

УДК 512.547.25

Ю. В. Петечук (Ужгородський нац. ун-т)

ПОЛІНОМИ ДІЛЕННЯ КРУГА НАД КІЛЬЦЯМИ

**Світлій пам'яті наукового керівника,
професора Гудивка П. М. присвячується**

The article deals with the properties of polynomials for the division of the ring $\Phi_n(x)$, $n \geq 1$, which are determined by the equality $x^n - 1 = \prod_{d|n} \Phi_d(x)$. It is found the criterion of the existence of

zeroes $\Phi_n(x)$, above broad enough class of rings and it is shown that the meaning of the polynomials for division of the ring $\Phi_n(x)$ according to the module p^l .

The properties of polynomials for the division of the ring $\Phi_n(x)$, $n \geq 1$ which are observed in the article are applied for finding canonical view of matrix of the finite order above some commutative rings.

В роботі вивчаються властивості поліномів ділення круга $\Phi_n(x)$, $n \geq 1$, які визначаються рівністю $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Знайдено критерій існування нулів $\Phi_n(x)$ над достатньо широким

класом кілець та обчислено значення поліномів ділення круга $\Phi_n(x)$ за модулем p^l , в кільці цілих чисел.

Розглянуті в роботі властивості поліномів ділення круга $\Phi_n(x)$, $n \geq 1$ застосовано до знаходження, з точністю до спряження, канонічного вигляду матриць скінченного порядку над деякими комутативними кільцями.

Поліноми ділення круга $\Phi_d(x)$ визначаються над кільцем цілих чисел \mathbf{Z} рівністю $x^n - 1 = \prod_{d|n} \Phi_d(x)$, $n \geq 1$, а многочлени, які мультиплікативно їх поро-

джують, формулою $f_n(x) = 1 + x + \dots + x^{n-1}$, $n \geq 1$.

У даній роботі розглядаються властивості поліномів ділення круга $\Phi_n(x)$ та многочленів $f_n(x)$, які безпосередньо впливають з означення або шляхом застосування формул перетворення М'юбіуса. Доведено, що поліноми ділення круга $\Phi_n(x)$ при $n = p_1^{n_1} \dots p_k^{n_k} > 1$ над кільцем $\mathbf{Z}[x]$ є лінійною комбінацією многочленів $f_{p_1} \left(x^{\frac{n}{p_1}} \right), \dots, f_{p_k} \left(x^{\frac{n}{p_k}} \right)$. Використовуючи отримані розклади знайдено критерій визначення нулів поліномів ділення круга над достатньо широкими класами асоціативних кілець.

У роботі обчислено значення поліномів ділення круга $\Phi_n(x)$ в нулі та в ± 1 . Доведено, що при $n > 1$ $\Phi_n(0) = 1$, а $\Phi_n(1)$ – просте число, якщо n – степінь цього простого числа і $\Phi_n(1) = 1$ в решті випадків.

Аналогічно при $n > 2$ показано, що $\Phi_n(-1)$ – просте число, якщо $\frac{n}{2}$ – його степінь і $\Phi_n(-1) = 1$ в решті випадків.

З отриманих результатів безпосередніми міркуваннями доведено, що $\Phi_n(x)$ – незвідний многочлен кільця $\mathbf{Z}[x]$, якщо n – степінь або подвоєна степінь простого числа.

Доведено, що поліноми ділення круга $\Phi_d(x)$, $d|n$ над областями цілісності, в яких $n \neq 0$, з точністю до оборотних елементів кільця при деяких умовах, співпадають з мінімальними многочленами первісних коренів $\frac{n}{d}$ -го степеня із 1 їх алгебраїчного замикання, а тому у розглянутих випадках є незвідними многочленами. Це є достатньо широким узагальненням відомого результату про

незвідність поліномів ділення круга над кільцем цілих чисел, з якого він, зрозуміло, також випливає.

Розглянуте в роботі вивчення поліномів ділення круга застосовується до знаходження, з точністю до спряження, канонічного вигляду матриць скінченного порядку над деякими класами комутативних кілець.

Основні результати роботи сформульовані в теоремах 1–5.

Більш широку інформацію щодо розглянутих в статті питань можна знайти в [1–8].

1. Мультиплікативні функції. Функція $\theta : N \rightarrow Z$ називається мультиплікативною, якщо $\theta(1) = 1$ і $\theta(ab) = \theta(a)\theta(b)$ для будь-яких взаємно-простих натуральних чисел a і b .

Функція $\mu : N \rightarrow Z$ називається функцією Мьобіуса, якщо $\mu(1) = 1$, $\mu(n) = (-1)^k$, якщо n – добуток k простих різних чисел і $\mu(n) = 0$ в решті випадків.

Очевидно, що добуток мультиплікативних функцій є мультиплікативною функцією і μ – мультиплікативна функція.

Нехай $n = p_1^{n_1} \cdots p_k^{n_k} > 1$ – канонічний розклад числа n в добуток степенів простих чисел p_1, \dots, p_k і θ – мультиплікативна функція. Безпосередньою перевіркою, розкриваючи дужки, встановлюємо, що має місце основна властивість мультиплікативної функції

$$\sum_{d|n} \theta(d) = (1 + \theta(p_1) + \cdots + \theta(p_1^{n_1})) \cdots (1 + \theta(p_k) + \cdots + \theta(p_k^{n_k})).$$

Зокрема, якщо замість θ підставити $\theta\mu$, то

$$\sum_{d|n} \theta(d)\mu(d) = (1 - \theta(p_1)) \cdots (1 - \theta(p_k)).$$

Якщо покласти $\theta(n) = 1$ при $n > 1$, то $\sum_{d|n} \mu(d) = 0$. Тому

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) = \begin{cases} 0, & n \neq 1, \\ 1, & n = 1. \end{cases}$$

Легко бачити, що якщо d пробігає всі дільники числа n , які діляться на t , то $\frac{d}{t}$ пробігає всі дільники числа $\frac{n}{t}$. Тому

$$\sum_{\frac{d}{t}|n} \mu\left(\frac{n}{d}\right) = \sum_{\frac{d}{t}|n} \mu\left(\frac{n}{t} \mid \frac{d}{t}\right) = \begin{cases} 0, & n \neq t, \\ 1, & n = t. \end{cases}$$

Ще одним прикладом мультиплікативної функції є функція Ейлера φ , де $\varphi(1) = 1$ і $\varphi(n)$ при $n > 1$ дорівнює числу чисел із множини $\{1, 2, \dots, n\}$, які є взаємно простими з числом n . Тому

$$\varphi(n) = \varphi(p_1^{n_1}) \cdots \varphi(p_k^{n_k}), \quad \varphi(n) = |Z_n^*|, \quad \text{де } Z_n = Z/nZ, \quad n > 1.$$

Легко бачити, що числами, які діляться на просте число p у множині $\{1, 2, \dots, p^l\}$ є числа $p, 2p, \dots, p^l$, число яких дорівнює p^{l-1} і які складають множини необоротних елементів кільця Z_{p^l} . Тому

$$\varphi(p^l) = p^l - p^{l-1} = p^l \left(1 - \frac{1}{p}\right), \quad 1 + \varphi(p) + \cdots + \varphi(p^l) = 1 + p - 1 + \cdots + p^l - p^{l-1} = p^l.$$

Тим самим доведено, що

$$\varphi(n) = p_1^{n_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{n_k} \left(1 - \frac{1}{p_k}\right) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

З основної властивості мультиплікативної функції φ випливає, що $\sum_{d|n} \varphi(d) = (1 + \varphi(p_1) + \cdots + \varphi(p_1^{n_1})) \cdots (1 + \varphi(p_k) + \cdots + \varphi(p_k^{n_k})) = p_1^{n_1} \cdots p_k^{n_k} = n$,

а також при $\theta(s) = \frac{1}{s}$, $s \in N$

$$\sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Домноживши отриману рівність на n , знаходимо ще одну формулу визначення функції $\varphi(n)$

$$\sum_{d|n} \mu(d) \frac{n}{d} = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \varphi(n).$$

Отже, мають місце формули

$$n = \sum_{d|n} \varphi(d), \quad \varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{d|n} d \mu\left(\frac{n}{d}\right).$$

Перетворення цих формул є частковим випадком при $f = \varphi$ і $g(n) = n$, $n \in N$ адитивного перетворення Мьобіуса.

2. Формули перетворення Мьобіуса.

Лема 1. Нехай f, g – функції із N в деяке асоціативне кільце. Тоді

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} g(d) \mu\left(\frac{n}{d}\right) \quad (\text{адитивне формулювання}),$$

$$g(n) = \prod_{d|n} f(d) \Leftrightarrow f(n) = \prod_{d|n} g(d) \mu^{\left(\frac{n}{d}\right)} \quad (\text{мультиплікативне формулювання}).$$

Доведення. Нехай $g(n) = \sum_{d|n} f(d)$. Тоді

$$\sum_{d|n} g(d) \mu\left(\frac{n}{d}\right) = \sum_{d|n} \left(\sum_{t|d} f(t)\right) \mu\left(\frac{n}{d}\right) = \sum_{t|d} \left(\sum_{\frac{d}{t}|\frac{n}{t}} \mu\left(\frac{n}{d}\right)\right) f(t) = f(n).$$

Аналогічно із $g(n) = \prod_{d|n} f(d)$ випливає, що

$$\prod_{d|n} g(d) \mu^{\left(\frac{n}{d}\right)} = \prod_{d|n} \left(\prod_{t|d} f(t)\right)^{\mu\left(\frac{n}{d}\right)} = \prod_{t|d} f(t)^{\sum_{\frac{d}{t}|\frac{n}{t}} \mu\left(\frac{n}{d}\right)} = f(n).$$

Навпаки. Нехай $f(n) = \sum_{d|n} g(d) \mu\left(\frac{n}{d}\right)$. Тоді

$$\sum_{d|n} f(d) = \sum_{d|n} \left(\sum_{t|d} g(t) \mu\left(\frac{d}{t}\right)\right) = \sum_{t|d} \left(\sum_{\frac{d}{t}|\frac{n}{t}} \mu\left(\frac{d}{t}\right)\right) g(t) = g(n).$$

Аналогічно із $f(n) = \prod_{d|n} g(d) \mu^{\left(\frac{n}{d}\right)}$ випливає, що

$$\prod_{d|n} f(d) = \prod_{d|n} \left(\prod_{t|d} g(t) \mu^{\left(\frac{d}{t}\right)}\right) = \prod_{d|n} \left(g(t)^{\sum_{\frac{d}{t}|\frac{n}{t}} \mu^{\left(\frac{d}{t}\right)}\right)} = g(n).$$

3. Поліноми ділення круга та породжуючі їх многочлени. Нехай $\Phi_n(x)$ і $f_n(x)$, $n \geq 1$ – многочлени над кільцем цілих чисел Z такі, що

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \quad f_n(x) = 1 + x + \cdots + x^{n-1}.$$

Многочлени $\Phi_n(x)$ називаються поліномами ділення круга, а $f_n(x)$ – породжуючими їх многочленами.

Зрозуміло, що

$$x - 1 = \Phi_1(x), \quad \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}, \quad f_n(x) = \frac{x^n - 1}{x - 1} = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x).$$

Тому, з індуктивних міркувань, поліноми ділення круга в кільці $Z[x]$ визначаються однозначно і є строго унітарними (нормалізованими) многочленами (многочлени, старші коефіцієнти яких дорівнюють одиниці). Зокрема, з рівності

$$x^{p^l} - 1 = \Phi_1(x)\Phi_p(x)\cdots\Phi_{p^l}(x) = (x^{p^{l-1}} - 1)\Phi_{p^l}(x),$$

де p – просте число і $l \geq 1$, випливає, що

$$\Phi_{p^l}(x) = \frac{x^{p^l} - 1}{x^{p^{l-1}} - 1} = 1 + x^{p^{l-1}} + \cdots + (x^{p^{l-1}})^{p-1} = f_p(x^{p^{l-1}}).$$

Тому $\Phi_p(x) = f_p(x)$ і $\Phi_{p^l}(x) = f_p(x^{p^{l-1}}) = \Phi_p(x^{p^{l-1}})$.

У загальному випадку, якщо p – просте число і $(p, m) = 1$, то

$$x^{p^l m} - 1 = \prod_{d|m, 0 \leq i \leq l} \Phi_{p^i d}(x) = \prod_{d|m} \Phi_{p^i d}(x) (x^{p^{l-1} m} - 1).$$

Це означає, що

$$\prod_{d|m} \Phi_{p^i d}(x) = \frac{x^{p^l m} - 1}{x^{p^{l-1} m} - 1} = f_p(x^{p^{l-1} m}) = \Phi_p(x^{p^{l-1} m}).$$

Застосуємо лему 1 до поліномів ділення круга.

Лема 2. *Мають місце формули*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}, \quad \Phi_n(x) = \begin{cases} \prod_{d|n} f_d(x)^{\mu(\frac{n}{d})}, & n \neq 1, \\ x - 1, & n = 1, \end{cases}$$

$$\Phi_n(x) = \Phi_{p^l m}(x) = \prod_{d|n} \Phi_p(x^{p^{l-1} d})^{\mu(\frac{m}{d})}, \quad n = p^l m, \quad l \geq 1, \quad (p, m) = 1, \quad p - \text{просте число.}$$

Доведення. Перша формула леми 2 випливає з означення поліномів ділення круга і його переформулювання за допомогою мультиплікативного перетворення Мьобіуса $g(n) = x^n - 1$ і $f(d) = \Phi_d(x)$, $d|n$.

Друга формула леми 2 випливає з рівності

$$\prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} = (x - 1)^{\sum_{d|n} \mu(\frac{n}{d})} \prod_{d|n} f_d(x)^{\mu(\frac{n}{d})} = \begin{cases} \prod_{d|n} f_d(x)^{\mu(\frac{n}{d})}, & n \neq 1, \\ x - 1, & n = 1. \end{cases}$$

Третя формула леми 2 також випливає із мультиплікативного перетворення Мьобіуса, якщо покласти $g(m) = \Phi_p(x^{p^{l-1} m})$ і $f(d) = \Phi_{p^i d}(x)$, $d|m$.

Лема 3. Нехай $n = p^l m$, де p – просте число, $(p, m) = 1$, $l \geq 1$, $m \geq 1$. Тоді

$$\Phi_n(x) = \frac{\Phi_m(x^{p^l})}{\Phi_m(x^{p^{l-1}})}.$$

Доведення. З леми 2 випливає, що

$$\Phi_n(x) = \prod_{i=0}^l \left(\prod_{d|m} (x^{p^i d} - 1)^{\mu\left(\frac{n}{p^i d}\right)} \right), \quad \Phi_m(x) = \prod_{d|m} (x^d - 1)^{\mu\left(\frac{m}{d}\right)},$$

де $0 \leq i \leq l$, а d пробігає всі дільники числа m .

Із мультиплікативності функції μ і взаємної простоти чисел p і $\frac{m}{d}$ випливає, що має місце рівність

$$(x^{p^i d} - 1)^{\mu\left(\frac{n}{p^i d}\right)} = \begin{cases} 1, & 0 \leq i \leq l-2, \\ (x^{p^{i-1} d} - 1)^{-\mu\left(\frac{m}{d}\right)}, & i = l-1, \\ (x^{p^l d} - 1)^{\mu\left(\frac{m}{d}\right)}, & i = l. \end{cases}$$

Це означає, що

$$\Phi_n(x) = \prod_{d|m} \frac{(x^{p^l d} - 1)^{\mu\left(\frac{m}{d}\right)}}{(x^{p^{l-1} d} - 1)^{\mu\left(\frac{m}{d}\right)}} = \frac{\Phi_m(x^{p^l})}{\Phi_m(x^{p^{l-1}})}.$$

Наслідок 1. Якщо p^2 ділить n , то $\Phi_n(x) = \Phi_{\frac{n}{p}}(x^p)$.

Доведення. Нехай $n = p^l m$, $(p, m) = 1$, $m \geq 1$, $l \geq 2$. Тоді

$$\Phi_n(x) = \frac{\Phi_m(x^{p^l})}{\Phi_m(x^{p^{l-1}})} = \frac{\Phi_m((x^p)^{p^{l-1}})}{\Phi_m((x^p)^{p^{l-2}})} = \Phi_{\frac{n}{p}}(x^p).$$

З аналогічних міркувань

$$\Phi_n(x) = \Phi_{\frac{n}{p}}(x^p) = \dots = \Phi_{\frac{n}{p^{l-1}}}(x^{p^{l-1}}).$$

Зокрема, з наслідку 1 випливає, що $\Phi_{pn}(x) = \Phi_n(x^p)$, якщо p ділить n .

Відмітимо, що за лемою 3 $\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$, якщо p не ділить n .

Наслідок 2. Нехай $n = p_1^{n_1} \dots p_k^{n_k}$, де $n_i \geq 1$, $1 \leq i \leq k$. Тоді

$$\Phi_n(x) = \Phi_{p_1 \dots p_k}(x^{p_1^{n_1-1} \dots p_k^{n_k-1}}).$$

Доведення випливає з послідовного застосування наслідку 1.

Легко бачити, що $f_n(x) - 1 = x f_{n-1}(x)$ при $n > 1$ і

$$(x-1)(f_n(x) - 1) = (x-1)f_n(x) - x + 1 = x^n - 1 - x + 1 = x(x^{n-1} - 1) \quad \text{при } n \geq 1.$$

Лема 4. Нехай n – непарне число. Тоді $f_n(x)f_n(-x) = f_n(x^2)$ при $n \geq 1$, $\Phi_n(x)\Phi_n(-x) = \Phi_n(x^2)$ при $n > 1$ і $\Phi_1(x)\Phi_1(-x) = -\Phi_1(x^2)$.

Доведення. Легко бачити, що при $n \geq 1$ має місце рівність

$$f_n(x)f_n(-x) = \frac{x^n - 1}{x - 1} \cdot \frac{x^n + 1}{x + 1} = \frac{x^{2n} - 1}{x^2 - 1} = f_n(x^2).$$

Нехай $n = p^l m > 1$, де p – непарне просте число, m – непарне число, $(p, m) = 1$, $l \geq 1$. Якщо $m = 1$, то

$$\Phi_n(x)\Phi_n(-x) = f_p(x^{p^l})f_p(-x^{p^l}) = f_p(x^{2p^l}) = \Phi_n(x^2).$$

Нехай $m > 1$. З індуктивних міркувань можна вважати, що $\Phi_m(x)\Phi_m(-x) = \Phi_m(x^2)$. Тому

$$\Phi_n(x)\Phi_n(-x) = \frac{\Phi_m(x^{p^l})}{\Phi_m(x^{p^{l-1}})} \cdot \frac{\Phi_m(-x^{p^l})}{\Phi_m(-x^{p^{l-1}})} = \frac{\Phi_m(x^{2p^l})}{\Phi_m(x^{2p^{l-1}})} = \Phi_n(x^2).$$

Безпосередньою перевіркою встановлюємо, що $\Phi_1(x)\Phi_1(-x) = -\Phi_1(x^2)$.

Наслідок 3. Нехай $n = 2^l m$, де m – непарне натуральне число, $l \geq 1$. Тоді $\Phi_n(x) = \Phi_m(-x^{2^{l-1}})$ при $m > 1$ і $\Phi_n(x) = -\Phi_m(-x^{2^{l-1}})$ при $m = 1$.

Доведення. При $m > 1$, згідно з лемою 4,

$$\Phi_n(x) = \frac{\Phi_m(x^{2^l})}{\Phi_m(x^{2^{l-1}})} = \Phi_m(-x^{2^{l-1}}).$$

При $m = 1$ має місце рівність

$$\Phi_n(x) = \Phi_{2^l}(x) = f_2(x^{2^{l-1}}) = 1 + x^{2^{l-1}} = -\Phi_1(-x^{2^{l-1}}) = -\Phi_m(-x^{2^{l-1}}).$$

Зокрема, $\Phi_{2m}(x) = \Phi_m(-x)$, якщо $m > 1$ – непарне число.

4. Властивості многочленів $f_n(x)$. Алгоритм Евкліда послідовного ділення многочленів з остачею можна застосовувати у кільці $R[x]$ над комутативним кільцем R до унітарних многочленів (многочленів, старші коефіцієнти яких є оборотними в R), якщо ненульові остачі від ділення, які при цьому виникають, також є унітарними многочленами. Для таких многочленів найбільший спільний дільник є останньою відмінною від нуля остачею алгоритму Евкліда.

Зокрема, такими є двочлени вигляду $x^n - 1$, $n \geq 1$. При $i \leq n$ має місце рівність

$$x^n - 1 = (x^i - 1)(x^{n-i} + \dots + x^{n-ti}) + x^{n-it} - 1 = (x^i - 1)x^{n-ti}f_t(x^i) + x^{n-it} - 1,$$

де $n - ti \geq 0$. З неї випливає, що $x^i - 1$ при $i \leq n$ ділить $x^n - 1$ тоді і тільки тоді, коли i ділить n .

Лема 5. Нехай R – область цілісності, n_1, \dots, n_k – натуральні числа, $k \geq 2$. Тоді, з точністю до оборотних елементів кільця R ,

$$(x^{n_1} - 1, \dots, x^{n_k} - 1) = x^{(n_1, \dots, n_k)} - 1 \in \langle x^{n_1} - 1, \dots, x^{n_k} - 1 \rangle_{R[x]}.$$

Доведення. За алгоритмом Евкліда послідовного ділення многочленів з остачею, знаходимо, що, з точністю до оборотних елементів кільця R , найбільший спільний дільник двочленів $x^{n_1} - 1$ і $x^{n_2} - 1$ має вигляд $x^d - 1$ і належить $\langle x^{n_1} - 1, x^{n_2} - 1 \rangle_{R[x]}$, де d ділить n_1 і n_2 . Тому

$$(x^{n_1} - 1, x^{n_2} - 1) = x^{(n_1, n_2)} - 1 \in \langle x^{n_1} - 1, x^{n_2} - 1 \rangle_{R[x]}.$$

Ця формула за індукцією поширюється на скінченну кількість многочленів $x^{n_1} - 1, \dots, x^{n_k} - 1$. Адже, з точністю до оборотних елементів кільця R ,

$$\begin{aligned} (x^{n_1} - 1, \dots, x^{n_k} - 1) - 1 &= ((x^{n_1} - 1, \dots, x^{n_{k-1}} - 1), x^{n_k} - 1) = (x^{(n_1, \dots, n_{k-1})} - 1, x^{n_k} - 1) = \\ &= x^{(n_1, \dots, n_{k-1}, n_k)} - 1 = x^{(n_1, \dots, n_k)} - 1 \in \langle x^{(n_1, \dots, n_{k-1})} - 1, x^{n_k} - 1 \rangle_{R[x]} \in \\ &\in \langle x^{n_1} - 1, \dots, x^{n_{k-1}} - 1, x^{n_k} - 1 \rangle_{R[x]}. \end{aligned}$$

Якщо R – область цілісності, то не всякий елемент кільця $R[x]$ можна вивести за знак найбільшого спільного дільника. Однак, в деяких випадках це можна робити.

Лема 6. Нехай R – область цілісності, $P_1(x), \dots, P_n(x)$, $n \geq 2$ – многочлени кільця $R[x]$, $r \in R$. Тоді

$$((x - r)P_1(x), \dots, (x - r)P_n(x)) = (x - r)(P_1(x), \dots, P_n(x)).$$

Доведення. Достатньо довести, що довільний дільник $d(x)$ многочленів $(x - r)P_1(x), \dots, (x - r)P_n(x)$ ділить многочлен $(x - r)(P_1(x), \dots, P_n(x))$. За припущенням $(x - r)P_1(x) = d(x)P'_1(x)$, де $P'_i(x) \in R[x]$, $1 \leq i \leq n$.

За теоремою Безу, якщо лінійний двочлен над областю цілісності ділить добуток двох многочленів, то він ділить один із них.

Якщо $x - r$ ділить $d(x)$, то $d(x) = (x - r)d'(x)$ і $d'(x)$ ділить многочлени $P_1(x), \dots, P_n(x)$. Тому $d(x)$ ділить $(x - r)(P_1(x), \dots, P_n(x))$.

Якщо $x - r$ не ділить $d(x)$, то $x - r$ ділить $P'_1(x), \dots, P'_n(x)$ і $P_i(x) = d(x) \frac{P'_i(x)}{x - r}$. Це означає, що $d(x)$ ділить многочлени $P_1(x), \dots, P_n(x)$ і, як наслідок, многочлен $(x - r)(P_1(x), \dots, P_n(x))$.

Наслідок 4. Нехай R – область цілісності, $f_n(x) = 1 + x + \dots + x^{n-1}$, $n \geq 1$, n_1, \dots, n_k , $k \geq 2$ – натуральні числа. Тоді, з точністю до оборотних елементів кільця R , $(f_{n_1}(x), \dots, f_{n_k}(x)) = f_{(n_1, \dots, n_k)}(x) \in \langle f_{n_1}(x), \dots, f_{n_k}(x) \rangle_{R[x]}$.

Доведення. Очевидно, що $x^n - 1 = (x - 1)f_n(x)$. Згідно з лемами 3 і 4, з точністю до оборотних елементів кільця R ,

$$\begin{aligned} (x - 1)(f_{n_1}(x), \dots, f_{n_k}(x)) &= (x^{n_1} - 1, \dots, x^{n_k} - 1) = x^{(n_1, \dots, n_k)} - 1 = (x - 1)f_{(n_1, \dots, n_k)}(x) \in \\ &\in \langle x^{n_1} - 1, \dots, x^{n_k} - 1 \rangle_{R[x]} \subset (x - 1) \langle f_{n_1}(x), \dots, f_{n_k}(x) \rangle_{R[x]}. \end{aligned}$$

Після скорочення на $x - 1$ отримуємо твердження наслідку 4.

Лема 7. Нехай R – область цілісності. Тоді в кільці $R[x]$ має місце формула $f_{n_1 n_2}(x) = f_{n_1}(x) \cdot f_{n_2}(x^{n_1}) = f_{n_2}(x) \cdot f_{n_1}(x^{n_2})$, де n_1, n_2 – довільні натуральні числа.

Доведення. Легко бачити, що

$$(x-1)f_{n_1 n_2}(x) = x^{n_1 n_2} - 1 = (x^{n_1} - 1) \cdot f_{n_2}(x^{n_1}) = (x-1)f_{n_1}(x) \cdot f_{n_2}(x^{n_1}).$$

Після скорочення на $x-1$ отримуємо формулу леми 7. Зокрема, якщо d ділить n , то $f_n(x) = f_d(x) \cdot f_{\frac{n}{d}}(x^d) = f_{\frac{n}{d}}(x) \cdot f_d(x^{\frac{n}{d}})$.

Наслідок 5. Нехай R – область цілісності. В кільці $R[x]$ при $n \geq 1$ має місце рівність $f_{p^n}(x) = f_p(x) \dots f_p(x^{p^{n-1}})$, де p – натуральне (не обов'язково просте) число.

Доведення. Проведемо доведення індукцією за числом n . При $n=1$ наслідок 5 очевидний. При $n > 1$, згідно з лемою 7, має місце рівність $f_{p^n}(x) = f_p(x) \cdot f_{p^{n-1}}(x^p)$. За індукцією $f_{p^{n-1}}(x) = f_p(x) \dots f_p(x^{p^{n-2}})$. Тому $f_{p^{n-1}}(x^p) = f_p(x^p) \dots f_p(x^{p^{n-1}})$. Тим самим наслідок 5 доведений.

З наслідку 5 випливає, що при $n = p_1^{n_1} \dots p_k^{n_k} > 1$ має місце формула

$$f_n(x) = \prod_{i=1}^k \left(\prod_{j=0}^{n_i-1} f_{p_i}(x^{p_1^{n_1} \dots p_{i-1}^{n_{i-1}} p_i^j}) \right).$$

Лема 8. Нехай R – область цілісності. В кільці $R[x]$ має місце включення $n \in \langle f_n(x), x-1 \rangle_{R[x]}$.

Доведення. При $n=1$ твердження леми 8 очевидне. При $n \geq 2$ доведення леми 8 випливає з формули

$$f_n(x) = (x-1)(x^{n-2} + 2x^{n-3} + \dots + (n-2)x + n-1) + n.$$

Відмітимо, що $x^n - 1 \in \langle \Phi_n(x) \rangle_{R[x]}$. Тому $x^{nt} - 1 = (x^n - 1)f_t(x^n) \in \langle \Phi_n(x) \rangle_{R[x]}$ для будь-якого натурального числа t . Зокрема, для будь-якого дільника $d > 1$ числа n має місце рівність $x^n - 1 = x^{\frac{n}{d}d} - 1 = (x^{\frac{n}{d}} - 1)f_d(x^{\frac{n}{d}})$, з якої випливає, що $f_d\left(\frac{n}{x^d}\right) = \frac{x^{\frac{n}{d}} - 1}{x^{\frac{n}{d}} - 1} \in \langle \Phi_n(x) \rangle_{R[x]}$.

Лема 9. Нехай R – область цілісності і n_1, n_2 – різні натуральні числа, $\Phi = \langle \Phi_{n_1}(x), \Phi_{n_2}(x) \rangle_{R[x]}$. Якщо відношення n_1 і n_2 або n_2 і n_1 не є степенями простого числа, то $1 \in \Phi$. Якщо відношення чисел n_1 і n_2 є степенем простого числа p , то $p \in \Phi$.

Доведення. Згідно з лемою 5 $x^{(n_1, n_2)} - 1 \in \langle x^{n_1} - 1, x^{n_2} - 1 \rangle_{R[x]}$. Якщо n_1 і n_2 не є дільниками один одного, то елемент (n_1, n_2) відмінний від n_1 і n_2 і

$$1 \in \left\langle \frac{x^{n_1} - 1}{x^{(n_1, n_2)} - 1}, \frac{x^{n_2} - 1}{x^{(n_1, n_2)} - 1} \right\rangle_{R[x]} \subset \Phi.$$

Нехай $\frac{n_1}{n_2}$ – натуральне число і p – просте число, яке ділить $\frac{n_1}{n_2}$. Тоді $\frac{n_1}{p} =$

$= n_2 \frac{n_1}{n_2 p}$. Згідно з лемою 8 і сказаним перед лемою 9

$$p \in \left\langle f_p \left(x^{\frac{n_1}{p}} \right), x^{n_1 p} - 1 \right\rangle_{R[x]} \subset \Phi.$$

Якщо $\frac{n_1}{n_2}$ не є степенем простого числа, то існує просте число $q \neq p$ таке, що $q \in \Phi$. Тоді $1 = (p, q) \in \langle p, q \rangle_R \subset \Phi$.

Якщо R – область цілісності, $a_1, \dots, a_n, x_1, \dots, x_n$ елементи R , b_1, \dots, b_n , $\sum_i x_i b_i$ – ненульові елементи R такі, що $\frac{a_1}{b_1} = \dots = \frac{a_n}{b_n} = t$. Тоді $a_1 = b_1 t, \dots, a_n = b_n t$,

$$\sum_i x_i a_i = t \sum_i x_i b_i, \frac{a_1}{b_1} = \dots = \frac{a_n}{b_n} = t = \frac{\sum_i x_i a_i}{\sum_i x_i b_i} \text{ (властивість рівних дробів) .}$$

5. Адитивні розклади поліномів ділення круга.

Лема 10. *Нехай $n = p_1^{n_1} \dots p_k^{n_k}$, $k \geq 2$, $n_i \geq 1$, $1 \leq i \leq k$. Тоді*

$$1 \in \left\langle \Phi_{\frac{n}{p_1^{n_1}}} \left(x^{p_1^{n_1-1}} \right), \dots, \Phi_{\frac{n}{p_k^{n_k}}} \left(x^{p_k^{n_k-1}} \right) \right\rangle_{Z[x]} .$$

Доведення проведемо індукцією за числом k . При $k = 2$ $\frac{n}{p_1^{n_1}} = p_2^{n_2}$ і $\frac{n}{p_2^{n_2}} = p_1^{n_1}$. Згідно з наслідком 4, з точністю до знаку,

$$1 = f_1(x) = f_{(p_1, p_2)}(x) = (f_{p_1}(x), f_{p_2}(x)) \in \langle f_{p_1}(x), f_{p_2}(x) \rangle_{Z[x]} .$$

Тому після заміни x на $x^{p_1^{n_1-1} p_2^{n_2-1}}$ отримуємо включення

$$1 \in \left\langle f_{p_1} \left(x^{p_1^{n_1-1} p_2^{n_2-1}} \right) = \Phi_{\frac{n}{p_2^{n_2}}} \left(x^{p_2^{n_2-1}} \right), f_{p_2} \left(x^{p_1^{n_1-1} p_2^{n_2-1}} \right) = \Phi_{\frac{n}{p_1^{n_1}}} \left(x^{p_1^{n_1-1}} \right) \right\rangle_{Z[x]} .$$

Тим самим лема 10 при $k = 2$ доведена.

Припустимо, що для числа $m = p_1^{n_1} \dots p_{k-1}^{n_{k-1}}$ при $k - 1 \geq 2$ лема 10 уже доведена. Це означає, що

$$1 \in \left\langle \Phi_{\frac{m}{p_1^{n_1}}} \left(x^{p_1^{n_1-1}} \right), \dots, \Phi_{\frac{m}{p_{k-1}^{n_{k-1}}}} \left(x^{p_{k-1}^{n_{k-1}-1}} \right) \right\rangle_{Z[x]} .$$

Тому після заміни x на $x^{p_k^{n_k}}$ отримуємо включення

$$1 \in \left\langle \Phi_{\frac{m}{p_1^{n_1}}} \left(x^{p_1^{n_1-1} p_k^{n_k}} \right), \dots, \Phi_{\frac{m}{p_{k-1}^{n_{k-1}}}} \left(x^{p_{k-1}^{n_{k-1}-1} p_k^{n_k}} \right) \right\rangle_{Z[x]} .$$

Доведемо, що лема 10 має місце при $n = m p_k^{n_k}$. Легко бачити, що $\frac{n}{p_i^{n_i}} = p_k^{n_k} \cdot \frac{m}{p_i^{n_i}}$, $1 \leq i \leq k - 1$. За лемою 3

$$\Phi_{\frac{n}{p_i^{n_i}}}(x) = \frac{\Phi_{\frac{m}{p_i^{n_i}}}(x^{p_k^{n_k}})}{\Phi_{\frac{m}{p_i^{n_i}}}(x^{p_k^{n_k-1}})}, \quad 1 \leq i \leq k - 1.$$

Тому після заміни x на $x^{p_i^{n_i-1}}$ відповідно, отримуємо, що

$$\Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i-1}} \right) = \frac{\Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i-1} p_k^{n_k}} \right)}{\Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i-1} p_k^{n_k-1}} \right)}, \quad 1 \leq i \leq k-1.$$

Це означає, що

$$1 \in \left\langle \Phi_{\frac{n}{p_1}} \left(x^{p_1^{n_1-1}} \right), \dots, \Phi_{\frac{n}{p_{k-1}}} \left(x^{p_{k-1}^{n_{k-1}-1}} \right) \right\rangle_{Z[x]} \subset \left\langle \Phi_{\frac{n}{p_1}} \left(x^{p_1^{n_1-1}} \right), \dots, \Phi_{\frac{n}{p_{k-1}}} \left(x^{p_{k-1}^{n_{k-1}-1}} \right) \right\rangle_{Z[x]}.$$

Теорема 1. Нехай $n = p_1^{n_1} \cdots p_k^{n_k} > 1$. Поліном ділення круга $\Phi_n(x)$ є лінійною комбінацією многочленів $f_{p_1} \left(x^{p_1} \right), \dots, f_{p_k} \left(x^{p_k} \right)$ в кільці $Z[x]$.

Доведення проводимо індукцією за числом k . При $k = 1, n = p_1^{n_1}$ твердження теореми 1 випливає із рівності

$$\Phi_n(x) = \Phi_{p_1^{n_1}}(x) = f_{p_1} \left(x^{p_1^{n_1-1}} \right) = f_{p_1} \left(x^{p_1} \right).$$

Нехай $k \geq 2$. За лемою 3

$$\Phi_n(x) = \frac{\Phi_{\frac{n}{p_1}} \left(x^{p_1^{n_1}} \right)}{\Phi_{\frac{n}{p_1}} \left(x^{p_1^{n_1-1}} \right)} = \dots = \frac{\Phi_{\frac{n}{p_k}} \left(x^{p_k^{n_k}} \right)}{\Phi_{\frac{n}{p_k}} \left(x^{p_k^{n_k-1}} \right)}$$

За властивістю рівних дробів для многочленів $u_1(x), \dots, u_k(x)$ кільця $Z[x]$ має місце рівність

$$\Phi_n(x) = \frac{\sum_{i=1}^k u_i(x) \Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i}} \right)}{\sum_{i=1}^k u_i(x) \Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i-1}} \right)},$$

якщо $\sum_{i=1}^k u_i(x) \Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i-1}} \right) \neq 0$.

Згідно з лемою 10 існують многочлени $u_1(x), \dots, u_k(x)$ кільця $Z[x]$ такі, що $\sum_{i=1}^k u_i(x) \Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i-1}} \right) = 1$. В такому разі $\Phi_n(x) = \sum_{i=1}^k u_i(x) \Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i}} \right)$.

За припущенням індукції поліном ділення круга $\Phi_{\frac{n}{p_i}}(x)$, $1 \leq i \leq k$ є лінійною комбінацією многочленів

$$f_{p_1} \left(x^{\frac{n}{p_i^{n_i} p_1}} \right), \dots, f_{p_{i-1}} \left(x^{\frac{n}{p_i^{n_i} p_{i-1}}} \right), f_{p_{i+1}} \left(x^{\frac{n}{p_i^{n_i} p_{i+1}}} \right), \dots, f_{p_k} \left(x^{\frac{n}{p_i^{n_i} p_k}} \right)$$

в кільці $Z[x]$.

Зробивши заміну x на $x^{p_i^{n_i}}$ отримуємо, що поліном ділення круга $\Phi_{\frac{n}{p_i}} \left(x^{p_i^{n_i}} \right)$, $1 \leq i \leq k$ є лінійною комбінацією многочленів

$$f_{p_1} \left(x^{\frac{n}{p_1}} \right), \dots, f_{p_{i-1}} \left(x^{\frac{n}{p_{i-1}}} \right), f_{p_{i+1}} \left(x^{\frac{n}{p_{i+1}}} \right), \dots, f_{p_k} \left(x^{\frac{n}{p_k}} \right)$$

в кільці $Z[x]$.

Тому поліноми ділення круга $\Phi_n(x)$ при $n > 1$ є лінійною комбінацією многочленів $f_{p_1}\left(x^{\frac{n}{p_1}}\right), \dots, f_{p_k}\left(x^{\frac{n}{p_k}}\right)$ в кільці $Z[x]$.

Тим самим теорема 1 доведена.

Легко бачити, що у вище розглянутих міркуваннях кільце Z , без обмеження загальності, можна замінити на довільну область цілісності R .

6. Формули $\Phi_n(x)$ і $f_n(x)$ в кільці $Z_p[x]$. Нехай p – просте число $n = p^l m$, де $l \geq 1, m \geq 1, (p, m) = 1$. Оскільки $|Z_p^*| = p - 1$, то в полі Z_p має місце рівність $a^{p-1} = 1$ для будь-якого $a \neq 0$ (мала теорема Ферма). Тому в Z_p $a^p = a$ для всіх $a \in Z$. Окрім цього в кільцях Z_p і $Z_p[x]$ мають місце рівності $(a + b)^p = a^p + b^p$ і, як наслідок, $(a + b)^{p^t} = a^{p^t} + b^{p^t}, f(x^{p^t}) = f(x)^{p^t}$, де $f(x)$ – довільний многочлен кільця $Z_p[x], t \geq 0$. Тому в кільці $Z_p[x]$ мають місце формули

$$\Phi_n(x) = \frac{\Phi_m(x^{p^l})}{\Phi_m(x^{p^{l-1}})} = \Phi_m(x)^{p^l - p^{l-1}} = \Phi_m(x)^{\varphi(p^l)},$$

$$f_n(x) = f_{p^l}(x) f_{\frac{n}{p^l}}(x^{p^l}) = f_p(x) \cdots f_p(x^{p^{l-1}}) f_m(x^{p^l}) =$$

$$= f_p(x)^{1 + \dots + p^{l-1}} f_m(x)^{p^l} = f_p(x)^{f_l(p)} \cdot f_m(x)^{p^l}.$$

З них випливає, що якщо просте число p не ділить натуральне число n , то для будь-якого $l \geq 1$ в $Z_p[x]$ мають місце рівності

$$\Phi_{p^l n}(x) = \Phi_n(x)^{\varphi(p^l)}, \quad f_{p^l n}(x) = f_p(x)^{f_l(p)} f_n(x)^{p^l}.$$

7. Критерій знаходження нулів поліномів ділення круга в асоціативних кільцях. Найменше з натуральних чисел, в якому степінь елемента деякої групи дорівнює одиниці, називається порядком елемента, а сам елемент називається елементом скінченного порядку. Якщо таких натуральних чисел не існує, то кажуть, що елемент нескінченного порядку.

Елементи деякого кільця R з $1 \neq 0$, n -а степінь яких дорівнює одиниці, прийнято називати коренями n -го степеня із одиниці цього кільця. Корені k -го степеня із одиниці кільця R , порядок яких дорівнює k , називаються первісними коренями k -го степеня із одиниці кільця R .

Елемент кільця R називається дільником нуля, якщо його добуток з деяким ненульовим елементом кільця R дорівнює нулю.

Нехай R – асоціативне кільце з $1 \neq 0$, r – елемент центра ζR кільця R . Відображення $1 \rightarrow 1, x \rightarrow g(x)$ індукує гомоморфізм $Z \rightarrow R, Z[x] \rightarrow R[x]$, а відображення $1 \rightarrow 1, x \rightarrow r$ гомоморфізм $R[x] \rightarrow R[r] \subset R$, де образом многочлена $f(x) \in R[x]$ є елемент $f(r) \in R$, який утворюється з многочлена $f(x)$ заміною елемента x на r .

Лема 11. Нехай R – асоціативне кільце з $1 \neq 0$, n – натуральне число, $f_n(x) = 1 + x + \dots + x^{n-1}, n \geq 1, a$ – елемент центра ζR порядку n, i – натуральне число, $d = (i, n)$. Тоді $f_n(a^i) = df_{\frac{n}{d}}(a^d)$.

Доведення. Легко бачити, що $a^{\frac{n}{d}i} = 1$ і $f_d(a^{\frac{n}{d}i}) = f_d(1) = d$. Як бу-

ло показано вище $f_n(x) = f_{\frac{n}{d}}(x)f_d(x^{\frac{n}{d}})$. Тому $f_n(a^i) = df_{\frac{n}{d}}(a^i)$. Доведемо, що $f_{\frac{n}{d}}(a^i) = f_{\frac{n}{d}}(a^d)$.

Очевидно, що $a^i = (a^d)^{\frac{i}{d}}$ і $i \in dZ + nZ$. Навпаки. В кільці цілих чисел Z існують цілі числа u і v такі, що $d = ui + vn$. Тому $d \in iZ + nZ$, $a^d = (a^i)^u$. Розглянемо множини $A = \{0d, 1d, \dots, (\frac{n}{d} - 1)d\}$, $B = \{0i, 1i, \dots, (\frac{n}{d} - 1)i\}$. Їх образи в кільці $Z_n = Z/nZ$ позначимо через \bar{A} і \bar{B} відповідно. Тоді $\bar{A} \subseteq i\bar{Z} \subseteq \bar{B} \subseteq d\bar{Z} \subseteq \bar{A}$. Це означає, що множини \bar{A} і \bar{B} в кільці Z_n співпадають. Тому

$$f_{\frac{n}{d}}(a^d) = \sum_{x \in A} a^x = \sum_{x \in A} a^{\bar{x}} = \sum_{y \in B} a^{\bar{y}} = \sum_{y \in B} a^y = f_{\frac{n}{d}}(a^i).$$

Тим самим доведено, що $f_n(a^i) = df_{\frac{n}{d}}(a^i) = df_{\frac{n}{d}}(a^d)$.

Наслідок 6. Якщо в лемі 11 $(i, n) = 1$, то $f_n(a^i) = f_n(a)$, а якщо i – дільник числа n , то $f_n(a^i) = if_{\frac{n}{i}}(a^i)$.

Доведення випливає з формули лемі 11, в якій $d = 1$, якщо $(i, n) = 1$ і $d = i$, якщо i ділить n .

Наслідок 7. Нехай R – асоціативне кільце з $1 \neq 0$, a – елемент порядку $n > 1$ центра ζR кільця R , $f_d(a^{\frac{n}{d}}) = 0$ для всіх дільників $d \neq 1$ числа n . Тоді $f_n(a) = \dots = f_n(a^{n-1}) = 0$. Якщо n не є дільником нуля в R , то вірно і навпаки.

Доведення. Нехай $1 \leq i \leq n - 1$, $d = (i, n)$. Згідно з лемою 11 $f_n(a^i) = df_{\frac{n}{d}}(a^d) = 0$. Навпаки. Нехай n не є дільником нуля в R і $f_n(a) = \dots = f_n(a^{n-1}) = 0$. Згідно з наслідком 6 $if_{\frac{n}{i}}(a^i) = f_n(a^i) = 0$, $f_{\frac{n}{i}}(a^i) = 0$ для будь-якого дільника $1 \leq i < n$ числа n . Тому $f_d(a^{\frac{n}{d}}) = 0$ для всіх дільників $d > 1$ числа n .

Теорема 2. Нехай R – асоціативне кільце з $1 \neq 0$, a – елемент центра ζR кільця R , $\Phi_n(a) = 0$ для деякого натурального числа $n > 1$. Тоді $f_n(a) = \dots = f_n(a^{n-1}) = 0$. Якщо n не є дільником нуля в R , то вірно і навпаки.

Доведення. Нехай $n = p_1^{n_1} \dots p_k^{n_k} > 1$ і $\Phi_n(a) = 0$. Тоді $a^n - 1 = \prod_{d|n} \Phi_d(a) = 0$.

Доведемо теорему 2 індукцією за числом k .

Нехай $k = 1$, $n = p_1^{n_1} > 1$. Оскільки $\Phi_n(x) = \Phi_{p_1^{n_1}}(x) = f_{p_1}(x^{p_1^{n_1-1}})$, то $f_{p_1}(a^{p_1^{n_1-1}}) = \Phi_n(a) = 0$. Нехай $d = (i, n)$, де $1 \leq i \leq n - 1$. Тоді $d = p_1^l$, де $0 \leq l \leq n_1$. За лемою 11 $f_n(a^i) = df_{\frac{n}{d}}(a^d) = p_1^l f_{p_1^{n_1-l}}(a^{p_1^l})$. Згідно з наслідком 5 $f_{p_1^{n_1-l}}(x) = f_{p_1}(x) \dots f_{p_1}(x^{p_1^{n_1-l-1}})$. Тому при $x = a^{p_1^l}$ має місце рівність

$$f_{p_1^{n_1-l}}(a^{p_1^l}) = f_{p_1}(a^{p_1^l}) \dots f_{p_1}(a^{p_1^{n_1-l-1}}) = 0.$$

Це означає, що $f_n(a^i) = p_1^l f_{p_1^{n_1-l}}(a^{p_1^l}) = 0$ для всіх $1 \leq i \leq n - 1$.

Припустимо, що $k > 1$ і твердження теореми 2 доведено для чисел, які є добутками степенів простих чисел, число яких не перевищує $k - 1$ і доведемо

його для чисел, які є добутками степенів k простих чисел. Згідно з лемою 3

$$\Phi_n(x) = \frac{\Phi_{\frac{n}{p_i}}(x^{p_i})}{\Phi_{\frac{n}{p_i}}(x^{p_i-1})},$$

де $1 \leq i \leq k$. Тому $\Phi_{\frac{n}{p_i}}(a^{p_i}) = \Phi_n(a)\Phi_{\frac{n}{p_i}}(a^{p_i-1}) = 0$ для всіх $1 \leq i \leq k$.

Оскільки $n > p_i^{n_i}$, то за припущенням індукції

$$f_{\frac{n}{p_i}}(a^{p_i}) = \dots = f_{\frac{n}{p_i}}\left(a^{p_i\left(\frac{n}{p_i}-1\right)}\right) = 0$$

для всіх $1 \leq i \leq k$. Тому $f_{\frac{n}{p_i}}\left(a^{\left(j+\frac{n}{p_i}t\right)p_i}\right) = f_{\frac{n}{p_i}}(a^{jp_i}) = 0$, $t \in Z$ для всіх натуральних чисел j , які не є кратними $\frac{n}{p_i}$. Оскільки $f_n(x) = f_{p_i}(x) \cdot f_{\frac{n}{p_i}}(x^{p_i})$, то при $x = a^j$ має місце рівність $f_n(a^j) = 0$ для всіх натуральних чисел j , які не є кратними $\frac{n}{p_i}$.

Оскільки для будь-якого числа $1 \leq j < n$ існує число i , $1 \leq i \leq k$ таке, що $\frac{n}{p_i}$ не ділить j , то $f_n(a) = \dots = f_n(a^{n-1}) = 0$.

Якщо припустити, що n не є дільником нуля в R , то теорема 2 вірна і навпаки. Дійсно, нехай $f_n(a) = \dots = f_n(a^{n-1}) = 0$. Очевидно, що в такому разі $n \neq 1$, $a \neq 1$ і $a^n - 1 = (a - 1)f_n(a) = 0$. Нехай k – порядок елемента a . Тоді $1 \leq k \leq n$. Якщо $k < n$, то $k \leq n - 1$ і $0 = f_n(a^k) = f_n(1) = n$, що протирічить припущенню. Тому a – елемент порядку n . Згідно з наслідком 7 $f_d(a^{\frac{n}{d}}) = 0$ для всіх дільників d числа n , а, отже і всіх простих дільників d числа n . Згідно з теоремою 1 $\Phi_n(a) = 0$.

Наслідок 8. *Нехай R – асоціативне кільце з $1 \neq 0$, натуральне число $n \neq 0$ в R , a – елемент центра ζR кільця R , $\Phi_n(a) = 0$. Тоді a – первісний корінь n -го степеня із 1 кільця R . Якщо n і $a^i - 1$ не є дільниками нуля в R для всіх $1 \leq i < n$, то вірно і навпаки.*

Доведення. Нехай $\Phi_n(a) = 0$. Тоді $a^n - 1 = \prod_{d|n} \Phi_d(a) = 0$, a – корінь n -го степеня із 1 кільця R . Якщо $n=1$, то $a=1$ – первісний корінь n -го степеня із 1 кільця R . При $n > 1$, за теоремою 2, має місце рівність $f_n(a) = \dots = f_n(a^{n-1}) = 0$. Якщо $a^i = 1$ для деякого $1 \leq i < n$, то $n = f_n(1) = 0$, що протирічить припущенню.

Навпаки. Нехай a – первісний корінь n -го степеня із 1 кільця R . Якщо $n = 1$, то $a = 1$, $\Phi_1(a) = 0$. Нехай $n > 1$, n і $a^i - 1$ не є дільниками нуля в R для всіх $1 \leq i < n$. З рівності $(a^i - 1)f_n(a^i) = a^{in} - 1 = 0$ випливає, що $f_n(a^i) = 0$ для всіх $1 \leq i < n$. За теоремою 2 $\Phi_n(a) = 0$.

Відмітимо, що у випадку, коли $a^i - 1$, $1 \leq i < n$ не є дільником нуля в R , умови $f_n(a^i) = 0$ і $a^{in} - 1 = 0$ рівносильні.

Наслідок 9. *Нехай R – область цілісності, натуральне число $n \neq 0$ в R , $a \in R$. Рівність $\Phi_n(a) = 0$ має місце тоді і тільки тоді, коли a – первісний корінь n -го степеня із 1 кільця R .*

Доведення випливає з наслідку 8. Адже, якщо a – первісний корінь n -го степеня із 1, то $a^i - 1$ не є дільниками нуля в R для всіх $1 \leq i < n$.

Наслідок 10. *Нехай $R = Z_p$, p – просте число, $(n, p) = 1$, $n \geq 1$. Поліном ділення круга $\Phi_n(x)$ має корені в полі Z_p тоді і тільки тоді, коли n ділить $p - 1$.*

Доведення. Нехай $a \in Z_p$ і $\Phi_n(a) = 0$ в Z_p . Тоді, згідно з наслідком 9, a – первісний корінь n -го степеня із 1 поля Z_p . Оскільки в полі Z_p має місце рівність $a^{p-1} = 1$, то n ділить $p - 1$.

Навпаки. Якщо n ділить $p - 1$, то $a = \varepsilon^{\frac{p-1}{n}}$ – первісний корінь n -го степеня із 1, де ε – первісний корінь $p - 1$ -го степеня із 1 поля Z_p . За наслідком 9 $\Phi_n(a) = 0$.

Нехай I – множина всіх простих дільників значень многочлена позитивного степеня $p(x) \in Z[x]$ на множині цілих чисел, $p(0) \neq 0$ і n_0 деяке натуральне число, яке більше від 1 і всіх показників степенів простих чисел, що є дільниками $p(0)$.

Якщо I – скінчена множина, яка складається з простих чисел p_1, \dots, p_t і $a = (p_1 \dots p_t)^{n_0}$, то $p(a^l)$, $l \geq 1$ не містить дільників p^k , де p – просте число і $k \geq n_0$. Адже, в протилежному випадку, $p \in I$ і p^{n_0} ділить $p(0)$, що протирічить припущенню.

Тому $p(a^l) = 0$ або $p(a^l)$, з точністю до знаку, є добутком степенів простих чисел p_1, \dots, p_t з показниками степеня меншими від n_0 . Це означає, що множина J значень $p(a^l)$ є скінченою множиною. Нехай J складається з цілих чисел j_1, \dots, j_r . Тоді многочлен $p_0(x) = (p(x) - j_1) \dots (p(x) - j_r)$ має нескінчену кількість коренів a^l , $l \geq 1$. Тому $p_0(x) \equiv 0$ і, як наслідок, многочлен $p(x)$ не є многочленом позитивного степеня.

Отримане протиріччя показує, що I – нескінчена множина. Тому існує нескінченне число простих чисел p , для яких многочлен $p(x)$ має корені в полі Z_p .

Зокрема, якщо в ролі $p(x)$ вибрати поліном ділення круга $\Phi_n(x)$, то існує нескінченне число простих чисел p таких, що $\Phi_n(x)$ має корені в Z_p і, згідно з наслідком 10, n ділить $p - 1$, $p \in 1 + nZ$.

Насправді для будь-яких взаємно простих натуральних чисел m і n існує нескінченне число простих чисел p , таких що $p \in m + nZ$ (теорема Діріхле).

8. Корені з одиниці в комутативних кільцях. Нехай G – група, порядки всіх елементів якої обмежені деяким числом. Найменше спільне кратне порядків всіх елементів групи G називають експонентою групи G і позначають $\text{exp } G$.

У тих випадках, коли мова йде про експоненту вважають, що вона існує. Ясно, що $g^{\text{exp } G} = 1$ для всіх елементів g групи G .

Лема 12. *Експонента комутативної групи є найменшим з натуральних чисел, які обмежують порядки всіх елементів групи.*

Доведення. Нехай G – комутативна група, порядки всіх елементів якої обмежені деяким натуральним числом n_0 і g_0 – елемент групи G порядок якого дорівнює n_0 . Очевидно, що $n_0 \leq \text{exp } G$.

Нехай p – довільне просте число і p^t , $t \geq 0$ – найбільша степінь числа p , яка ділить n_0 . Тоді $g_0^{p^t}$ має порядок $\frac{n_0}{p^t}$. Зрозуміло, що якщо група G містить елемент, порядок якого ділиться на p^{t+1} , то вона містить елемент h , порядок якого дорівнює p^{t+1} . В такому разі порядки елементів $g_0^{p^t}$ і h є взаємно простими

числами $\frac{n_0}{p^t}$ і p^{t+1} відповідно. Тому порядок елемента $g_0^{p^t} h$ дорівнює $\frac{n_0}{p^k} \cdot p^{t+1} = n_0 p > n_0$, що протирічить припущенню. Тим самим доведено, що порядки всіх елементів групи G ділять n_0 . Згідно з означенням експоненти групи G має місце нерівність $\text{exp } G \leq n_0$ і, як наслідок, $\text{exp } G = n_0$.

Це означає, що експонента будь-якої комутативної групи співпадає з найвищим порядком її елементів.

Зокрема, експонента скінченної комутативної групи G ділить її порядок $|G|$, а тому $\text{exp } G \leq |G|$. Більше того, скінченна комутативна група є циклічною тоді і тільки тоді, коли $\text{exp } G = n_0 = |G|$. Тому прямий добуток скінчених комутативних груп є циклічною групою тоді і тільки тоді, коли ці групи є циклічними групами попарно взаємно простих порядків.

Лема 13. *Нехай R – область цілісності, G – підгрупа групи R^* експоненти $\text{exp } G$. Тоді G – скінченна циклічна група, порядок якої $|G| = \text{exp } G$.*

Доведення. Нехай, як в лемі 13, g_0 – елемент найвищого порядку n_0 групи G , $n_0 = \text{exp } G$. Оскільки всі елементи $1, g_0, \dots, g_0^{n_0-1}$ є різними коренями двочлена $x^{n_0} - 1$, то в кільці $R[x]$ має місце розклад

$$x^{n_0} - 1 = (x - 1)(x - g_0) \cdots (x - g_0^{n_0-1}).$$

З нього випливає, що $G = \langle g_0 \rangle$ – циклічна група, яка породжена елементом найвищого порядку g_0 групи G . При цьому $|G| = n_0 = \text{exp } G$.

Наслідок 11. *Нехай R – область цілісності, n – натуральне число, G – група коренів n -го степеня із 1 кільця R . Тоді G – скінченна циклічна група, порядок якої $|G| = \text{exp } G$ ділить n .*

Доведення. Очевидно, що $|G| = \text{exp } G = n_0$ ділить n . Тому, згідно з лемою 13, G – скінченна циклічна група, порядок якої ділить n .

Група коренів n -го степеня із 1 області цілісності R є підгрупою групи коренів n -го степеня із 1 алгебраїчного замикання $\overline{Q(R)}$ поля відношень $Q(R)$ кільця R , яка також є циклічною групою.

Якщо при цьому $n \neq 0$ в R , то $n \in Q(R)^*$, характеристика $\text{char } Q(R)$ поля $Q(R)$ не ділить n . Із взаємної простоти многочленів $x^n - 1$ і nx^{n-1} при $n > 1$ в $\overline{Q(R)}[x]$ випливає, що всі n коренів n -го степеня із 1 в $\overline{Q(R)}$ є різними. Вони утворюють циклічну групу порядку n , породжуючий елемент якої є первісним коренем n -го степеня із 1.

Якщо $n = 0$, то $n = p^l k$, де $p = \text{char } Q(R)$ – просте число, $l \geq 1$, $(p, k) = 1$, $k \in Q(R)^*$. Оскільки $x^n - 1 = (x^k - 1)^{p^l}$, то корені n -го степеня із 1 поля $\overline{Q(R)}$ є коренями k -го степеня із 1 і утворюють циклічну групу порядку k , породжуючий елемент якої є первісним коренем k -го степеня із 1.

Теорема 3. *Нехай R – комутативне кільце з $1 \neq 0$, n – натуральне число, J – простий ідеал R , такий що всі елементи множини $n + J$ не є дільниками нуля в R , G – група коренів n -го степеня з 1 кільця R . Тоді G – скінченна циклічна група, порядок якої ділить n .*

Доведення. Нехай $\bar{G} = \Lambda_J G$, де $\Lambda_J : R \rightarrow \bar{R} = R/J$ – натуральний гомоморфізм. Якщо $g \in G \cap \ker \Lambda_J$, то $g = 1 + j$, де $j \in J$. З рівності $(1 + j)^n = 1$ випливає, що $j(n + jr) = 0$, де $r \in R$. Оскільки $n + jr$ не є дільником нуля в R , то $j = 0$ і $g = 1$. Це означає, що $\Lambda_J : G \rightarrow \bar{G}$ є ізоморфізмом груп G і \bar{G} .

Згідно з наслідком 11, $\bar{G} = \langle \bar{\varepsilon} \rangle$ – скінчена циклічна група, порядок якої k ділить n , $\varepsilon \in G$. Оскільки G і \bar{G} – ізоморфні групи, то $G = \langle \varepsilon \rangle$ – скінчена циклічна група, порядок якої k ділить n . При цьому $\varepsilon^i - \varepsilon^j \notin J$ для всіх $1 \leq i \neq j \leq k$.

Наслідок 12. *Нехай в умовах теореми 3 $(1 + J)^t = 1$, де $(n, t) = 1$. Тоді група G ізоморфна групі всіх коренів n -го степеня із 1 кільця \bar{R} .*

Доведення. За наслідком 11 корені n -го степеня з 1 кільця \bar{R} утворюють циклічну групу G' , порядок якої ділить n . Очевидно, що $\bar{G} \subset G'$.

Нехай $r \in R$, такий що \bar{r} породжує групу G' . Тоді \bar{r}^t також породжує групу G' . Оскільки $r^n \in 1 + J$, то $r^{nt} = 1$, $r^t \in G$ і, як наслідок, $G' \subset \bar{G}$. Тому $\bar{G} = G'$. За теоремою 3 групи G і $\bar{G} = G'$ – ізоморфні. Тим самим доведено, що група G ізоморфна групі всіх коренів n -го степеня із 1 кільця \bar{R} .

Із теореми 3 випливає, що якщо R – комутативне локальне кільце, $n \in R^*$, $J = J(R)$ – радикал Джекобсона кільця R , то корені n -го степеня із 1 кільця R утворюють скінченну циклічну групу, порядок якої ділить n .

Якщо при цьому $(1 + J(R))^t = 1$, $(t, n) = 1$, то група коренів n -го степеня із 1 кільця R і поля $R/J(R)$ є ізоморфними.

Відмітимо, що в довільній області цілісності тільки ± 1 є коренями другого степеня із 1. Тому, якщо J – простий ідеал, $n = 2$, елементи множини $2 + J$ не є дільниками нуля в R , то група коренів 2-го степеня із 1 кільця R належить ± 1 .

Легко бачити, що в кільці $R[x]$

$$x^n - 1 = (x^k)^{\frac{n}{k}} - 1 = (x^k - 1) f_{\frac{n}{k}}(x^k), f_{\frac{n}{k}}(x^k) = \prod_{d|n, d \nmid k} \Phi_d(x) = \prod_{d|\frac{n}{k}, d \neq 1} \Phi_d(x^k).$$

З теореми 3 випливає, що многочлен $f_{\frac{n}{k}}(x^k)$ не має коренів в $\bar{R} = R/J$.

Адже, якщо $r \in R$ і $f_{\frac{n}{k}}(\bar{r}^k) = \bar{0}$, то $\bar{r}^n = \bar{1}$ і, як наслідок, теореми 3, $\bar{r}^k = \bar{1}$ і $\bar{0} = f_{\frac{n}{k}}(\bar{r}^k) = \bar{\frac{n}{k}}$. Тому $n \in J$ і $n + J$ містить нульовий елемент, що протирічить припущенню про те, що всі елементи множини $n + J$ не є дільниками нуля в R .

Це означає, що поліноми ділення круга $\Phi_d(x)$, $d|n$, $d \neq k$ і $\Phi_d(x^k)$, $d|\frac{n}{k}$, $d \neq 1$ не мають коренів в кільцях \bar{R} і R .

Нехай R – область цілісності, в якій $J = 0$, $n \neq 0$, $k = 1$. Тоді n – непарне число і $\Phi_d(x)$, $d|n$, $d \neq 1$ не мають коренів в R .

Зокрема, $\Phi_3(x) = x^2 + x + 1$ не має коренів і є незвідним в полі Z_p , якщо 3 не ділить $p - 1$.

Однак, розраховувати на те, що поліноми ділення круга $\Phi_n(x)$ є незвідними над полями, в яких вони не мають коренів і $n \neq 0$ не можна. Адже, над полем $R = Z_3[\sqrt{5}]$, в якому $5 \neq 0$ і не містить неодиначних коренів 5-го степеня із 1, поліном ділення круга

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = (x^2 - (\sqrt{5} + 1)x + 1)(x^2 + (\sqrt{5} - 1)x + 1)$$

не має коренів в R , але є звідним.

9. Структура кільця Z_{p^l} . Нехай p – просте число, l – натуральне число. Тоді Z_{p^l} – комутативне локальне кільце з радикалом pZ_{p^l} і фактор-кільцем по радикалу, яке ізоморфне полю Z_p .

Оскільки $p - 1 \in Z_{p^l}^*$, $(1 + pZ_{p^l})^{p^l} = 1$ в Z_{p^l} , то, згідно з наслідком 12, група коренів $p - 1$ -го степеня із 1 кільця Z_{p^l} ізоморфна групі коренів $p - 1$ -го степеня із 1 поля Z_p , яке є циклічною групою порядку $p - 1$. Тим самим доведено, що кільце Z_{p^l} містить циклічну групу порядку $p - 1$.

Як було сказано вище порядок групи $Z_{p^l}^*$ дорівнює $\varphi(p^l) = p^{l-1}(p - 1)$. Тому група $Z_{p^l}^*$ є одиничною тоді і тільки тоді, коли $p = 2$ і $l = 1$, а неединична група $Z_{p^l}^*$ має парний порядок.

Лема 14. *Нехай p – просте число, $l \geq 1$. Елемент $1 + p$ в кільці Z_{p^l} породжує циклічну групу порядку p^{l-1} при $p > 2$ або при $p = 2$, $l \leq 2$ і циклічну групу порядку p^{l-2} при $p = 2$, $l \geq 3$, яка не містить -1 .*

Доведення. Легко бачити, що при $(p, t) = 1$ має місце рівність

$$(1 + p^i t)^p = 1 + p^{i+1}t + \frac{p(p-1)}{2} (p^i t)^2 + \dots = 1 + p^{i+1}t_1,$$

де $(p, t_1) = 1$ при $p > 2$, $i \geq 1$ або $p = 2$, $i > 1$. В цих випадках порядок елемента $1 + p^i t$ в групі $Z_{p^l}^*$ дорівнює p^{l-i} .

Тому елемент $1 + p$ при $p > 2$ має порядок p^{l-1} . Це твердження, як показує безпосередня перевірка, залишається вірним і при $p = 2$, $l \leq 2$.

Нехай $p = 2$, $l \geq 3$. Елемент $(1 + p)^p = 1 + p^3$, згідно з вищесказаним, має порядок p^{l-3} . Тому елемент $1 + p$ має порядок p^{l-2} .

Якщо при цьому $-1 = (1 + p)^s$, то p^2 ділить $2 + ps$, $(p, s) = 1$, $1 = (1 + p)^{ps}$, p^{l-2} ділить ps . Тому при $l > 3$ елемент -1 не є степенем елемента $1 + p$. Як показує безпосередня перевірка, це твердження залишається вірним і при $p = 2$, $l = 3$.

З вище наведеного випливає, що група $Z_{p^l}^*$ при $p > 2$ містить циклічні підгрупи порядків $p - 1$ і p^{l-1} , а тому є циклічною групою порядку $\varphi(p^l)$. При $p = 2$, $l = 1$ група $Z_{p^l}^*$ є одиничною, а при $p = 2$, $l = 2$ є циклічною. При $p = 2$, $l \geq 3$ група $Z_{p^l}^*$ є прямим добутком циклічних груп порядків p^{l-2} і p , породжених елементом $1 + p$ і елементом -1 відповідно, а тому не є циклічною.

Зауважимо, що якщо a – елемент порядку $p - 1$ групи $Z_{p^l}^*$, то

$$a = a^p = \dots = a^{p^{l-1}} = a^{p^l}, (a^i - 1)(f_p(a^i) - 1) = a^i(a^{i(p-1)} - 1) = 0,$$

при $i \geq 1$. Оскільки комутативна група $Z_{p^l}^*$ породжується елементом a і коренем p^{l-1} -степеня із 1, то для всіх елементів $r \in Z_{p^l}^*$ в кільці Z_{p^l} має місце рівність $r^{p^{l-1}} = r^{p^l}$, яка дорівнює 1 або є степенем елемента a .

При $p > 2$ елементи $a^i - 1 \in Z_{p^l}^*$, $f_p(a^i) = 1$ для всіх $1 \leq i < p$.

З леми 14 також випливає результат про умови циклічності групи Z_n^* для довільного натурального числа $n > 1$.

Нехай $n = p_1^{n_1} \dots p_k^{n_k}$ – розклад натурального числа $n > 1$ в добуток степенів різних простих чисел p_1, \dots, p_k , $k \geq 1$. За китайською теоремою про остачі

$$Z_n \cong Z_{p_1^{n_1}} \oplus \dots \oplus Z_{p_k^{n_k}}, Z_n^* \cong Z_{p_1^{n_1}}^* \otimes \dots \otimes Z_{p_k^{n_k}}^*.$$

Оскільки неединичні групи $Z_{p_i^{n_i}}^*$ мають парний порядок, то Z_n^* – циклічна група тоді і тільки тоді, коли $k \leq 2$ і при $k = 2$ одна із груп $Z_{p_1^{n_1}}^*$, $Z_{p_2^{n_2}}^*$ є

одиночною, а друга циклічною групою. Як було показано вище це можливо лише якщо кільце Z_n має вигляд Z_2 або Z_4 або Z_{p^l} або $Z_2 \oplus Z_{p^l}$, тобто коли n дорівнює 2 або 4 або є степенем або подвоєним степенем простого непарного числа.

10. Значення поліномів ділення круга в кільці Z . Нехай $n \geq 1$. Очевидно, що $f_n(0) = 1$, $f_n(1) = n$ і

$$f_n(-1) = \begin{cases} 1, & n - \text{непарне число} \\ 0, & n - \text{парне число} . \end{cases}$$

Лема 15. Нехай $n > 1$. Тоді $\Phi_n(0) = 1$. Якщо n – степінь простого числа p , то $\Phi_n(1) = p$. В решті випадків $\Phi_n(1) = 1$.

Доведення. Нехай $n = p^l m$, $(p, m) = 1$, $l \geq 1$, $m \geq 1$. Якщо $m = 1$, то $\Phi_n(x) = f_p(x^{p^{l-1}})$. Тому $\Phi_n(0) = f_p(0) = 1$ і $\Phi_n(1) = f_p(1) = p$.

Нехай $m > 1$. З індуктивних міркувань за числом різних простих дільників числа m випливає, що $\Phi_m(0) = 1$ і $\Phi_m(1) = q$, якщо m – степінь простого числа q і $\Phi_m(1) = 1$ в решті випадків. З формули $\Phi_n(x)\Phi_m(x^{p^{l-1}}) = \Phi_m(x^{p^l})$ випливає, що $(\Phi_n(0) - 1)\Phi_m(0) = 0$ і $(\Phi_n(1) - 1)\Phi_m(1) = 0$. Оскільки $\Phi_m(0) = 1$ і $\Phi_m(1) \neq 0$ є дільниками нуля в кільці Z , то $\Phi_n(0) = 1$ і $\Phi_n(1) = 1$.

Легко бачити, що $\Phi_1(0) = -1$ і $\Phi_1(1) = 0$.

Наслідок 13. Нехай $n > 2$. Якщо n – парне число і $\frac{n}{2}$ – степінь простого числа q , то $\Phi_n(-1) = q$. В решті випадків $\Phi_n(-1) = 1$.

Доведення. Нехай $n = p^l m$, $(p, m) = 1$, $l \geq 1$, $m \geq 1$, де p – просте число. Нехай n – непарне число, $n > 1$. За формулою $\Phi_n(x)\Phi_n(-x) = \Phi_n(x^2)$ і лемою 15 $\Phi_n(-1) = 1$.

Нехай n – парне число. Можна вважати, що $p = 2$ і m – непарне число. За наслідком 3

$$\Phi_n(-1) = \begin{cases} -\Phi_m(-(-1)^{2^{l-1}}), & m = 1, \\ \Phi_m(-(-1)^{2^{l-1}}), & m > 1. \end{cases}$$

Тому при $l > 1$ має місце рівність

$$\Phi_n(-1) = \begin{cases} -\Phi_m(-1) = 2, & m = 1, \\ \Phi_m(-1) = 1, & m > 1. \end{cases}$$

При $l = 1$ за умовою $m > 1$ і $\Phi_n(-1) = \Phi_m(1)$. Згідно з лемою 15 $\Phi_n(-1) = q$, якщо $m = \frac{n}{2}$ – степінь простого числа q і $\Phi_n(-1) = 1$ в решті випадків.

Очевидно, що $\Phi_1(-1) = -2$ і $\Phi_2(-1) = 0$.

З леми 15 та наслідку 13 випливає що $\Phi_n(x)$ є незвідним многочленом над Z , якщо n – степінь або подвоєна степінь простого числа, тобто в рівності $n = p^l m$, де $(p, m) = 1$ число m дорівнює 1 або 2, $\Phi_m(x) = x \mp 1$ відповідно. Тому в кільці $Z_p[x]$ має місце рівність $\Phi_n(x) = (x \mp 1)^{\varphi(p^l)}$.

Якщо $\Phi_n(x) = u(x)v(x)$ в кільці $Z[x]$, де $\deg u(x) < \varphi(n)$ і $\deg v(x) < \varphi(n)$, то в $Z_p[x]$ многочлени $u(x)$ і $v(x)$ є степенями двочленів $x \mp 1$. Тому $u(1)$ і $v(1)$ або $u(-1)$ і $v(-1)$ діляться на p , а $\Phi_n(\pm 1)$ на p^2 відповідно, що, згідно з лемою 15 та її наслідком 13, є неможливим.

Насправді $\Phi_n(x)$ є незвідним многочленом над кільцем цілих чисел для всіх натуральних чисел n .

11. Значення поліномів ділення круга в кільці Z_{p^l} .

Лема 16. Нехай $n = p^l m$, p – просте число, $(p, m) = 1$, $l \geq 1$, $m \geq 1$, $m = 2^\alpha p_1^{n_1} \dots p_k^{n_k}$, p_1, \dots, p_k – непарні числа, a – елемент порядку $p-1$, b – степінь a порядку $p_1 \dots p_k$ кільця Z_{p^l} , r – довільний елемент кільця Z_{p^l} , $r^{p^{l-1}} = a^s$, $1 \leq s \leq p-1$. Тоді $\Phi_n(r) = 1$ або m ділить $p-1$, $\frac{p-1}{m}$ ділить s і $\Phi_n(r) = \Phi_{pp_1 \dots p_k}(\pm b^{\frac{sm}{p-1}})$.

Доведення. Очевидно $m \notin pZ_{p^l}^*$. Нехай $r \in Z_{p^l}$, $r_1 = r^{p^{l-1}}$, a – елемент порядку $p-1$ кільця Z_{p^l} . Зрозуміло, що $a = 1$ при $p = 2$ і $a^i - 1 \in Z_{p^l}^*$, $f_p(a^i) = 1$ для всіх $1 \leq i < p-1$ при $p > 2$.

Якщо $r \in pZ_{p^l}$, то $r_1 \in p^{p^{l-1}}Z_{p^l} = 0$.

Оскільки група $Z_{p^l}^*$, згідно з лемою 14 породжується елементом a і коренями p^{l-1} степеня із 1 кільця Z_{p^l} , то $r_1 = 1$ при $p = 2$ і $r_1 = a^s$, де $1 \leq s \leq p-1$ при $p > 2$. Зрозуміло, що при $s = p-1$ елемент $r_1 = 1$.

З формули $\Phi_n(x)\Phi_m(x^{p^{l-1}}) = \Phi_m(x^{p^l})$ випливають рівності $(\Phi_n(r) - 1)\Phi_m(0) = 0$ при $r \in pZ_{p^l}$, $(\Phi_n(r) - 1)\Phi_m(a^s) = 0$ при $r \in Z_{p^l}^*$.

Згідно з лемою 15, $\Phi_m(0) = 1$ при $m \geq 1$. Тому $\Phi_n(r) = 1$ для всіх $r \in pZ_{p^l}$. Нехай $r \in Z_{p^l}^*$. Якщо $m = 1$, то $\Phi_n(r) = f_p(r_1)$ дорівнює p при $r_1 = 1$ і дорівнює 1 в решті випадків.

Нехай $m > 1$ і $r_1 = 1$. Згідно з лемою 15 $\Phi_m(1) = 1$ або $\Phi_m(1) = q$ – просте число, якщо m – степінь q . Оскільки q ділить m , то $q \in Z_{p^l}^*$, $\Phi_m(1) \in Z_{p^l}^*$, $\Phi_n(r) = 1$.

Зрозуміло, що $\Phi_n(r) = 1$ і тоді коли $\Phi_m(a^s) \in Z_{p^l}^*$ при $p > 2$ і $1 \leq s < p-1$.

Розглянемо випадок $m > 1$ і $\Phi_m(a^s) \in p^j Z_{p^l}$, де $p > 2$, $1 \leq j \leq l$, $r^{p^{l-1}} = a^s$, $1 \leq s < p-1$. Тоді $\Phi_m(a^s) = 0$ в полі Z_p і за наслідком 8 порядок елемента a^s дорівнює m . Тому a в полі Z_p має порядок ms_1 , де s_1 ділить s , $s = s_1 s_2$. З другого боку, порядок елемента a в полі Z_p дорівнює $p-1$. Тому $s_1 m = p-1$. З отриманої рівності, зокрема, випливає, що якщо m не ділить $p-1$, то $\Phi_n(r) = 1$ для всіх $r \in Z_{p^l}^*$.

Нехай m ділить $p-1$, $m = 2^\alpha m_1$, де $\alpha \geq 0$, m_1 – непарне число, $m_1 \geq 1$.

Якщо $m_1 > 1$, то $m_1 = p_1^{n_1} \dots p_k^{n_k}$, де p_1, \dots, p_k – різні прості непарні числа. При $m_1 = 1$ вважаємо, що прості числа p_1, \dots, p_k – відсутні.

Отже, $n = p^l m = p^l 2^\alpha p_1^{n_1} \dots p_k^{n_k}$.

Нехай $\alpha \geq 1$. За наслідками 2 і 3

$$\Phi_n(x) = \Phi_{2pp_1 \dots p_k} \left(x^{2^{\alpha-1} p^{l-1} p_1^{n_1-1} \dots p_k^{n_k-1}} \right) = \Phi_{pp_1 \dots p_k} \left(-x^{2^{\alpha-1} p^{l-1} p_1^{n_1-1} \dots p_k^{n_k-1}} \right).$$

Нехай $b = -a^{2^{\alpha-1} p_1^{n_1-1} \dots p_k^{n_k-1} s_1}$. Оскільки $a^{p-1} = 1$, то $b^{p-1} = 1$, $b^{2p_1 \dots p_k} = a^{m s_1} = 1$, то $(b^{p_1 \dots p_k} + 1)(b^{p_1 \dots p_k} - 1) = 0$. Якщо $b^{p_1 \dots p_k} + 1$ ділиться на p , то в полі Z_p має місце рівність $a^{\frac{p-1}{2}} = a^{2^{\alpha-1} m_1 s_1} = -b^{p_1 \dots p_k} = 1$, що протирічить порядку елемента a . Тому $b^{p_1 \dots p_k} = 1$.

З рівності $1 = b^{p_1 \dots p_{i-1} p_{i+1} \dots p_k} = -a^{\frac{p-1}{2p_i}}$ випливає, що $a^{\frac{p-1}{p_i}} = 1$, що протирічить порядку елемента a .

Це означає, що в кільці Z_{p^l} і за наслідком 12 в полі Z_p елемент b має порядок

$p_1 \cdot \dots \cdot p_k$. При цьому

$$\begin{aligned}\Phi_n(r) &= \Phi_{2pp_1 \dots p_k} \left(r^{2^{\alpha-1} p^{l-1} p_1^{n_1-1} \dots p_k^{n_k-1}} \right) = \Phi_{pp_1 \dots p_k} \left(-a^{2^{\alpha-1} p_1^{n_1-1} \dots p_k^{n_k-1} s} \right) = \\ &= \Phi_{pp_1 \dots p_k} (\pm b^{s_2}).\end{aligned}$$

Аналогічно при $m_1 \geq 1$ і $\alpha = 0$ показуємо, що елемент $b = a^{p_1^{n_1-1} \dots p_k^{n_k-1} s_1}$ має порядок $p_1 \dots p_k$ і $\Phi_n(r) = \Phi_{pp_1 \dots p_k}(b^{s_2})$.

Зрозуміло, що якщо $m_1 = 1$, то в обох випадках $b = 1$.

Якщо $\Phi_p(\pm b^d) = 0$, то згідно з наслідком 8, $b^{dp} = \pm 1$ відповідно. Тому dp або відповідно $2dp$ і, як наслідок, d діляться на $p_1 \dots p_k$. Це означає, що $\Phi_p(\pm b^d) \in Z_{p^l}^*$ для всіх d , які не діляться на $p_1 \dots p_k$ і $\Phi_p(\pm b^d) = \Phi_p(\pm 1)$ дорівнює p або 1 для всіх d , які діляться на $p_1 \dots p_k$.

Без обмеження загальності можна вважати, що s_2 ділиться на $p_1 p_2 \dots p_t$ і не ділиться на p_{t+1}, \dots, p_k , де $t \leq k$. Для всіх дільників d числа $p_1 \cdot p_2 \cdot \dots \cdot p_k$, які діляться на $p_{t+1} \cdot \dots \cdot p_k$ має місце рівність $b^{s_2 d} = 1$, $\Phi_p(b^{s_2 d}) = \Phi_p(1) = p$. В решті випадків $\Phi_p(\pm b^{s_2 d}) \in Z_{p^l}^*$. Згідно з лемою 2

$$\Phi_{pp_1 \dots p_k}(x) = \prod_{d|p_1 \dots p_k} \Phi_p(x^d)^{\mu\left(\frac{p_1 \dots p_k}{d}\right)}.$$

Позначимо $F_i(x) = \prod_{d|p_1 \dots p_k} \Phi_p(x^d)$ для яких $\mu\left(\frac{p_1 \dots p_k}{d}\right) = (-1)^{i+1}$, де $i = 1, 2$.

Зрозуміло, що $\Phi_{pp_1 \dots p_k}(x) = \frac{F_1(x)}{F_2(x)}$, $F_i(b^{s_2}) = p^{j - \sum_{\text{парні}} C_t^j} \alpha_i = p^{2^{t-1}} \alpha_i$, де $\alpha_i \in Z_{p^l}^*$. Тому $(\Phi_n(r) - \alpha) p^{2^{t-1}} = 0$ в Z_{p^l} , де $\alpha \in Z_{p^l}^*$.

З леми 16 випливає

Теорема 4. *Нехай $n = p^l m$, p – просте число, $(p, m) = 1$, $l \geq 1$, $m \geq 1$, $m = 2^\alpha p_1^{n_1} \dots p_k^{n_k}$, p_1, \dots, p_k – непарні прості числа, a – елемент порядку $p-1$, b – степінь a порядку $p_1 \dots p_k$, $r^{p^l-1} = a^s$ за модулем p^l , $1 \leq s \leq p-1$, r – довільний елемент кільця Z . Тоді за модулем p^l $\Phi_n(r) = 1$ або m ділить $p-1$ і $\frac{p-1}{m}$ ділить s та $\Phi_n(r) = \Phi_{pp_1 \dots p_k}(\pm b^{\frac{sm}{p-1}})$.*

12. Поліноми ділення круга над комутативними кільцями. З теореми 4 випливає, що поліном ділення круга $\Phi_n(x)$ при $n > 1$ має корені в кільці Z_n коли n є добутком простих чисел без кратності.

Нехай R – комутативне кільце з $1 \neq 0$. В кільці $R[x]$ розглянемо многочлени, які є образами многочленів кільця $Z[x]$ при гомоморфізмі кільця $Z[x] \rightarrow R[x]$, який індукується кільцевим гомоморфізмом $Z \rightarrow R$ за правилом $1 \rightarrow 1$, $x \rightarrow x$. Ці образи в $R[x]$ будемо позначати і називати так, як і їх прообрази в кільці $Z[x]$.

Нехай k – дільник n . Згідно з означенням в $Z[x]$ і $R[x]$ мають місце рівності

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \quad x^k - 1 = \prod_{d|k} \Phi_d(x).$$

З них випливає, що

$$x^n - 1 = (x^k - 1) \prod_{d|n, d \nmid k} \Phi_d(x), \quad x^n - 1 = (x^k)^{\frac{n}{k}} - 1 = (x^k - 1) \prod_{d|\frac{n}{k}, d \neq 1} \Phi_d(x^k).$$

З другого боку $x^n - 1 = (x^k)^{\frac{n}{k}} - 1 = (x^k - 1) f_{\frac{n}{k}}(x^k)$.

Оскільки строго унітарний двочлен $x^k - 1$ не є дільником нуля в кільцях $Z[x]$ і $R[x]$, то

$$f_{\frac{n}{k}}(x^k) = \prod_{d|n, d \nmid k} \Phi_d(x) = \prod_{d|\frac{n}{k}, d \neq 1} \Phi_d(x^k).$$

Нехай \tilde{R} – комутативне розширення кільця R і група коренів n -го степеня із 1 кільця \tilde{R} є циклічною групою з породжуючим елементом ε , порядок якого дорівнює k і $\varepsilon^i - \varepsilon^j$ не є дільниками нуля в \tilde{R} для всіх $0 < i \neq j \leq k$. Тоді k ділить n , $x^k - 1 = \prod_{0 < i \leq k} (x - \varepsilon^i)$.

Нехай d – дільник k . Тоді елемент $\varepsilon^{\frac{k}{d}}$ має порядок d і елементи $\varepsilon^{\frac{k}{d}s}$, $0 < s \leq d$, $(s, d) = 1$ складають множину всіх первісних коренів d -го степеня із 1 кільця \tilde{R} . Їх число дорівнює $\varphi(d)$. Оскільки первісні корені різних степенів d , які ділять k , є різними і $\sum_{d|k} \varphi(d) = k$, то множина всіх коренів n -го степеня із 1 кільця \tilde{R} є

об'єднанням різних підмножин первісних коренів d -го степеня із 1 кільця \tilde{R} по всіх дільниках d числа k . Позначимо

$$\Phi'_1(x) = x - 1, \Phi'_d(x) = \prod_{0 < s \leq d, (s,d)=1} (x - \varepsilon^{\frac{k}{d}s}) \text{ при } d > 1.$$

Зрозуміло, що $\Phi'_d(x)$ – строго унітарний многочлен кільця \tilde{R} , $\deg \Phi'_d(x) = \varphi(d)$, $x^k - 1 = \prod_{d|k} \Phi'_d(x)$. Із аналогічних міркувань доводиться, що для дільників l числа

k має місце рівність $x^l - 1 = \prod_{d|l} \Phi'_d(x)$. Це означає, що поліноми ділення круга

$\Phi_d(x)$ і многочлени $\Phi'_d(x)$ в кільці $\tilde{R}[x]$ знаходяться за таким же правилом, як і поліноми ділення круга $\Phi_d(x)$ в кільці $Z[x]$. Тому

$$\Phi_d(x) = \Phi'_d(x) = \prod_{0 < s \leq d, (s,d)=1} (x - \varepsilon^{\frac{k}{d}s}), \quad \deg \Phi'_d(x) = \varphi(d)$$

для всіх дільників d числа k і має місце розклад

$$x^k - 1 = \prod_{d|k} \Phi_d(x), \Phi_k(x) = \prod_{0 < s \leq d, (s,d)=1} (x - \varepsilon^s).$$

Оскільки корені многочлена $\Phi_d(x)$ є первісними коренями порядку d кільця \tilde{R} , то корені многочлена $\Phi_k(x)$ не є коренями многочлена $\Phi_d(x)$, де $0 < d < k$ і $d|k$.

Зокрема, якщо \overline{R} – область цілості, то в якості \tilde{R} можна вибрати алгебраїчне замикання $\overline{Q(R)}$ його поля відношень $Q(R)$. Нехай $n = p^l k$, де $p = \text{char} Q(R)$, $p > 0$, $(p, k) = 1$. Корені n -го степеня з 1 поля $\overline{Q(R)}$ є коренями k -го степеня із 1, які утворюють циклічну групу порядку k . З вище наведеного випливає, що первісні корені k -го степеня із 1 поля $\overline{Q(R)}$ складають множину всіх коренів полінома ділення круга $\Phi_k(x)$ в $\overline{Q(R)}$.

13. Мінімальні многочлени Нехай R – комутативне кільце з $1 \neq 0$, R_0 – підкільце R , \tilde{R} – комутативне розширення кільця R .

Елемент \tilde{R} , який є коренем деякого многочлена позитивного степеня кільця $R_0[x]$, прийнято називати алгебраїчним над R_0 .

Многочлен мінімального позитивного степеня кільця $R_0[x]$, коренем якого є алгебраїчний над R_0 елемент, називають мінімальним многочленом цього елемента. Зрозуміло, що мінімальний многочлен визначається неоднозначно і є незвідним над R_0 , якщо R_0 – область цілісності.

Лема 17. *Мінімальний многочлен алгебраїчного над R_0 елемента \tilde{R} ділить добуток будь-якого многочлена $R_0[x]$, коренем якого є цей елемент, і відповідного степеня старшого коефіцієнта мінімального многочлена.*

Доведення. Нехай $\varepsilon \in \tilde{R}$ – алгебраїчний над R_0 елемент, $f(x)$ – мінімальний многочлен елемента ε , a – старший коефіцієнт $f(x)$, $g(x) \in R_0[x]$, $g(\varepsilon) = 0$. Ясно, що $a \in R_0$ і $a \neq 0$. За алгоритмом ділення многочленів $a^{\deg g(x)}g(x) = f(x)q(x) + r(x)$, де $q(x)$, $r(x)$ належать $R_0[x]$, $\deg r(x) < \deg f(x)$, $r(\varepsilon) = 0$, $\deg r(x) = 0$ і $r(x) = 0$.

Зрозуміло, що якщо R_0 – область цілісності, то старший коефіцієнт многочлена $q(x)$ дорівнює $a^{\deg g(x)-1}b$, де b – старший коефіцієнт многочлена $g(x)$.

Наслідок 14. *Нехай R_0 – факторіальне кільце і алгебраїчний над R_0 елемент є коренем деякого унітарного многочлена кільця $R_0[x]$. Тоді існує унітарний мінімальний многочлен даного алгебраїчного елемента, який ділить будь-який многочлен кільця $R_0[x]$, коренем якого є цей алгебраїчний елемент.*

Доведення. Нехай ε – алгебраїчний над R_0 елемент, $f(x)$ його мінімальний многочлен зі старшим коефіцієнтом a і $g(x)$ – многочлен кільця $R_0[x]$ такий, що $g(\varepsilon) = 0$. Якщо R_0 – факторіальне кільце, то за лемою Гауса, зміст (найбільший спільний дільник коефіцієнтів) добутоків многочленів, з точністю до оборотних елементів кільця R_0 , дорівнює добутку змістів заданих многочленів. Тому, з рівності $a^{\deg g(x)}g(x) = f(x)q(x)$ випливає, що $a^{\deg g(x)}d(g) = d(f)d(q)$, де $d(g), d(f), d(q)$ – змісти многочленів $g(x), f(x), q(x)$, які ділять їх старші коефіцієнти $b, a, a^{\deg g(x)-1}b$ відповідно.

Якщо $d(f)$ не співпадає з a або $d(q)$ не співпадає з $a^{\deg g(x)-1}b$, то $d(f)d(q)$ – дільник $a^{\deg g(x)}b$, який з ним не співпадає. Тому $d(g)$ – дільник b , який з ним не співпадає. При $b \in R^*$, тобто коли $g(x)$ – унітарний многочлен, це неможливо. В такому разі $d(f) = a$, $d(q) = a^{\deg g(x)-1}$,

$$a^{\deg g(x)}g(x) = f(x)q(x) = a^{\deg g(x)} \cdot \frac{f(x)}{d(f)} \cdot \frac{q(x)}{d(q)}, \quad g(x) = \frac{f(x)}{d(f)} \cdot \frac{q(x)}{d(q)}.$$

Зрозуміло, що унітарний многочлен $\frac{f(x)}{d(f)}$ – також мінімальний многочлен елемента ε , який ділить будь-який многочлен кільця $R_0[x]$ коренем якого є ε .

З наслідку 14 випливає, що серед мінімальних многочленів кореня n -го степеня із 1 кільця \tilde{R} над факторіальним кільцем R_0 існує унітарний мінімальний многочлен.

Нехай R_0 – підкільце R , яке породжене 1. Образи цілих чисел в R_0 при гомоморфізмі $Z \rightarrow R_0$ за правилом $1 \rightarrow 1$ будемо позначати так як і їх прообрази в Z .

Нехай p – просте натуральне число, $p \notin R^*$, J_p – максимальний ідеал кільця R , який містить pR . Очевидно, що $R_p = R/J_p$ – поле характеристики p .

Якщо p не ділить деяке натуральне число k в Z , то $1 = (p, k)$ і $k \notin J_p$. Зокрема, $(p-1)! \notin J_p$. В кільці Z , за малою теоремою Ферма, число $(z^{p-1} - 1)(p-1)! \in pZ$, для будь-якого цілого числа $z \in pZ$. Тому $z^{p-1} - 1 \in J_p$ і, як наслідок, $r^p - r \in J_p$ для всіх $r \in R_0$. Насправді під R_0 можна розуміти підкільце R , яке містить 1 і в якому для всіх простих натуральних чисел $p \in R^*$, виконується умова $r^p - r \in J_p$ для всіх $r \notin R_0$.

Лема 18. *Нехай R – область цілісності, R_0 – підкільце R , яке породжене 1, $\overline{Q(R)}$ – алгебраїчне замикання поля відношень $Q(R)$ кільця R , ε – первісний корінь k -го степеня із 1 поля $\overline{Q(R)}$, $f(x) \in R_0[x]$ – мінімальний многочлен ε , a – старший коефіцієнт $f(x)$, p – просте натуральне число, яке не ділить k , $p \notin R^*$, $pR + aR = R$. Тоді $f(x)$ – мінімальний многочлен елементів ε^{p^l} для всіх $l \geq 0$.*

Доведення. За умовою $pR \neq R$. Нехай I_p – максимальний ідеал R , який містить pR , але не містить елемент a . Очевидно, що I_p – максимальний ідеал R і $R_p = R/I_p$ – поле характеристики p , в якому $a \neq 0$ і $k \neq 0$.

За умовою $a^k(x^k - 1) = f(x)h(x)$, де $h(x) \in R_0[x]$. Припустимо, що $f(\varepsilon^p) \neq 0$. Тоді $h(\varepsilon^p) = 0$ і в полі $R_p(\varepsilon)$, яке утворене з поля R_p приєднанням ε , має місце рівність $h(\varepsilon)^p = h(\varepsilon^p) = 0$. Це означає, що ε є коренем многочленів $f(x)$ і $h(x)$ в полі $R_p(\varepsilon)$. Тому ε є двократним коренем двочлена $a^k(x^k - 1)$ і, як наслідок, є коренем одночлена $a^k k x^{k-1}$ в полі $R_p(\varepsilon)$, $a^k k \in I_p$. Отримане протиріччя показує, що $f(\varepsilon^p) = 0$.

Нехай $g(x) \in R_0[x]$ – мінімальний многочлен елемента ε^p і b – старший коефіцієнт $g(x)$. Якщо $f(x)$ не є мінімальним многочленом елемента ε^p , то $\deg g(x) < \deg f(x)$ і $b^{\deg f(x)} f(x) = g(x)q(x)$, де $q(x) \in R_0[x]$ і $\deg q(x) < \deg f(x)$. Оскільки $g(\varepsilon)q(\varepsilon) = 0$, то $g(\varepsilon) = 0$ або $q(\varepsilon) = 0$, що протирічить мінімальності многочлена $f(x)$ елемента ε .

Тим самим доведено, що $f(x)$ – мінімальний многочлен елемента ε^p , який також є первісним коренем k -го степеня із 1 поля $\overline{Q(R)}$. З аналогічних міркувань $f(x)$ – мінімальний многочлен елементів ε^{p^l} для всіх $l \geq 0$.

Теорема 5. *Нехай R – область цілісності, R_0 – підкільце R , яке породжене 1, натуральне число $k \neq 0$ в R , ε – первісний корінь k -го степеня із 1 поля $\overline{Q(R)}$, d – дільник k , $f_d(x)$ – мінімальний многочлен елемента $\varepsilon^{\frac{k}{d}}$, a_d – старший коефіцієнт $f_d(x)$. Якщо $p \notin R^*$ і $pR + a_d R = R$ для всіх простих дільників p цілих чисел $0 < s \leq d$, $(s, d) = 1$, то $\Phi_d(x)$ – мінімальний многочлен елемента $\varepsilon^{\frac{k}{d}}$ і $f_d(x) = a_d \Phi_d(x)$, $a_d \in R^*$.*

Доведення. Елемент $\varepsilon^{\frac{k}{d}}$ має порядок d . Як було доведено вище поліном ділення круга $\Phi_d(x)$ має вигляд

$$\Phi_d(x) = \prod_{0 < s \leq d, (s, d) = 1} (x - \varepsilon^{\frac{k}{d}s}) \in R_0[x].$$

За припущенням $p \notin R^*$ і $pR + a_d R = R$ для всіх простих дільників p цілих чисел $0 < s \leq d$, $(s, d) = 1$.

Згідно з лемою 18 $f_d(x)$ – мінімальний многочлен всіх елементів $\varepsilon^{\frac{k}{d}s}$, $0 < s \leq d$, $(s, d) = 1$. Тому $\Phi_d(x)$ ділить $f_d(x)$ в $\overline{Q(R)[x]}$ і, як наслідок, $\deg \Phi_d(x) \leq \deg f_d(x)$. Із мінімальності многочлена $f_d(x)$ елемента $\varepsilon^{\frac{k}{d}}$ випливає, що $\deg \Phi_d(x) = \deg f_d(x)$ і $\Phi_d(x)$ – мінімальний многочлен елемента $\varepsilon^{\frac{k}{d}}$. Тому $f_d(x) = a_d \Phi_d(x)$, $a_d \in R^*$, $\Phi_d(x)$ – незвідний многочлен кільця $R_0[x]$.

Нехай R_0 – факторіальне кільце і в $\overline{Q(R)}$ існує первісний корінь k -го степеня із 1. Тоді, як було показано в наслідку 14, мінімальні многочлени коренів k -го степеня із 1 кільця $R_0[x]$ можна вважати унітарними і для таких многочленів умова $pR + a_dR = R$ теореми 5 виконується автоматично. Тому, якщо $p \notin R^*$ для всіх простих дільників p цілих чисел $0 < s \leq d$, $(s, d) = 1$, $d | k$, то $\Phi_d(x)$ – незвідний многочлен кільця $R_0[x]$.

Наслідок 15. *Над кільцем цілих чисел поліноми ділення круга незвідні.*

Доведення. Нехай в теоремі 1, $R = R_0 = Z$, k – довільне натуральне число. Для будь-якого натурального числа $s > 1$ виконується умова $sZ \neq Z$. Оскільки Z – факторіальне кільце, то за теоремою 5 мінімальний многочлен кореня k -го степеня із 1 алгебраїчного замикання поля раціональних чисел, з точністю до знаку, співпадає з поліномом ділення круга $\Phi_k(x)$. Тому $\Phi_k(x)$ – незвідний многочлен над Z .

14. Застосування поліномів ділення круга до матриць скінченного порядку. Нехай R – комутативне кільце з $1 \neq 0$, V – R -модуль, $a \in \text{End}(V)$, $f(x) \in R[x]$, $f(a) = 0$. Якщо $f(x) = f_1(x) \cdot f_2(x)$, де $f_1(x), f_2(x) \in R[x]$ і $1 \in \langle f_1(x), f_2(x) \rangle_{R[x]}$, то $V = V_1 \oplus V_2$, де $V_i = \{v \in V \mid f_i(a)v = 0\}$, $1 \leq i \leq n$.

Адже, $V = f_1(a)V + f_2(a)V$ і $f_1(a)V \subset V_2$, $f_2(a)V \subset V_1$, $V_1 \cap V_2 = 0$.

Зокрема, якщо

$$f_1(x) = x - \varepsilon, f_2(\varepsilon) \in R^*, \text{ то } 1 \in \langle x - \varepsilon, f_2(x) \rangle_{R[x]}, V = V_1 \oplus V_2,$$

де $V_1 = \{v \in V \mid av = \varepsilon v\}$ і $V_2 = \{v \in V \mid f_2(a)v = 0\}$.

Ендоморфізм $a \in \text{End}(V)$ або $R[a]$ -модуль V називається нерозкладним, якщо V не є прямою сумою ненульових інваріантних відносно a R -підмодулів модуля V .

Лема 19. *Нехай R – комутативне кільце з $1 \neq 0$, $n \in R^*$, ε – породжує корені n -го степеня із 1 кільця R , k – порядок ε , $\varepsilon^i - 1 \in R^*$ для всіх $1 \leq i < k$, V – вільний R -модуль скінченного рангу t , прямі доданки якого є вільними R -підмодулями V , елемент $a \in GL(t, V) \cong GL(t, R)$ є коренем двочлена $x^n - 1$, $n \in R^*$. Тоді, з точністю до спряження, a є діагональною матрицею з степенями ε на діагоналі і нерозкладними матрицями, які є коренями поліномів ділення круга $\Phi_d(x^k)$, де d – дільник числа $\frac{n}{k}$.*

Доведення. Без обмеження загальності можна вважати, що a – нерозкладна матриця. За умовою k – дільник n і

$$x^k - 1 = \prod_{1 \leq i < k} (x - \varepsilon^i), f_{\frac{n}{k}}(\varepsilon^{ik}) = f_{\frac{n}{k}}(1) = \frac{n}{k} \in R^*.$$

З рівності

$$x^n - 1 = (x^k - 1) f_{\frac{n}{k}}(x^k) = \prod_{1 \leq i < k} (x - \varepsilon^i) f_{\frac{n}{k}}(x^k)$$

і включень

$$1 \in \langle x - \varepsilon^i, x - \varepsilon^j \rangle_{R[x]}, 1 \leq i \neq j \leq k, 1 \in \langle x - \varepsilon^i, f_{\frac{n}{k}}(x^k) \rangle_{R[x]}$$

випливає що $a | V = \varepsilon^i$, $1 \leq i \leq k$ або $f_{\frac{n}{k}}(a^k) V = 0$. Тому достатньо розглянути випадок, коли $f_{\frac{n}{k}}(a^k) = 0$. З аналогічних міркувань можна вважати, що існує d , $1 \leq d \leq n$ таке, що a, \dots, a^{d-1} – корені многочлена $f_{\frac{n}{k}}(x^k)$, а a^d – скалярна матриця з степенем ε на діагоналі.

Легко бачити, що $Z = \bigcup_{1 \leq i \leq d, t \in Z} \{i + dt\}$. Тому елементи a^{i+dt} , де $1 \leq i \leq d$, $t \in Z$ вичерпують всі степені a . Із рівності $(a^{dt})^k = (a^d)^{kt} = 1$ для будь-яких $t \in Z$ випливає, що a^{i+dt} при $1 \leq i < d$ є коренями многочлена $f_{\frac{n}{k}}(x^k)$ і є скалярними матрицями при $i = d$. Тому серед степенів елемента a скалярними є тільки ті, показники яких діляться на d , а решта є коренями многочлена $f_{\frac{n}{k}}(x^k)$. Оскільки $a^{\frac{n}{k}}$ не є коренем многочлена $f_{\frac{n}{k}}(x^k)$, то $a^{\frac{n}{k}}$ – скалярна матриця і, як наслідок, d ділить $\frac{n}{k}$, $d \in R^*$.

З леми 7 випливає рівність $f_{\frac{n}{k}}(x) = f_d(x) f_{\frac{n}{dk}}(x^d)$. Оскільки

$$f_{\frac{n}{k}}(a^{ik}) = 0 \text{ і } f_{\frac{n}{dk}}(a^{ikd}) = \frac{n}{dk} \in R^*,$$

то $f_d(a^{ik}) = 0$ для всіх $1 \leq i < d$. За теоремою 2 a^k – корінь многочлена $\Phi_d(x)$. Тому a – корінь многочлена $\Phi_d(x^k)$, де d ділить $\frac{n}{k}$.

Зауваження. Лема 19 також випливає з формули

$$x^n - 1 = (x^k)^{\frac{n}{k}} - 1 = \prod_{d | \frac{n}{k}} \Phi_d(x^k)$$

і включень $1 \in \langle \Phi_{d_1}(x), \Phi_{d_2}(x) \rangle_{R[x]}$, де d_1, d_2 – різні дільники натурального числа $\frac{n}{k}$, $n \in R^*$.

1. Винберг Э. Б. Курс алгебры. – 2-е изд. испр. и доп. – М.: Факториал Пресс., 2001. – 544 с.
2. Гудивок П. М. Представления конечных групп над коммутативными локальными кольцами. – Ужгород: Ужгородский национальный университет, 2003. – 119 с.
3. Гудивок П. М., Рудько В. П., Бовді А. А. Кристаллографічні групи. – Ужгород: Ужгородський національний університет, 2006. – 173 с.
4. Дроботенко В. С., Рудько В. П. Елементи теорії кілець. – Ужгород: Ужгородський національний університет, 2004. – 128 с.
5. Дрозд Ю. А., Кириченко В. В. Конечномерные алгебры. – Киев: Вища школа, 1980. – 192 с.
6. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. – 3-е изд. перераб. и доп. – М.: Наука, 1982. – 288 с.
7. Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр. – М.: Наука, 1969. – 688 с.
8. Петечук В. М. Стабільність колець // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2009. – Вип. 19. – С. 87–111.

Одержано 11.10.2013