найменше $k \in \mathbb{N}_0$, що p не ділить b_k і таке найменше $l \in \mathbb{N}_0$, що p не ділить c_l . Тоді d_{k+l} не ділиться на p , оскільки $d_{k+l} = (b_0 c_{k+l} + \dots + b_{k-1} c_{l+1}) + b_k c_l + (b_{k+1} c_{l-1} + \dots + b_{k+l} c_0)$ і два, виділені дужками, доданки в цій сумі діляться на p , а доданок $b_k c_l$, зрозуміло, на p не ділиться. \square

Теорема 9.46. Якщо $f(x), g(x), h(x) \in \mathbb{Q}(x) \setminus \{0\}$ і $f(x) = g(x) \cdot h(x)$, то $f^*(x) = g^*(x) \cdot h^*(x)$.

Доведення. Оскільки $g^*(x), h^*(x)$ — примітивні поліноми, асоційовані, відповідно, з $g(x)$ і $h(x)$, то за лемою 9.45 добуток $g^*(x) \cdot h^*(x)$ — примітивний поліном, асоційований з поліномом $g(x) \cdot h(x) = f(x)$. \square

Наслідок 9.47. Поліном $f(x) \in \mathbb{Z}[x]$ степеня ≥ 1 незвідний в кільці $\mathbb{Q}[x]$ тоді і тільки тоді, коли він незвідний в кільці $\mathbb{Z}[x]$ (тобто не розкладається в $\mathbb{Z}[x]$ на множники менших степенів).

Достатньо зауважити, що $f(x) = kf^*(x)$, де $k \in \mathbb{Z}$.

Наслідок 9.48. Нехай $f(x)$ — поліном степеня $n > 0$ із $\mathbb{Q}[x]$ і $f^*(x) = a_0^* + a_1^*x + \dots + a_n^*x^n$ — асоційований з $f(x)$ примітивний поліном. Якщо $c = \frac{u}{v} \in \mathbb{Q}$, де $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $(u, v) = 1$, є коренем $f(x)$, то v ділить a_n^* , u ділить a_0^* і $tv - u$ ділить $f^*(m)$ для будь-якого $m \in \mathbb{Z}$, зокрема $v - u$ ділить $f^*(1)$ і $v + u$ ділить $f^*(-1)$.

Доведення. Досить зауважити, що $f^*(x) = (x - c)^* h^*(x)$ для відповідного примітивного $h^*(x) \in \mathbb{Z}[x]$ і $(x - c)^* = vx - u$. \square

Для будь-яких $m \in \mathbb{N}$ і $c \in \mathbb{Z}$ через $r_m(c)$ позначимо остатчу від ділення c на m , яку можна розглядати як елемент кільця \mathbb{Z}_m . Операції в кільці поліномів $\mathbb{Z}_m[x]$ позначимо символами \oplus і \otimes . Для будь-якого полінома $f(x) = \sum_{i \geq 0} a_i x^i \in \mathbb{Z}[x]$ через $r_m(f(x))$ позначимо поліном з $\mathbb{Z}_m[x]$ вигляду

$\sum_{i \geq 0} r_m(a_i)x^i$. Легко показати, що для будь-яких поліномів $g(x), h(x) \in \mathbb{Z}[x]$ виконується співвідношення $r_m(g(x) \cdot h(x)) = r_m(g(x)) \otimes r_m(h(x))$.

Наслідок 9.49. Якщо $f(x) \in \mathbb{Q}[x]$ — звідний поліном степеня n і $a_n^* x^n$ — старший член полінома $f^*(x)$, то для кожного простого $p \in \mathbb{N}$, який не ділить a_n^* , поліном $r_p(f^*(x))$ звідний у кільці $\mathbb{Z}_p[x]$.

Доведення. Якщо $f(x) = g(x)h(x)$, де $\deg g(x) = k \in \overline{1, n-1}$, то $r_p(f^*(x)) = r_p(g^*(x)) \otimes r_p(h^*(x))$, причому, оскільки p не ділить a_n^* , можна стверджувати, що p не ділить b_k^* і що $\deg r_p(f^*(x)) = n$, $\deg r_p(g^*(x)) = k$. \square

Отримані результати можна використовувати для знаходження раціональних коренів і перевірки незвідності поліномів з $\mathbb{Q}[x]$.

Приклади 9.12. 1. Знайдемо раціональні корені полінома $f(x) = x^3 - \frac{3}{2}x - \frac{3}{2}$. Зауважимо, що $f^*(x) = 2x^3 - 3x - 3$ і якщо елемент $c = \frac{u}{v} \in \mathbb{Q}$, де $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $(u, v) = 1$, є коренем полінома $f(x)$, то за наслідком 9.48 елемент u ділить 3 і елемент v ділить 2, тобто $c \in \{\pm 3, \pm 1, \pm \frac{1}{2}, \pm \frac{3}{2}\}$. Крім того, повинні виконуватися співвідношення $v - u$ ділить $f^*(1) = -4$ і $v + u$ ділить $f^*(-1) = -2$, тому залишається лише один кандидат в корені $f(x)$: $c = -3$. Але $f(-3) = -24 \neq 0$ і тому поліном $f(x)$ не має коренів в \mathbb{Q} . Звідси за твердженням 9.17 випливає також, що $f(x)$ незвідний над \mathbb{Q} .

2. З'ясуємо, чи є незвідним поліном $f(x) = x^4 + \frac{3}{7}x^3 + 3x^2 + \frac{4}{7}x + 5 \in \mathbb{Q}[x]$. Скористаємося наслідком 9.49. Отримуємо $f(x) = 7x^4 + 3x^3 + 21x^2 + 4x + 35$. Будемо перебирати прості числа $p \neq 7$. Для $p = 2$ маємо: $r_2(f^*(x)) = x^4 + x^3 + x^2 + 1$ — звідний поліном в $\mathbb{Z}_2[x]$: $r_2(f^*(x)) = (x+1) \otimes (x^3+x+1)$. Для $p = 3$ отримуємо: $r_3(f^*(x)) = x^4 + x + 2 \in \mathbb{Z}_3[x]$. Цей поліном незвідний над \mathbb{Z}_3 , оскільки він не має коренів в \mathbb{Z}_3 і не ділиться ні на один з трьох існуючих в $\mathbb{Z}_3[x]$ незвідних унітарних поліномів степеня 2: $x^2 + 1$, $x^3 + x + 2$, $x^2 + 2x + 2$ (безпосередня перевірка). Отже, поліном $f(x)$ незвідний над \mathbb{Q} . Для доведення незвідності $f(x)$ можна і не переконуватися в незвідності $r_3(f(x))$, а зауважити лише, що $r_3(f(x))$ не має коренів в \mathbb{Z}_3 , оскільки з дослідження полінома $r_2(f(x))$ випливає, що якщо $f(x)$ звідний, то він має дільник першого степеня.

Зауваження 9.11. Метод перевірки незвідності поліномів з кільця $\mathbb{Q}[x]$, що випливає з наслідку 9.49, не є універсальним у тому сенсі, що існують такі унітарні незвідні поліноми $f(x) \in \mathbb{Z}[x]$, що для будь-якого простого $p \in \mathbb{N}$ поліном $r_p(f(x))$ звідний над \mathbb{Z}_p . Наприклад, таким є поліном $x^4 - 10x^2 + 1$.

На завершення доведемо одну широко використовувану ознаку (теорему Ейзенштейна²) незвідності поліномів над \mathbb{Q} .

Теорема 9.50 (Ейзенштейн). Нехай $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$, $n > 0$, і для деякого простого $p \in \mathbb{N}$ виконуються умови:

$$p \text{ не ділить } a_n; \quad (9.36)$$

$$p \text{ ділить } a_i, i = \overline{0, n-1}; \quad (9.37)$$

$$p^2 \text{ не ділить } a_0. \quad (9.38)$$

Тоді поліном $f(x)$ незвідний над \mathbb{Q} .

Доведення. Якщо поліном $f(x)$ звідний в $\mathbb{Q}[x]$, то за наслідком 9.47 існують такі поліноми $g(x)$, $h(x) \in \mathbb{Z}[x]$, що $f(x) = g(x) \cdot h(x)$, $\deg g(x) = k \in \overline{1, n}$, $\deg h(x) = l \in \overline{1, n}$, $k + l = n$. З (9.36), (9.37) випливає, що поліном $r_p(f(x)) \in \mathbb{Z}_p[x]$ має вигляд $r_p(f(x)) = r_p(a_n)x^n$, $r_p(a_n) \neq 0$. Звідси, зважаючи на рівність $r_p(f(x)) = r_p(g(x)) \otimes r_p(h(x))$ в $\mathbb{Z}_p[x]$, отримуємо: $r_p(g(x)) = r_p(b_k)x^k$, $r_p(h(x)) = r_p(c_l)x^l$. Оскільки $k \geq 1$, $l \geq 1$, то з останніх рівностей випливає, що p ділить b_0 і p ділить c_0 . Але тоді p^2 ділить a_0 , оскільки $a_0 = b_0 c_0$, що суперечить умові (9.38). \square

Важливе значення цієї теореми полягає не тільки в тому, що вона дозволяє просто доводити незвідність деяких поліномів, але і в тому, що вона дає можливість їх легко будувати. Зокрема, з неї випливає такий результат, що показує принципову відмінність між властивостями множини незвідних поліномів над полем \mathbb{Q} і множини незвідних поліномів над полями \mathbb{R} і \mathbb{C} .

²Фердинанд Готтхольд Макс Эйзенштейн (нім. Ferdinand Gotthold Max Eisenstein; 16 квітня 1823 – 11 жовтня 1852) — німецький математик.

Наслідок 9.51. Над полем \mathbb{Q} існують незвідні поліноми будь-якого натурального степеня n .

Доведення. Наприклад, для будь-якого простого $p \in \mathbb{N}$ поліном $x^n - p$ незвідний над \mathbb{Q} . \square

Зауважимо, що наведений приклад істотно підсилює відоме із середньої школи твердження про ірраціональність числа $\sqrt[n]{p}$.

Зауважимо також, що у книзі [13] викладено метод Кронекера, який дозволяє визначити звідний чи ні поліном над \mathbb{Q} і, у випадку звідності, отримати його канонічне розкладання.

За основною теоремою алгебри $f(x)$ має комплексний корінь c . Якщо $c \in \mathbb{R}$, то $x - c$ ділить $f(x)$. Якщо $c \in \mathbb{C} \setminus \mathbb{R}$, то коренем полінома $f(x)$ буде і спряжене число \bar{c} . Дійсно, переходячи до спряжених чисел в рівності $a_0 + a_1c + \dots + a_nc^n = 0$, і використовуючи твердження 8.5 і той факт, що $\bar{a}_i = a_i$ для $0 \leq i \leq n$, одержимо $a_0 + a_1\bar{c} + \dots + a_n\bar{c}^n = 0$, тобто $f(\bar{c}) = 0$. Звідси випливає, що $f(x)$ ділиться на $x - \bar{c}$ і на $x - c$, але $x - \bar{c}$ і $x - c$ взаємно прості. Отже, $f(x)$ ділиться на поліном $(x - c)(x - \bar{c}) = x^2 - (c + \bar{c})x + c\bar{c}$, коефіцієнти якого, очевидно, дійсні.

Розглянемо властивості поліномів із $\mathbb{F}[x]$ (тобто над полем $F = \mathbb{R}$ дійсних чисел).

Лема 9.52. Якщо комплексне число z є коренем полінома $f(x) \in \mathbb{C}[x]$, то \bar{z} також є коренем цього полінома.

Доведення. Нехай

$$f(x) = a_n x^n + \dots + a_1 x + a_0, \quad a_i \in \mathbb{R}.$$

Тоді $f(z) = a_n z^n + \dots + a_1 z + a_0 = 0$. Оскільки $(\overline{z_1 + z_2}) = \bar{z}_1 + \bar{z}_2$, $(\overline{z_1 \cdot z_2}) = \bar{z}_1 \cdot \bar{z}_2$, то

$$\begin{aligned} 0 = \bar{0} &= \overline{a_n z^n + \dots + a_1 z + a_0} = \\ &= \bar{a}_n \bar{z}^n + \dots + \bar{a}_1 \bar{z} + \bar{a}_0 = \\ &= a_n \bar{z}^n + \dots + a_1 \bar{z} + a_0 = f(\bar{z}). \end{aligned}$$

Лема 9.53. Якщо $z \in \mathbb{C} \setminus \mathbb{R}$ (тобто $z \neq \bar{z}$), то

$$\text{НСД}(x - z, x - \bar{z}) = 1.$$

Доведення. Якщо $d(x) = \text{НСД}(x - z, x - \bar{z})$, то або $\deg d(x) = 0$ (тобто $d(x) = 1$), або $\deg d(x) = 1$. Якщо $\deg d(x) = 1$, то

$$(x - z) = d(x) \cdot c, \quad (x - \bar{z}) = d(x) \cdot d, \quad c, d \in \mathbb{C}$$

тобто

$$d(x) = c^{-1}(x - z) = d^{-1}(x - \bar{z}).$$

Тому $c^{-1} = d^{-1}$, $c^{-1}z = d^{-1}\bar{z}$, тобто $z = \bar{z}$, що суперечить припущення.

Наслідок 9.54. Якщо $f(x) \in \mathbb{R}[x]$, $z \in \mathbb{C} \setminus \mathbb{R}$, $f(z) = 0$, то

$$f(x) = \varphi(x)q(x),$$

де $\varphi(x) = (x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z} \in \mathbb{R}[x]$, $q(x) \in \mathbb{R}[x]$.

Доведення. Оскільки $f(z) = 0$, то $f(\bar{z}) = 0$. Тоді

$$f(x) = (x - z)q_1(x)$$

ділиться на $(x - z)$, але $x - z$ і $x - \bar{z}$ взаємно прості (оскільки $z \neq \bar{z}$), а тому

$$f(x) = (x - z)(x - \bar{z})q(x).$$

Оскільки $f(x)$, $(x - z)(x - \bar{z}) \in \mathbb{R}[x]$, то $q(x) \in \mathbb{R}[x]$. \square

Лема 9.55. Якщо $f(x) \in \mathbb{R}[x]$, $z \in \mathbb{C} \setminus \mathbb{R}$, $f(z) = 0$, то кратності коренів z і \bar{z} у поліномі $f(x)$ співпадають.

Доведення. Нехай кратність коренів z та \bar{z} дорівнюють відповідно k та l . Припустимо протилежне, що $k > l$ (симетрично, $k < l$, і тоді врахуємо, що $z = \bar{\bar{z}}$). Тоді для $\varphi(x) = (x - z)(x - \bar{z})$ маємо

$$f(x) = (x - \bar{z})^k (x - z)^l q(x) = \varphi(x)^l (x - z)^{k-l} q(x), \quad q(z) \neq 0, \quad q(\bar{z}) \neq 0.$$

Тоді $f'(x) = (x - z)^{k-l} q(x) \in \mathbb{R}[x]$ (як частка від ділення двох поліномів із $\mathbb{R}[x]$: $f(x)$ на $\varphi(x)^l$), проте $f'(z) = 0$, але $f'(\bar{z}) = (\bar{z} - z)^{k-l} q(\bar{z}) \neq 0$, що суперечить нашій теоремі для $f'(x) \in \mathbb{R}[x]$. \square

Наслідок 9.56. Комплексні корені, які не є дійсними, попарно спряжені.

Наслідок 9.57. (про розклад на незвідні поліноми над полем \mathbb{R} дійсних чисел). Незвідні поліноми над \mathbb{R} – це поліноми 1-го степеня і поліноми 2-го степеня без дійсних чисел. Кожен поліном $f(x) \in \mathbb{R}[x]$, $\deg f(x) \geq 1$, зображується (причому однозначно з точністю до порядку співмножників) у вигляді добутку константи $a \in \mathbb{R}$, поліномів вигляду $(x - \alpha)$, $\alpha \in \mathbb{R}$, і поліномів вигляду $(x - z)(x - \bar{z})$, де $z \in \mathbb{C} \setminus \mathbb{R}$ з відповідним парі спряжених коренів z і \bar{z} . Доведення єдності випливає із єдності розкладу на лінійні множники над полем \mathbb{C} комплексних чисел.

ЛНУ
Для підготовки
до колоквіуму,
а не для
списування
на ньому