УДК 512.547.25

Ю. В. Петечук (Ужгородський національний університет)

ТЕОРІЯ МАТРИЦЬ СКІНЧЕННОГО ПОРЯДКУ НАД КОМУТАТИВНИМИ КІЛЬЦЯМИ

The concept of complete work of polynomials with elements in commutative rings is introduced in this article. It is well-proven that if R is a commutative ring from $1 \neq 0$, $n = p_1^{n_1} ... p_k^{n_k} > 1$, so $x^n - 1$, is a complete work of polynomials of division of circle $\Phi_d(x)$, $d|n$ with an element $n^{(1+n_1)\dots(1+n_k)}$. It is shown that if V- is left R-modul, $a \in EndV$, $p(x)$ is a complete work of degrees of polynomials $p_1(x), ..., p_t(x)$ of ring R[x] with an element $p \in R$, such, that $pV = V$, $Ann_V p = 0$, $p(a) = 0$, there is a decomposition $V = V_1 \oplus ... \oplus V_t$, where $aV_i \subset V_i$, $A_i = a|V_i, a = diag\ (A_1, \dots, A_t)$ and $p_i(A_i)$, are nilpotent elements for all $1 \leq i \leq t$. In particular, if V– is the module of complete grade, projective modules over R are free, $p(x) = x^n - 1$, $p \in R^*$so the degrees of matrix A_i- are roots of some degrees of polynomials $p_1(x), ..., p_t(x)$.

В роботі вводиться поняття повного добутку многочленів з елементами в комутативних кільцях. Доведено, що якщо R - комутативне кільце з $1 \neq 0$, $n = p_1^{n_1} ... p_k^{n_k} > 1$, то $x^n - 1$ є повним добутком поліномів ділення круга $\Phi_d(x)$, $d|n$ з елементом $n^{(1+n_1)\dots(1+n_k)}$. Показано, що якщо V - лівий R -модуль, $a \in EndV$, $p(x)$ - повний добуток степенів многочленів $p_1(x), ..., p_t(x)$ кільця R[x] з елементом $p \in R$, таким, що $pV = V$, $Ann_V p = 0$, $p(a) = 0$, то існує розклад $V = V_1 \oplus ... \oplus V_t$, де $aV_i \subset V_i$, $A_i = a|V_i$, $a = diag(A_1, ..., A_t)$ і $p_i(A_i)$ - нільпотентні елементи для всіх $1 \leq i \leq t$. Якщо V - модуль скінченного рангу, проективні модулі над R вільні, $p(x) = x^n - 1$, $p \in R^*$, то степені матриць A_i - корені деяких степенів многочленів $p_1(x), ..., p_t(x)$.

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

1. Передмова. У даній статті розглядаються елементи теорії комутативних кілець, кілець многочленів та зображень скінчених груп, які є необхідними для доведення основних результатів та мають самостійну цінність. Окремі з них є новими або узагальненням відомих результатів.

В роботі вводиться поняття повного добутку многочленів з елементами в комутативних кільцях. Більш точно, многочлен $p(x)$ кільця R[x] над комутативним кільцем R з $1 \neq 0$ називається повним добутком многочленів $p_1(x), ..., p_t(x)$, $t \geq 1$ кільця R[x] з елементом $p \in R$, якщо $p(x) = p_1(x)...p_t(x)$ і при $t > 1$ $p \in \langle p_i(x), p_j(x) \rangle_{R[x]}$ для всіх $1 \leq i \neq j \leq t$.

Якщо $p \in R^*$, то $p(x)$ називається повним добутком многочленів $p_1(x), ..., p_t(x)$.

Доведено, що якщо R - комутативне кільце з $1 \neq 0$, $n = p_1^{n_1} ... p_k^{n_k} > 1$, то $x^n - 1$ є повним добутком поліномів ділення круга $\Phi_d(x)$, $d|n$ з елементом $p = n^{(1+n_1)\dots(1+n_k)}$. Більше того, якщо поліноми ділення круга $\Phi_d(x)$, $d|n$ є повними добутками многочленів $p_{dl}(x)$ з елементом $p_d \in R$, то $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$ з елементом $p \prod\limits_{d|n} p_d$.

Зокрема, якщо $\Phi_d(x)$, $d|n$ є повним добутком многочленів $p_{dl}(x)$, то $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$ з елементом p, множина простих дільників якого співпадає з множиною простих дільників числа n.

Многочлени, які є повними добутками многочленів з елементами кілець при деяких обмеженнях, породжують розклади модулів над цими кільцями.

В роботі показано, що якщо R - комутативне кільце з $1 \neq 0$, V - лівий R-модуль, $a \in EndV$, $p(x)$ - повний добуток степенів многочленів $p_1(x), ..., p_t(x)$

кільця R[x] з елементом $p \in R$, таким, що $pV = V$, $Ann_V p = 0$, $p(a) = 0$, то існує розклад $V = V_1 \oplus ... \oplus V_t$, де $aV_i \subset V_i$, $A_i = a\,|V_i$, $a = diag(A_1, ..., A_t)$ і $p_i(A_i)$ - нільпотентні елементи для всіх $1 \leq i \leq t$. Якщо $b \in EndV$ і $ab = ba$, то $bV_i = V_i$.

Зокрема, якщо V є R -модулем скінченного рангу m над комутативним кільцем R, проективні модулі над яким вільні, $p \in R^*$, $a \in GL(m, R) \equiv GL(m, V)$, $p(x) = x^n - 1$, то, з точністю до спряження, a - діагональний елемент з матрицями на діагоналі, степені кожної з яких є коренями деякого степеня одного із множників повного добутку двочлена $x^n - 1$ (не обов'язково одного і того ж самого).

Спираючись на класичні теореми Гільберта про базис і лему Круля доведено, що матриці n -го порядку групи $\ker \Lambda_{J(R)}$ є одиничними, якщо $J(R)$ - радикал Джекобсона комутативного кільця R, який містить натуральні числа, що є взаємно-простими з n, $\Lambda_{J(R)} : R_m \to (R/J(R))_m$, $m \geq 1$.

Зокрема, якщо R - комутативне локальне кільце, характеристика поля $R/J(R)$ якого відмінна від нуля і не ділить n, то група $\ker \Lambda_{J(R)}$ містить тільки одиничні елементи порядку n.

Отримані результати застосовуються при знаходженні канонічного вигляду матриць скінченного порядку над комутативними локальними кільцями, в яких ці порядки є оборотними елементами. Вони лежать в основі описання зображень деяких зверхрозв'язних груп над комутативними локальними кільцями.

В роботі показано, що даний підхід цілком придатний при описанні незвідних зображень та знаходженні канонічного вигляду матриць скінченного порядку над довільними кільцями головних ідеалів.

Основні результати роботи сформульовані в теоремах 1-4.

Більш детальну інформацію про класичні результати можна знайти в [1-8].

2. Розклад елементів у комутативних кільцях. Нехай R - комутативне кільце з $1 \neq 0$ на якому задана операція множення на елементи множини X. Суму $\sum\limits_{\text{i}} x_i a_i = x_1 a_1 + \ldots + x_n a_n$, де $x_i \in X$, $1 \leq \text{i} \leq \text{n}$ будемо називати лінійною комбінацією елементів $a_1, \ldots, a_n$ кільця R над X, а елементи $x_1, \ldots, x_n$ її коефіцієнтами. Множину всіх лінійних комбінацій елементів $a_1, \ldots, a_n$ кільця R над X будемо позначати $< a_1, \ldots, a_n >_X$. Зрозуміло, що $< a_1, \ldots, a_n >_R = a_1 R + \ldots + a_n R$ - ідеал кільця R, який породжений елементами $a_1, \ldots, a_n$. Ідеали кільця R, які породжуються скінченим числом елементів кільця R, будемо називати скінченнопородженими.

Очевидно, що для довільних елементів $a_1, \ldots, a_{n+1}$ кільця R мають місце включення $< a_1, \ldots, a_n >_R \subset < a_1, \ldots, a_{n+1} >_R$, $< r_1 a_1, \ldots, r_n a_n >_R \subset < a_1, \ldots, a_n >_R$, де $r_i \in R$, $1 \leq i \leq n$.

Лема 1. *Нехай R - комутативне кільце, p, $a_1, \ldots, a_n$ - елементи R, $n \geq 2$, $b_i = a_1 \ldots a_{i-1} a_{i+1} \ldots a_n$, $p^k \in < a_i, b_i >_R$ для всіх $1 \leq i \leq n$. Тоді $p^{k+(n-2)(k+1)} \in < b_1, \ldots, b_n >_R$.*

Якщо $a_1 \ldots a_n = 0$, то $p^k B_i = 0$ для всіх $1 \leq i \leq n$, де $B_i = < b_i >_R \bigcap < b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n >_R$.

Доведення. проведемо індукцією за числом n. При $n = 2$ лема 1 очевидна. Нехай $n > 2$, $b'_i = a_1 \ldots a_{i-1} a_{i+1} \ldots a_{n-1}$, $1 \leq i \leq n-1$. Очевидно, що $b_i = b'_i a_n$ і $p^k \in < a_i, b_i >_R \subset < a_i, b'_i >_R$, $1 \leq i \leq n-1$. За припущенням індук-

кції $p^{k+(n-3)(k+1)} \in < b'_1, \dots b'_{n-1} >_R$. Тому $p^{(n-2)(k+1)}a_n = p \cdot p^{k+(n-3)(k+1)}a_n \subset < b_1, \dots, b_{n-1} >_R$. В такому разі

$p^{k+(n-2)(k+1)} \in p^{(n-2)(k+1)} \cdot p^k \in p^{(n-2)(k+1)} < a_n, b_n >_R \subset < b_1, \dots, b_n >_R$.

Якщо $a_1 \dots a_n = 0$, то $a_i b_i = 0$ і, як наслідок, $b_i b_j = 0$ для всіх $1 \le i \ne j \le n$. Тоді $a_i B_i = 0$, $b_i B_i = 0$ і, як наслідок, $p^k B_i = 0$ для всіх $1 \le i \le n$.

Неважко бачити, що із включення $p_i \in < a, a_i >_{\mathrm{R}}$, $1 \le i \le n$ елементів $p_1, \dots, p_n, a, a_1, \dots, a_n$ комутативного кільця R випливає, що $r_i a_i \in p_i + < a >_R$, $r_i \in R$. Тому $r_1 \dots r_n a_1 \dots a_n \in p_1 \dots p_n + < a >_R$, $p_1 \dots p_n \in < a, a_1 \cdots a_n >_R$.

Зокрема, якщо $p \in < a_i, a_j >$, $1 \le i \ne j \le n$, то $p^{n-1} \in < a_i, a_1 \cdots a_{i-1}a_{i+1} \cdots a_n >_R$.

Наслідок 1. *Нехай R - комутативне кільце, p_{ij}, $1 \le i \ne j \le n$, a_i, $1 \le i \le n$ - елементи R, $n \ge 2$, $b_i = a_1 \dots a_{i-1}a_{i+1} \dots a_n$, такі що $p_{ij} \in < a_i, a_j >_R$, $p = \prod\limits_{i,j} p_{ij}$. Тоді $p^{2n-3} \in < b_1, \dots, b_n >_R$ і для будь-яких елементів $r_1, \dots, r_n$ кільця R існує $r \in R$, такий що $r - pr_i \in < a_i >_R$ для всіх $1 \le i \le n$.*

Якщо $a_1 \dots a_n = 0$, то $pB_i = 0$, де $B_i = < b_i >_R \bigcap < b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n >_R$.

Доведення. Зафіксуємо $1 \le i \le n$. Із $p_{ij} \in < a_i, a_j >_{\mathrm{R}}$, згідно з вищесказаним, випливає, що $p_i = \prod\limits_j p_{ij} \in < a_i, a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_n >_R = < a_i, b_i >_R$. Тому елемент $p = p_1 \dots p_n \in < a_i, b_i >_R$ для всіх $1 \le i \le n$. Згідно з лемою 1, в якій $\mathrm{k} = 1$, $p^{2n-3} \in < b_1, \dots, b_n >_R$.

Нехай $\beta_1, \dots, \beta_n$ - елементи кільця R, такі, що $p - \beta_i b_i \in < a_i >_R$, $r = r_1\beta_1 b_1 + \dots + r_n\beta_n b_n$. Тоді $r - pr_i \in < a_i >_R$. Адже, $b_j \in < a_i >_R$ при $i \ne j$ і $r_i\beta_i b_i - pr_i = r_i(\beta_i b_i - p) \in < a_i >_R$.

Якщо $a_1 \dots a_n = 0$, то, згідно з лемою 1, $p_i B_i = 0$ і, як наслідок, $pB_i = 0$ для всіх $1 \le i \le n$.

Наслідок 2. *Нехай R - комутативне кільце з $1 \ne 0$, $1 \in < a_i, a_j >_R$ для всіх $1 \le i \ne j \le n$, $b_i = a_1 \dots a_{i-1}a_{i+1} \dots a_n$. Тоді $R = Rb_i + \dots + Rb_n$ і для будь-яких елементів $r_1, \dots, r_n$ кільця R існує $r \in R$, такий, що $r - r_i \in < a_i >_R$, $1 \le i \le n$ (китайська теорема про остачі в комутативних кільцях).*

Якщо $a_1 \dots a_n = 0$, то $R = Rb_1 \oplus \dots \oplus Rb_n$.

Доведення. випливає із наслідку 1, якщо $p \in R^*$. Адже, тоді можна вважати, що $p = 1$.

Лема 2. *Нехай натуральні числа $1 \le i \ne j \le n$ пробігають множину дільників числа $n = p_1^{n_1} \dots p_k^{n_k} > 1$, а p_{ij} визначаються за правилом: p_{ij} - просте число, якщо відношення i та j або j та i є його степенем і $p_{ij} = 1$ в решті випадків, $p = \prod\limits_{i,j} p_{ij}$. Тоді $p = n^{(n_1+1)\dots(n_k+1)}$.*

Доведення. Обчислимо степінь кожного простого числа p_i з яким це число входить в p. Нехай d - фіксований довільний дільник числа $\frac{n}{p_i^{n_i}}$. Від кожної пари різних чисел dp_i^t та dp_i^s елемент p_i входить в p один раз. Оскільки таких пар $n_i(n_i + 1)$, а число дільників числа $\frac{n}{p_i^{n_i}}$ дорівнює $(n_1 + 1) \dots (n_{i-1} + 1)(n_{i+1} + 1) \dots (n_k + 1)$, то p_i входить в p з показником степеня $n_i(n_1 + 1) \dots (n_k + 1)$. Тому $p = (p_1^{n_1} \dots p_k^{n_k})^{(n_1+1)\dots(n_k+1)} = n^{(n_1+1)\dots(n_k+1)}$.

Лема 3. *Нехай R - комутативне кільце з $1 \neq 0$, V - довільний R - модуль, n і m - натуральні числа, множини простих дільників яких співпадають або $n = m = 1$. Тоді $nV = V$ або $Ann_V n = 0$ тоді і тільки тоді, коли $mV = V$ або $Ann_V m = 0$ відповідно.*

Доведення. При $n = m = 1$ твердження леми 3 очевидне.

Нехай $n = p_1^{n_1} \dots p_k^{n_k} > 1$, $m = p_1^{m_1} \dots p_k^{m_k} > 1$. Очевидно, що $nV \subset p_i V$ і $Ann_V p_i \subset Ann_V n$ для всіх $1 \leq i \leq k$. Якщо $nV = V$, то $p_i V = V$ для всіх $1 \leq i \leq k$ і $mV = V$. Аналогічно, якщо $Ann_V n = 0$, то $Ann_V p_i = 0$ для всіх $1 \leq i \leq k$ і $Ann_V m = 0$. Навпаки аналогічно.

Зауважимо, що умова $rV = V$, $r \in R$ у випадку коли V -вільний R -модуль рівносильна включенню $r \in R^*$.

3. Окремі властивості комутативних кілець. Будемо казати, що елемент a кільця R є дільником елемента b кільця R, або по-другому a ділить b, або ще по-другому, b ділиться на a, якщо b є добутком елемента a на деякий елемент кільця R, який будемо позначати $\frac{b}{a}$. Запис $\frac{b}{a}$ прийнято вживати виключно при $a \neq 0$.

Найбільшим спільним дільником елементів a і b кільця R будемо називати спільний дільник, який ділиться на будь-який інший їх спільний дільник і будемо його позначати (a, b). При цьому вважаємо, що найбільший спільний дільник існує, якщо про нього йде мова. Очевидно, що $(a, b) \neq 0$, якщо $a \neq 0$ або $b \neq 0$.

Неважко бачити, що a ділить b тоді і тільки тоді, коли a є найбільшим спільним дільником елементів a і b. Оскільки $0 = \mathrm{a} \cdot 0$, то будь-який елемент a кільця R ділить нульовий елемент і $(0, a) = a$.

Дільники одиниці називаються оборотними елементами кільця R. Вони утворюють групу оборотних елементів кільця R, яку позначають R^*. Елементи R, які не є оборотними, називаються необоротними елементами кільця R. Необоротні елементи, які не можна розкласти в добуток хоча б двох необоротних елементів кільця R прийнято називати простими елементами кільця. Очевидно, що нульовий елемент є необоротним, але не є простим елементом кільця.

Елемент кільця, добуток якого з деяким ненульовим елементом кільця дорівнює нулю, називається дільником нуля.

Комутативне кільце з $1 \neq 0$, в якому не має відмінних від нуля дільників нуля, прийнято називати областю цілісності.

В області цілісності рівності можна скорочувати на ненульові елементи. Тому елемент $\frac{b}{a}$ визначається однозначно. Очевидно, що $\frac{0}{a} = 0$.

Неважко бачити, що якщо в області цілісності R елемент a ділить b, а елемент b ділить a, то b є добутком елемента a на деякий оборотний елемент кільця R. В такому разі будемо казати, що елементи a і b співпадають з точністю до оборотних елементів кільця R і будемо записувати $a = b$. Зрозуміло, що в області цілісності найбільший спільний дільник елементів визначається, з точністю до оборотних елементів, однозначно.

Для будь-яких елементів a, b, c області цілісності R елемент $c(a, b)$ ділить (ca, cb) і $((a, b), c) = (a, (b, c))$. Остання рівність дозволяє розширити поняття найбільшого спільного дільника на будь-яку скінченну кількість елементів $a_1, \dots, a_n$, $n > 2$ області цілісності R за правилом $(a_1, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$. Очевидно, що $c(a_1, \dots, a_n)$ ділить $(ca_1, \dots, ca_n)$ і, як наслідок, $(\frac{a_1}{b}, \dots, \frac{a_n}{b})$ ділить $\frac{(a_1, \dots, a_n)}{b}$, якщо b ділить елементи $a_1, \dots, a_n$.

Елементи $a_1, \ldots, a_n$, $n \geq 1$ області цілісності R називаються взаємно простими, якщо $(a_1, \ldots, a_n) = 1$.

Неважко бачити, що якщо елементи $a_1, \ldots, a_n$ є взаємно-простими в області цілісності R, то елементи $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ також є взаємно-простими в R.

Область цілісності R з однозначним, з точністю до оборотних елементів кільця R, розкладом на прості множники ненульових необоротних елементів R називається факторіальним кільцем. Нехай p - простий елемент факторіального кільця R. Якщо деяка степінь $p^i, i \geq 1$ ділить добуток $ab \neq 0$ елементів a і b, то a і b - ненульові необоротні елементи R і із однозначності їх розкладу на прості множники випливає, що p^i ділить елемент $a(a, b)$ або $(a, b)b$.

Зокрема, якщо p ділить $ab \neq 0$, то p ділить a або b. Це означає, що прості елементи факторіального кільця породжують прості ідеали (ідеали, фактор-кільця по яких є областями цілісності).

Із сказаного вище випливає, що якщо деякий необоротний елемент d ділить добуток $ab \neq 0$, то d - ненульовий елемент, який ділить елемент $(d, a)b$ і, як наслідок, $\frac{d}{(d,a)}$ ділить b. Це доводить, що якщо d ділить ненульові добутки ac і bc, то $\frac{d}{(d,c)}$ ділить (a, b) і, як наслідок, d ділить $(a, b)c$. Тому (ca, cb) ділить $c(a, b)$. Ця властивість залишається вірною, якщо хоча б один із елементів ca або cb дорівнює 0.

Тим самим доведено, що у факторіальному кільці R $(ca, cb) = c(a, b)$, $(ca_1, \ldots, ca_n) = c(a_1, \ldots a_n)$, $\left(\frac{a_1}{b}, \ldots, \frac{a_n}{b}\right) = \frac{(a_1, \ldots, a_n)}{b}$, де b ділить $a_1, \ldots a_n$.

Комутативне кільце R з $1 \neq 0$ називається ньотеровим, якщо будь-який зростаючий ланцюг ідеалів кільця R стабілізується.

Очевидно, що якщо в комутативному кільці R з $1 \neq 0$ кожний ідеал є скінченнопородженим, то об'єднання ідеалів будь-якого зростаючого ланцюга ідеалів є скінченно породженим, а тому належить, починаючи з деякого номера, всім ідеалам ланцюга. Це означає, що комутативні кільця, кожний ідеал яких є скінченно породженим, є ньотеровими. Навпаки очевидно.

Виявляється, що в області цілісності R, яка є ньотеровим кільцем, будь-який ненульовий необоротний елемент розкладається в добуток простих елементів. Адже, якщо A - не порожня множина ненульових необоротних елементів R, які не можна розкласти в добуток простих елементів R і $a_0 \in A$, то a_0 - не простий елемент R і $a_0 = a_1 b_1$, де a_1, b_1 - необоротні елементи R. В такому разі $a_1 \in A$ або $b_1 \in A$. Нехай $a_1 \in A$. Тоді $a_1 = a_2 b_2$, де a_2, b_2 - необоротні елементи R, хоча б один з яких належить A. Продовжуючи цей процес отримуємо нескінченну строго зростаючу послідовність ідеалів $a_0 R \subset a_1 R \subset a_2 R \ldots$, що протирічить ньотеровості кільця R. Тому A - порожня множина.

Область цілісності називається кільцем головних ідеалів, якщо кожний її ідеал є головним, тобто породжується одним елементом.

Як було показано вище кільце головних ідеалів є ньотеровим кільцем, в якому має місце розклад ненульових необоротних елементів на прості множники.

Неважко бачити, що в кільці головних ідеалів R для будь-яких елементів a і b існує елемент $d \in R$, такий що $dR = aR + bR$ і $(a, b) = d = ax + by$ для деяких елементів x, y кільця R.

Нехай p - простий елемент кільця головних ідеалів R, який ділить добуток ab. Оскільки (p, a) ділить p, то $(p, a) = p$ або $(p, a) = 1$. У першому випадку

p ділить a, а у другому випадку $1 = px + ay$ і $b = pbx + aby$ ділиться на p. Це означає, що в кільці головних ідеалів простий елемент, який ділить добуток елементів ділить один із них. Тому, якщо два добутки простих елементів виявляються рівними, то множини простих дільників у них співпадають і, як показує поступове скорочення, входять в добутки з однаковими показниками степенів.

Із сказаного випливає, що кільця головних ідеалів є факторіальними. Неважко бачити, що якщо R - область цілісності, в якій елемент d є дільником елементів $a_1, \ldots, a_n$ і $d \in < a_1, \ldots, a_n >_R$, то $d = (a_1, \ldots, a_n)$. Якщо R - кільце головних ідеалів, то вірно і навпаки. Адже, якщо $d = (a_1, \ldots, a_n)$ і $d'R =< a_1, \ldots, a_n >_R$, то d ділить d', а d' ділить d і, як наслідок $d = d' \in < a_1, \ldots, a_n >_R$.

Зокрема, якщо R - область цілісності і $1 \in < a_1, \ldots, a_n >_R$, то $a_1, \ldots, a_n$-взаємно-прості елементи R. Якщо R – кільце головних ідеалів, то вірно і навпаки.

До цих пір відношення $\frac{b}{a}$ розглядались в області цілісності R. Якщо допустити, щоб формальні відношення $\frac{b}{a}$ елементів a і b цілісного кільця R утворювали множину $Q(R)$ деякого розширення кільця R, то $Q(R)$ перетворюється в поле, якщо в ньому задати операції додавання і множення за правилами $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Поле $Q(R)$ називається полем відношень області цілісності R. Воно містить R, якщо вважати, що елементи $r \in R$ ототожнюється з елементами $\frac{r}{1} \in Q(R)$. При цьому ототожненні ненульові елементи R є оборотними в $Q(R)$.

4. Многочлени над асоціативними кільцями. Нехай R - асоціативне кільце з $1 \neq 0$. Елементи, які комутують з усіма елементами R утворюють підкільце з 1, яке називають центром кільця R і позначають ζR. Елемент кільця R, добуток якого з деяким ненульовим елементом кільця R дорівнює нулю називається дільником нуля кільця R. Елемент $r \in R$, для якого існує елемент $r_1 \in R$ такий, що $rr_1 = r_1 r = 1$ називається оборотним елементом кільця R. Оборотні елементи R утворюють групу оборотних елементів, яку позначають R^*.

Нехай x - змінна, яка комутує з усіма елементами кільця R, $R[x]$ - кільце многочленів змінної x над R. Підкреслимо, що під $R[x]$ будемо розуміти множину однозначно визначених скінченних сум $\sum\limits_i \alpha_i x^i$, $\alpha_i \in R$, $i \geq 0$, які будемо називати многочленами, із заданими на них операціями додавання і множення $\sum\limits_i \alpha_i x^i + \sum\limits_i \alpha'_i x^i = \sum\limits_i (\alpha_i + \alpha'_i) x^i$, $\left(\sum\limits_i \alpha_i x^i\right)\left(\sum\limits_j \alpha_j x^j\right) = \sum\limits_{i,j} \alpha_i \alpha_j x^{i+j} = \sum\limits_t \left(\sum\limits_i \alpha_i \alpha_{t-i}\right) x^t$.

Найбільше ціле число $i_0 \geq 0$ для якого $\alpha_{i_0} \neq 0$ в многочлені $f(x) = \sum\limits_i \alpha_i x^i$ називають степенем многочлена $f(x)$ і позначають $\deg f(x)$, а α_{i_0} називають старшим коефіцієнтом многочлена $f(x)$. Елементи α_i, $0 \leq i \leq i_0$ називають коефіцієнтами многочлена $f(x)$.

Неважко бачити, що степінь добутку многочленів не перевищує суму їх степенів. При цьому рівність для всіх многочленів кільця $R[x]$ досягається тільки в кільцях без відмінних від нуля дільників нуля. Зокрема, $R[x]$ - область цілі-

сності, якщо R - область цілісності.

Рівність, в якій вираз, побудований із многочленів кільця $R[x]$ за допомогою операцій додавання і множення, тотожньо дорівнює нулю, називають формулою кільця $R[x]$.

Нехай $\varphi: R \to R'$ - кільцевий гомоморфізм асоціативного кільця R в асоціативне кільце R', r' - довільний елемент кільця R', який комутує з усіма елементами підкільця $\varphi(R)$ кільця R', $f(x) = \sum\limits_i \alpha_i x^i$ - многочлен кільця $R[x]$. Домовимося під $f\varphi(x)$ розуміти многочлен $\sum\limits_i \varphi(\alpha_i)x^i$ кільця $R'[x]$. Відображення $x \to f(x)$, $f(x) \to f(\varphi(x)) \to f(\varphi(r'))$ індукують кільцеві гомоморфізми $R[x] \to R[x]$, $R[x] \to R'[x] \to R'$ відповідно. Тому формули кільця $R[x]$ перетворюються у формули кільця $R[x]$ або у співвідношення кільця R', якщо в них замінити x на $f(x)$ або x на r' відповідно.

Зокрема, якщо $1 \in < p_1(x), \ldots, p_t(x) >_{R[x]}$, то $1 \in < p_1(x^k), \ldots, p_t(x^k) >_{R[x]}$ при $t \geq 1$, $k \geq 1$.

Якщо $R \subseteq R'$, то, згідно з алгоритмом ділення многочленів з остачею і застосуванням вищевказаного кільцевого гомоморфізма, $f(x) = (x - r')q(x) + f(r')$, де r' - довільний елемент центра ζR кільця R', а $f(x)$ - довільний многочлен кільця $R[x]$.

Тому многочлен $f(x)$ кільця $R[x]$ ділиться на двочлен $x - r$, де r - елемент центра кільця R тоді і тільки тоді, коли $f(r) = 0$ (теорема Безу).

Якщо R - комутативне кільце з $1 \neq 0$ і $R' = R_n$ - кільце всіх $n \times n$ матриць над R, $n \geq 1$, $\zeta R'$ - його центр, то $R \subset \zeta R'$ і в якості елемента r' можна вибрати будь-яку матрицю кільця $R_n = Hom_R(V, V)$, де V - вільний лівий R -модуль рангу n над R.

Многочлени кільця $R[x]$ будемо називати унітарними, якщо їх старші коефіцієнти є оборотними елементами кільця R. Многочлени кільця $R[x]$, у яких старші коефіцієнти дорівнюють 1, будемо називати строго унітарними або нормалізованими.

Неважко бачити, що унітарні многочлени не є дільниками нуля кільця $R[x]$ і можуть бути добутком тільки унітарних многочленів. Окрім цього будь-який многочлен у кільці $R[x]$ за алгоритмом послідовного ділення можна ділити на унітарні многочлени з остачею.

Многочлени позитивного степеня кільця $R[x]$ називаються незвідними, якщо їх не можна розкласти в добуток двох многочленів позитивного степеня кільця $R[x]$.

Неважко бачити, що будь-який многочлен позитивного степеня кільця $R[x]$ над асоціативним кільцем R є добутком степенів незвідних многочленів $R[x]$. Підкреслимо, що незвідний многочлен будемо вважати також добутком незвідних многочленів, який складається з одного множника.

Із сказаного вище випливає, що будь-який унітарний многочлен позитивного степеня кільця $R[x]$, з точністю до оборотних елементів кільця R, можна розкласти в добуток незвідних унітарних многочленів.

Зрозуміло, що кільцевий гомоморфізм кільця R відображає унітарні многочлени в унітарні. Тому розклад унітарного многочлена в добуток унітарних многочленів кільцевим гомоморфізмом перетворюється у відповідний розклад їх образів. При цьому кратність входження в розклад деякого унітарного мно-

гочлена зберігається.

Відмітимо, що якщо R - комутативне кільце з $1 \neq 0$, $n \notin J(R)$, де $J(R)$ - радикал Джекобсона кільця R , то двочлен $x^n - 1$, $n \geq 1$ може розкладатися в добуток многочленів позитивного степеня лише без кратностей. Адже, якщо $n \notin J(R)$, то існує максимальний ідеал I кільця R, такий що $n \notin I$ і над полем R/I двочлен $x^n - 1$ є взаємно-простим з одночленом nx^{n-1}, а тому може розкладатися в добуток многочленів позитивного степеня лише без кратностей.

5. Розклад многочленів над комутативними кільцями. 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. Очевидно, що $x^n - 1 = (x-1)f_n(x)$. З рівності $x^{n_1 n_2} - 1 = (x^{n_1})^{n_2} - 1 = (x^{n_1} - 1)f_{n_2}(x^{n_1}) = (x-1)f_{n_1}(x)f_{n_2}(x^{n_1})$ випливає, що $f_{n_1 n_2}(x) = f_{n_1}(x)f_{n_2}(x^{n_1})$ для будь-яких $n_i \geq 1$, $1 \leq i \leq 2$.

Лема 4. *В кільці $Z[x]$ має місце включення $n \in < f_n(x), x-1 >_{Z[x]}$.*

Доведення. При $n = 1$ твердження леми 4 очевидне. При $n \geq 2$ доведення леми 4 випливає з формули

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

Відмітимо, що $x^n - 1 \in \langle \Phi_n(x) \rangle_{Z[x]}$. Тому $x^{nt} - 1 = (x^n - 1)f_t(x^n) \in \langle \Phi_n(x) \rangle_{Z[x]}$ для будь-якого натурального числа t. Аналогічно $f_d(x^{\frac{n}{d}}) = \frac{x^n - 1}{x^{\frac{n}{d}} - 1} \in \langle \Phi_n(x) \rangle_{Z[x]}$ для будь-якого дільника $d > 1$ числа n.

Лема 5. *Нехай n_1, n_2 - різні натуральні числа, $\Phi = \langle \Phi_{n_1}(x), \Phi_{n_2}(x) \rangle_{Z[x]}$. 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. За алгоритмом Евкліда $x^{(n_1,n_2)} - 1 \in \langle x^{n_1} - 1, x^{n_2} - 1 \rangle_{Z[x]}$. Якщо n_1, n_2 не є дільниками один одного, то елемент (n_1, n_2) відмінний від n_1 і n_2 і

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

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 4 і сказаним перед лемою 5

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

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

Будемо казати, що многочлен $p(x)$ кільця $R[x]$ є повним добутком многочленів $p_1(x), ..., p_t(x)$, $t \geq 1$ кільця $R[x]$ з елементом $p \in R$, якщо

$$p(x) = p_1(x) ... p_t(x) \text{ і при } t > 1 \; p \in \langle p_i(x), p_j(x) \rangle_{R[x]}$$

для всіх $1 \leq i \neq j \leq t$.

Зрозуміло, що якщо многочлен кільця $Z[x]$ є повним добутком деяких многочленів $Z[x]$ з деяким елементом, то його образ в $R[x]$ є повним добутком образів цих многочленів з образом відповідного елемента.

Якщо $p \in R^*$, то будемо казати що $p(x)$ є повним добутком многочленів $p_1(x), ..., p_t(x)$.

Теорема 1. *Нехай R - комутативне кільце з $1 \neq 0$, $n = p_1^{n_1} \dots p_k^{n_k} > 1$, $p = n^{(1+n_1)\dots(1+n_k)}$. Тоді $x^n - 1$ є повним добутком поліномів ділення круга $\Phi_d(x), d\,|n$ з елементом p. Якщо поліноми ділення круга $\Phi_d(x), d\,|n$ є повними добутками многочленів $p_{dl}(x)$ з елементами $p_d \in R$, то $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$, $d\,|n$ з елементом $p \prod\limits_{d|n} p_d$.*

Доведення. За означенням $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$. Згідно з лемою 5 $p_{ij} \in \langle \Phi_i(x), \Phi_j(x) \rangle_{R[x]}$, $1 \leq i \neq j \leq n$, якщо відношення дільників i та j або j та i числа n є степенем простого числа p_{ij}. За лемою 2 $p = \prod\limits_{i,j} p_{ij} \in \langle \Phi_i(x), \Phi_j(x) \rangle_{R[x]}$ для всіх $1 \leq i \neq j \leq n$.

Неважко бачити, що якщо $p(x)$ є повним добутком многочленів $p_1(x), ..., p_t(x)$ з елементом $p \in R$, а кожний многочлен $p_i(x)$ є повним добутком многочленів $p_{i1}(x), ..., p_{il}(x)$, $l = l(i) \geq 1$ з елементом $p_{\text{i}} \in R$, то $p(x)$ є повним добутком многочленів $p_{ij}(x)$ з елементом $pp_1 \dots p_t$, $1 \leq i \leq t$, $1 \leq j \leq l$.

Це випливає із включення $p \in \langle p_i(x), p_j(x) \rangle_{R[x]} \subset \langle p_{it_i}(x), p_{jt_j}(x) \rangle_{R[x]}$, якщо $1 \leq i \neq j \leq t$ і $p_i \in \langle p_{ir}(x), p_{is}(x) \rangle_{R[x]}$, якщо $1 \leq r \neq s \leq l$.

Тому елемент $p \prod\limits_{d|n} p_d$ належить всім $\langle p_{ir}(x), p_{js}(x) \rangle_{R[x]}$, де $1 \leq i, j \leq n$ - всі дільники числа n, і $1 \leq r \neq s \leq l$ при $i = j$.

Це означає,що двочлен $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$, $d\,|n$ з елементом $p \prod\limits_{d|n} p_d$.

Зрозуміло, що множини простих дільників натуральних чисел p і n співпадають.

Наслідок 3. *Нехай R - комутативне кільце з $1 \neq 0$, $n = p_1^{n_1} \dots p_k^{n_k} > 1$, $p = n^{(1+n_1)\dots(1+n_k)}$, $\Phi_d(x), d\,|n$ є повними добутками многочленів $p_{dl}(x)$. Тоді $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$ з елементом, множина простих дільників якого співпадає з множиною простих дільників n.*

Якщо $n \in R^*$, то $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$.

Доведення. За теоремою 1, в якій $p_d \in R^*$, $d\,|n$ двочлен $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$ з елементом p, множина простих дільників якого співпадає з множиною простих дільників числа n.

Зокрема, якщо $n \in R^*$, то $p \in R^*$ і $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$.

Наслідок 4. *Нехай R - комутативне локальне кільце, яке містить натуральне число $n \in R^*$. Тоді двочлен $x^n - 1$ є повним добутком двочленів $x - \varepsilon^i$, $0 < i \leq k$ і многочленів, які складають повні добутки поліномів ділення круга $\Phi_d(x)$, $d|n$, $d \not| k$, де ε породжує корені n-го степеня із 1 кільця R, k - порядок ε.*

Доведення. Неважко довести, що група коренів n-го степеня із 1 кільця R утворює циклічну групу порядку k, породжену елементом ε. При цьому k ділить n, $\varepsilon^i - \varepsilon^j \in R^*$ для всіх $0 < i \neq j \leq k$.

Згідно з лемою 5, якщо n - оборотний елемент, то поліноми ділення круга $\Phi_d(x)$, $d|n$ складають повний добуток двочлена $x^n - 1$ над довільним комутативним кільцем. Зокрема, $x^k - 1$ є повним добутком многочленів $\Phi_d(x)$, $d|k$, а

$\frac{x^n-1}{x^k-1} = f_{\frac{n}{k}}\left(x^k\right)$ є повним добутком многочленів $\Phi_d(x)$, $d|n$, $d \not| k$.

Оскільки $\varepsilon^i - \varepsilon^j \in R^*$, $0 < i \neq j \leq k$, то $\Phi_d(x)$ при $d|k$ є повним добутком двочленів $x - \varepsilon^{\frac{k}{d}s}$, $0 < s \leq d$, $(s,d) = 1$, а $x^k - 1$ повним добутком двочленів $x - \varepsilon^i$, $0 < i \leq k$. Тому двочлен $x^n - 1$ є повним добутком многочленів $x - \varepsilon^i$, $0 < i \leq k$ і многочленів, які утворюють повні добутки многочленів $\Phi_d(x)$, $d|n$, $d \not| k$.

6. Розклад матриць скінченного порядку над комутативними кільцями.

Лема 6. *Нехай R - комутативне кільце з $1 \neq 0$, V - лівий R- модуль, $a \in EndV$, $b \in EndV$ і $ab = ba$, $p(x)$ - повний добуток многочленів $p_1(x), ..., p_t(x)$ кільця $R[x]$ з елементом $p \in R$. Тоді існують R-підмодулі $V_1, ..., V_t$ модуля Vi степінь p^l, $l \geq t-1$ такі, що $p^l V \subset V_1 + \cdots V_t$, $aV_i \subset V_i$, $bV_i \subset V_i$, $1 \leq i \leq t$.*

Якщо $p(a) = 0$, то $p^l W_i = 0$, $p_i(a) V_i = 0$, де $W_i = V_i \bigcap (V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_t) = 0$, $1 \leq i \leq t$.

Доведення. Нехай $a_i = p_i(a)$, $b_i = a_1 \cdots a_{i-1} a_{i+1} \cdots a_t$, $V_i = b_i V$. Згідно з лемою 1 $p^{t-1} \in \langle a_i, b_i \rangle_{R[a]}$ і, як наслідок, існує степінь p^l, $l \geq t-1$ така, що $p^l \in \langle b_1, ..., b_t \rangle_{R[a]}$. Тому $p^l V \subset V_1 + \cdots V_t$. За умовою $ab = ba$, $a_i b = b a_i$, $b_i b = b b_i$ і $bV_i \subset b_i V = V_i$ для всіх $1 \leq i \leq t$.

Якщо $p(a) = 0$, то $a_i b_i = 0$ і, як наслідок, $b_j b_i = 0$ для всіх $1 \leq i \neq j \leq t$. Тому $a_i V_i = 0$, $b_i (V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_t) = 0$, $a_i W_i = b_i W_i = 0$, $p^{t-1} W_i = 0$, $p^l W_i = 0$ для всіх $1 \leq i \leq t$, $l \geq t-1$. При цьому $p_i(a) V_i = a_i V_i = 0$.

Позначимо $A_i = a|_{V_i}$. Тоді $p_i(A_i) = p_i(a|_{V_i}) = p_i(a) V_i = 0$ для всіх $1 \leq i \leq t$.

Елемент кільця називається нільпотентним, якщо деяка його натуральна степінь дорівнює нулю.

Теорема 2. *Нехай R – комутативне кільце з $1 \neq 0$, V - лівийR-модуль, $a \in EndV$, $p(x)$ - повний добуток степенів многочленів $p_1(x), ..., p_t(x)$, $t \geq 1$ кільця $R[x]$ з елементом $p \in$ R, таким що $pV = V$ і $Ann_V p = 0$, $p(a) = 0$. Тоді існує розклад $V = V_1 \oplus \cdots \oplus V_t$, де $aV_i \subset V_i$, $A_i = a|_{V_i}$, $a = diag(A_1, ..., A_t)$ і $p_i(A_i)$ - нільпотентні елементи для всіх $1 \leq i \leq t$.*

Якщо $b \in EndV$ і $ab = ba$, то $bV_i = V_i$, $1 \leq i \leq t$.

Доведення. Оскільки $pV = V$, то за лемою 6 $V = p^l V = V_1 + \ldots + V_t$. Нехай $p(x) = p_1(x)^{n_1} \cdots p_t(x)^{n_t}$, $t \geq 1$. З рівності $Ann_V p = 0$ випливає, що в лемі 6 $W_i = 0$ для всіх $1 \leq i \leq t$. Це означає, що $V = V_1 \oplus \cdots \oplus V_t$, $aV_i \subset V_i$ $p_i(A_i)^{n_i} = 0$, $p_i(A_i)$ - нільпотентні елементи, $bV_i = V_i$.

Зокрема, якщо $p(x)$ - повний добуток многочленів $p_1(x), ..., p_t(x)$, тобто в теоремі 2 $n_1 = \ldots = n_t = 1$, то $p_i(A_i) = 0$ для всіх $1 \leq i \leq t$.

Наслідок 5. *Нехай R – комутативне кільце з $1 \neq 0$, V - лівийR-модуль, $a \in EndV$, $a^n = 1$, $nV = V$ і $Ann_V n = 0$, $\Phi_d(x), d\,|n$ є повним добутком многочленів $p_{dl}(x)$, $l = l(d) \geq 1$. Тоді існують інваріантні відносно a R - підмодулі V_{dl} модуля V, такі що $V = \oplus \sum\limits_{d,l} V_{dl}$, $p_{dl}(A_{dl}) = 0$, де $A_{dl} = a\,|_{V_{dl}}$.*

Доведення. Згідно з теоремою 1 $x^n - 1$ є повним добутком многочленів $p_{dl}(x)$ з натуральним числом p кільця R, множина простих дільників якого співпадає з множиною простих дільників натурального числа n. В такому разі $pV = V$ і $Ann_V p = 0$. Тому твердження наслідку 5 випливає з теореми 2.

Теорема 3. *Нехай R – комутативне кільце з $1 \neq 0$, V – вільний R – модуль скінченного рангу m, прямі доданки якого є вільними R-модулями, $a \in GL(m,R) \equiv GL(m,V)$, $m = \dim V \geq 1$, $a^n = 1$ і многочлени $p_1(x), ..., p_t(x)$ утворюють повний добуток двочлена $x^n - 1$. Тоді, з точністю до спряження, a - діагональний елемент з матрицями на діагоналі, степені кожної з яких є коренями степенів одного із многочленів $p_1(x), ..., p_t(x)$ (не обов'язково одного і того ж самого).*

Доведення. При $m = 1$ для кожного степеня елемента a, згідно з теоремою 2, існує розклад, а значить і многочлен із $p_1(x), ..., p_t(x)$ коренем деякого степеня якого є заданий степінь елемента a. Нехай $m > 1$. Якщо довільна степінь елемента a є коренем степеня одного з многочленів $p_1(x), ..., p_t(x)$, то теорема 3 доведена.

Припустимо, що деяка степінь $a^i, i > 1$ елемента a не є коренем жодного з степенів многочленів $p_1(x), ..., p_t(x)$.

Тоді a^i, згідно з теоремою 2, з точністю до спряження, має діагональний вигляд з матрицями на діагоналі, які є коренями деяких степенів хоча б двох з многочленів $p_1(x), ..., p_t(x)$. Оскільки a комутує з a^i, то a має діагональний вигляд з хоча б двома матрицями на діагоналі. З індуктивних міркувань a має шуканий вигляд.

Наслідок 6. *Нехай R – комутативне локальне кільце, $n \in R^*$, V - вільний R-модуль скінченного рангу m, $a \in GL(m,R) \equiv GL(m,V)$, $a^n = 1$ і многочлени $p_1(x), ..., p_t(x)$ складають повний добуток поліномів ділення круга $\Phi_d(x)$, $d|n, d \not| k$. Тоді, з точністю до спряження, a - діагональний елемент з матрицями на діагоналі, степені кожної з яких є діагональними матрицями з степенями ε на діагоналі і матрицями, степені яких є коренями деяких степенів многочленів $p_1(x), ..., p_t(x)$, де ε породжує корені n-го степеня із 1 кільця R, а k його порядок.*

Доведення. Як уже відмічалося, корені n-го степеня із 1 комутативного локального кільця R при $n \in R^*$ (або довільної області цілісності R) утворюють циклічну групу.

Нехай R – комутативне локальне кільце з $1 \neq 0$, $n \in R^*$, ε - породжує корені n-го степеня із 1 кільця R і k - порядок ε. Згідно з теоремою 1 $x^k - 1$ - повний добуток двочленів $x - \varepsilon^i$, $1 \leq i \leq k$, а $x^n - 1$ - повний добуток $x^k - 1$ і $f_{\frac{n}{k}}(x^k) = \prod_{d|n, d\not|k} \Phi_d(x)$ і, як наслідок, повний добуток двочленів $x - \varepsilon^i$, $1 \leq i \leq k$ і многочленів $p_1(x), ..., p_t(x)$, які складають повні добутки поліномів ділення круга $\Phi_d(x)$, $d|n, d \not| k$.

Тому, з точністю до спряження, a - діагональна матриця з степенями ε на діагоналі і матрицями, степені яких є коренями деяких степенів многочленів $p_1(x), ..., p_t(x)$ (не обов'язково одного і того ж самого).

Наслідок 7. *Нехай R – комутативне кільце з $1 \neq 0$, V - вільний R-модуль скінченного рангу, $a \in EndV$, $p(x) = \det(xE - a)$ - повний добуток степенів двочленів $p_i(x) = x - a_i$, $a_i \in R$, $1 \leq i \leq t$ і прямі доданки модуля V є вільними R-модулями. Тоді, з точністю до спряження, a- сума діагональної матриці d і нільпотентної матриці $a - d$.*

Якщо $a_i = 0$ для деякого $1 \leq i \leq t$ або $a_i \in R^*$ для всіх $1 \leq i \leq t$, то

$d = P(a)$, *де* $P(x) \in xR[x]$.

Доведення. Оскільки многочлен $p(\mathrm{x}) = p_1(x)^{k_1} \dots p_t(x)^{k_t}$, $k_i \geq 1$, $1 \leq i \leq t$ є повним добутком степенів двочленів $p_i(x)$ і за теоремою Гамільтона-Келі $p(a) = 0$, то за теоремою 2 $V = V_1 \oplus \dots \oplus V_t$, де $aV_i \subset V_i$, $p_i(a)^{k_i} V_i = 0$.

Нехай $A_i = a|V_i$, $n_i = dim_R V_i$, E_{n_i} - одинична матриця групи $GL(n_i, V_i)$. Тоді, з точністю до спряження, $a = diag(A_1, ..., A_t)$ і $(A_i - a_i E_{n_i})^{k_i} = p_i(a)^{k_i} |V_i = 0$.

Нехай $d = diag(a_1 E_{n_1}, ..., a_t E_{n_t})$. В такому разі $a - d = diag(A_1 - a_1 E_{n_1}, ..., A_t - a_t E_{n_t})$ - нільпотентна матриця, $a = d + a - d$ - сума діагональної матриці d і нільпотентної матриці $a - d$.

Нехай $a_i = 0$ для деякого $1 \leq i \leq t$ або $a_i \in R^*$ для всіх $1 \leq i \leq t$. Очевидно, що якщо $a_i \in R^*$, то $1 \in < x, x - a_i >_R$. За китайською теоремою про остачі, застосованою до многочленів $x, p_1(x), \dots, p_t(x)$, якщо $a_i \in R^*$ для всіх $1 \leq i \leq t$ і многочленів $p_1(x), \dots, p_t(x)$ якщо $a_i = 0$ для деякого $1 \leq i \leq t$, існує многочлен $P(x) \in xR[x]$ такий, що $P(x) - a_i \in p_i^{k_i}(x) R[x]$ для всіх $1 \leq i \leq t$. Адже, у випадку, якщо деякий елемент $a_i = 0$, то $P(x) \in x^{k_i} R[x] \subset xR[x]$.

Оскільки $(P(a) - a_i E_{n_i}) V_i = 0$, то $d = P(a)$.

Якщо $b \in EndV$ і $ab = ba$, то $db = bd$.

7. Ендоморфізми модулів над асоціативними кільцями. Нехай R – асоціативне кільце з $1 \neq 0$, V - ненульовий лівий R-модуль, $EndV$- кільце ендоморфізмів модуля V над R, G - підгрупа кільця $EndV$.

Група G називається звідною, якщо існує інваріантний відносно G ненульовий R-підмодуль $V_1 \neq V$, для якого існує R-підмодуль V_2 модуля V такий, що $V = V_1 \oplus V_2$. Якщо при цьому R-модуль V_2 інваріантний відносно G, то група G називається розкладною. В противному випадку група G називається незвідною і нерозкладною відповідно.

Аналогічні поняття розглядаються для модулів, які інваріантні відносно деяких ендоморфізмів.

Очевидно, що гомоморфний образ скінченнопородженого R-модуля V є скінченнопородженим. Тому прямі доданки вільного R-модуля V скінченного рангу є скінченнопородженими.

Більше того, якщо R – кільце головних ідеалів або локальне кільце, то ці доданки вільні і мають скінчені ранги, сума яких співпадає з рангом модуля. Тому, якщо над цими кільцями R-модуль V, має скінчену розмірність і $G \subset EndV$ - звідна група, то існує інваріантний відносно G ненульовий, відмінний від V, вільний R-підмодуль модуля V, R-базис якого доповнюється до R-базиса модуля V. Навпаки очевидно.

Це означає, що над вищевказаними кільцями запропоноване означення звідності групи G співпадає з класичним.

Зрозуміло, що розкладна група є звідною. Якщо G - скінчена група і $|G| \in R^*$, то вірно і навпаки. Це випливає з теореми Машке.

Теорема Машке. *Нехай R – асоціативне кільце з $1 \neq 0$, V - ненульовий лівий R-модуль, G - скінченна звідна підгрупа кільця $EndV$, $|G| \in R^*$. Тоді G-розкладна група.*

Доведення. Нехай $V = V_1 \oplus V_2$, $0 \neq V_1 \neq V_2$, де $GV_1 \subset V_1$. Розглянемо ендоморфізм R-модуля V на V_1, який називається проектором і визначається за правилом $h(v_1 + v_2) = v_1$ для будь-яких $v_1 \in V_1, v_2 \in V_2$. Нехай $e = \frac{1}{|G|} \sum\limits_{g \in G} ghg^{-1}$.

Тоді, $e|V_1 = 1$ - тотожній ендоморфізм модуля V_1. Тому $e^2v = e(ev) = ev$ для всіх $v \in V$, $e^2 = e$ - ідемпотент, $V_1 = eV$, $V = eV \oplus (1-e)V$ - розклад R-модуля V в пряму суму інваріантних G-підмодулів модуля V.

З теореми Машке випливає, що якщо $a \in GL(V) \equiv (EndV)^*$ є коренем двочлена $x^n - 1$, $n \in R^*$, то R-модуль V є прямою сумою інваріантних відносно a R-підмодулів.

Нехай R – комутативне кільце з $1 \neq 0$, $p(x)$ є повним добутком многочленів $p_1(x), ..., p_t(x)$, $t \geq 1$, W - незвідний інваріантний відносно a R-підмодуль модуля V, $a \in GL(V)$, $p(a) = 0$, $a_i = p_i(a)$, $b_i = a_1 \cdots a_{i-1}a_{i+1} \cdots a_t$, $1 \leq i \leq t$.

З теореми 2 випливає, що існує число $1 \leq j \leq t$ таке, що $W = b_jW$ і $b_iW = 0$ для всіх $1 \leq i \neq j \leq t$. При цьому $p_j(a)W = 0$.

Зрозуміло, що якщо $W \neq 0$, то $p_i(a)W \neq 0$ для всіх $1 \leq i \neq j \leq t$.

Таким чином, якщо a - є коренем повного добутку деяких многочленів на незвідному, інваріантному відносно a R- підмодулі, то a є коренем тільки одного з його множників.

Якщо R – область цілісності, а $Q(R)$ - поле відношень R, то ненульовий скінченнопороджений R-модуль V перетворюється в ненульовий $Q(R)$ -лінійний простір $Q(R)V$ скінченної розмірності, яка не перевищує число породжуючих елементів R-модуля V.

Якщо $G \subset End\ V$, W - незвідний $Q(R)G$ -підмодуль $Q(R)V$, то $V \bigcap W$- незвідний RG-підмодуль V. Окрім цього спадні ланцюги модуля скінченного рангу над областями цілісності стабілізуються.

Це означає, що вільний R-модуль скінченного рангу над областю цілісності R, при $n \in R^*$, $a^n = 1$ є скінченною прямою сумою незвідних інваріантних відносно a скінченно породжених R-підмодулів. Якщо R- кільце головних ідеалів, то твердження залишається вірним без вимоги $n \in R^*$. При цьому скінченнопороджені доданки є вільними R-підмодулями.

Аналогічно, якщо R – комутативне локальне кільце, $n \in R^*$, $a^n = 1$, то вільний R-модуль скінченного рангу є скінченною прямою сумою незвідних інваріантних відносно a вільних R-підмодулів.

8. Застосування класичних теорем до деяких матриць скінченного порядку. Фундаментальною теоремою кільця многочленів, яка поклала початок сучасної алгебри є теорема Гільберта про базиси.

Теорема Гільберта про базиси. *Нехай R - комутативне ньотерове кільце з $1 \neq 0$. Тоді $R[x]$ - ньотерове кільце.*

Доведення. від супротивного. Нехай I - деякий ідеал кільця $R[x]$, який не є скінченнопородженим. Це означає, що в I існує нульовий елемент $p_o(x) = 0$ і многочлени $P_1(x), P_2(x), \ldots$ із старшими коефіцієнтами $a_1, a_2, \ldots$ такі, що $P_{i+1}(x)$ - многочлен найменшого степеня, який належить I і не належить ідеалу $< P_0(x), \ldots, P_i(x) >_{R[x]}$, $i \geq 0$. Оскільки $P_{i+1}(x)$ не належить ідеалу $< P_0(x), \ldots, P_{i-1}(x) >_{R[x]}$, то $\deg P_i(x) \leq \deg P_{i+1}(x)$ для всіх $i \geq 1$. За умовою зростаючий ланцюг ідеалів $< a_1 >_R \subseteq < a_1, a_2 >_R \subseteq \ldots$ кільця R на деякому n -му кроці стабілізується, але за припущенням не всі члени послідовності $P_1(x), P_2(x), \ldots$ належать ідеалу $< P_1(x), \ldots, P_{\mathrm{n}}(x) >_{R[x]}$.

Якщо j - найменше натуральне число, таке що $P_j(x) \notin < P_1(x), \ldots, P_n(x) >_{R[x]}$, то $j > n$ і $a_{j+1} = a_1u_1 + \ldots + a_nu_n$, де $u_i \in R$, $1 \leq i \leq n$. Позначимо $v_i = u_i x^{\deg P_{j+1}(x) - \deg P_i(x)}$, де $1 \leq i \leq n$. Тоді $P_{j+1}(x) - (P_1(x)v_1 + \ldots + P_n(x)v_n)$-

многочлен меншого степеня, ніж $P_{j+1}(x)$, який належить I і не належить ідеалу $< P_1(x), \ldots, P_j(x) >_{R[x]}$ всупереч вибору многочлена $P_{j+1}(x)$. Отримане протиріччя показує, що будь-який ідеал кільця $R[x]$ є скінченно породженим в кільці $R[x]$. Тому $R[x]$ - ньотерове кільце.

З теореми Гільберта про базиси випливає, що кільце $R[x_1, \ldots, \mathrm{x_n}]$, $n \geq 1$ є ньотеровим кільцем, якщо R - комутативне ньотерове кільце. Оскільки при факторизаціях ньотерові кільця залишаються ньотеровими, то будь-яке підкільце $R_0[r_1, \ldots, \mathrm{r_n}]$, яке породжене ньотеровим підкільцем R_0 і елементами $r_1, ..., r_n$ комутативного кільця R з $1 \neq 0$, є ньотеровим.

Зокрема, в ролі R_0 можна взяти підкільце R, яке породжене одиницею кільця R.

Прикладами кілець головних ідеалів, а значить і ньотерових та факторіальних кілець, є кільце цілих чисел Z і $P[x]$ - кільце многочленів над полем P.

Нехай R - область цілісності. Тоді $R[x]$ - область цілісності. Якщо при цьому $R[x]$ є кільцем головних ідеалів, то ідеал $< x, r \neq 0 \in R >_{R[x]} = d(x) R[x]$. Тому $d(x)$ ділить елементи r і x. Це можливо тільки в тому випадку, коли $\deg d(x) = 0$ і $d(x) \in R^*$. В такому разі $< x, r \neq 0 \in R >_{R[x]} = R[x]$ і $rR = R$ - поле.

Зокрема, кільця $Z[x]$, $P[x_1, ..., x_n]$, де P - поле, $n \geq 2$, не є кільцями головних ідеалів, хоча при $n \geq 1$ вони є ньотеровими кільцями і, як буде показано нижче, факторіальними кільцями.

Нехай R - факторіальне кільце.

Змістом многочлена $f(x)$ кільця $R[x]$ називається найбільший спільний дільник його коефіцієнтів, який позначається $d(f)$. Як було доведено вище, $d(rf) = rd(f)$, якщо $r \in R$.

Зрозуміло, що $d(f)$ визначається з точністю до оборотних елементів кільця R і ділить старший коефіцієнт многочлена $f(x)$. Многочлен, зміст якого з точністю до оборотних елементів, дорівнює одиниці називається примітивним многочленом.

Очевидно, що унітарні многочлени є примітивними многочленами.

Неважко бачити, що будь-який многочлен $f(x) \in R[x]$ можна записати у стандартному вигляді $f(x) = d(f) f'(x)$, де $f'(x)$ - примітивний многочлен кільця $R[x]$.

Лема Гауса. *Нехай R - факторіальне кільце, $f(x)$ і $g(x)$ - многочлени кільця $R[x]$. Тоді, з точністю до оборотних елементів кільця R, $d(fg) = d(f) d(g)$.*

Доведення. Нехай $d(f) = d(g) = 1$, але $d(fg) \neq 1$. Тоді існує простий елемент $p \in R$, який ділить всі коефіцієнти многочлена $f(x) g(x)$, але не ділить всі коефіцієнти многочленів $f(x)$ і $g(x)$. Оскільки p - простий елемент кільця R, то $P = R/pR$ і $P[x]$ - області цілісності. Тому рівність $0 = f(x) g(x)$ для многочленів $f(x) \neq 0$ і $g(x) \neq 0$ в кільці $P[x]$ неможлива. Тим самим доведено, що добуток примітивних многочленів є примітивним многочленом.

У загальному випадку $f(x) = d(f) f'(x)$, $g(x) = d(g) g'(x)$, де $f'(x), g'(x)$ і як наслідок, добуток $f'(x) g'(x)$ - примітивні многочлени кільця $R[x]$. Оскільки $f(x) g(x) = d(f) d(g) f'(x) g'(x)$, то $d(fg) = d(f) d(g)$.

З леми Гауса випливає, що примітивний многочлен кільця $R[x]$ може розкладатися в добуток тільки примітивних многочленів кільця $R[x]$.

Наслідок 8. *Нехай R - факторіальне кільце, $Q(R)$ - поле відношень кільця R. Тоді будь-який незвідний многочлен кільця $R[x]$ є незвідним і в $Q(R)[x]$.*

Доведення. Нехай $F(x)$ - незвідний многочлен кільця $R[x]$. За означенням $F(x)$ - многочлен позитивного степеня. Якщо $F(x)$ - звідний многочлен в кільці $Q(R)[x]$, то в $Q(R)[x]$ існують многочлени позитивного степеня, які можна записати у стандартному вигляді $\frac{a}{b}f(x)$, $\frac{c}{d}g(x)$, де a, b, c, d - елементи R, такі, що $(a, b) = (c, d) = 1$, $f(x)$ і $g(x)$ - примітивні многочлени кільця $R[x]$ для яких, з точністю до оборотних елементів кільця R, $F(x) = \frac{ac}{bd}f(x)g(x)$. Оскільки $d(F)bd$ - зміст многочлена $bdF(x)$, а ac - зміст рівного йому многочлена $acf(x)g(x)$, то $d(F)bd = ac$. Тому $F(x) = d(F)f(x)g(x)$, що протирічить незвідності многочлена $F(x)$ у кільці $R[x]$.

Наслідок 9. *Нехай R - факторіальне кільце, $g(x)$ - унітарний многочлен кільця $R[x]$, $f(x)$ - многочлен $R[x]$, який ділить $g(x)$ в $Q(R)[x]$, a - старший коефіцієнт $f(x)$. Тоді a - зміст $f(x)$ і многочлен $\frac{f(x)}{a}$ кільця $R[x]$ ділить $g(x)$ в кільці $R[x]$.*

Доведення. За умовою існують $r \neq 0 \in R$ і $h(x) \in R[x]$ такі, що $rg(x) = f(x)h(x)$. Неважко бачити, що старший коефіцієнт многочлена $h(x)$, з точністю до оборотніх елементів кільця R, дорівнює $\frac{r}{a}$. За лемою Гауса, з точністю до оборотніх елементів кільця R, $r = d(f)d(h)$ ділить $a \cdot \frac{r}{a} = r$, де $d(f)$ - зміст многочлена $f(x)$, а $d(h)$ - зміст многочлена $h(x)$. Тому, з точністю до оборотніх елементів кільця R, $d(f) = a$ і $d(h) = \frac{r}{a}$. Це означає, що a ділить всі коефіцієнти многочлена $f(x)$, $\frac{r}{a}$ всі коефіцієнти $h(x)$, а r ділить всі коефіцієнти многочлена $f(x)h(x)$. Після скорочення заданої рівності $rg(x) = f(x)h(x)$ на елемент r, отримуємо, що многочлен $\frac{f(x)}{a} \in R[x]$ ділить $g(x)$ в кільці $R[x]$.

Нехай R – факторіальне кільце. Як було сказано вище кільце $Q(R)[x]$ - факторіальне. Роль простих елементів в ньому виконують незвідні многочлени. Серед них знаходяться примітивні многочлени кільця $R[x]$, які є незвідними в $R[x]$ і, як наслідок, в $Q(R)[x]$. Разом з простими елементами факторіального кільця R вони складають множину всіх простих елементів кільця $R[x]$.

Адже, будь-який ненульовий необоротний многочлен кільця $R[x]$ може бути зображений добутком простих елементів кільця R і примітивних незвідних многочленів кільця $R[x]$.

Очевидно, що примітивні многочлени кільця $R[x]$ співпадають в $Q(R)[x]$, тоді і тільки тоді, коли вони, з точністю до оборотних елементів кільця R, співпадають в $R[x]$.

Тому, якщо в кільці $R[x]$ є два рівні добутки вищеназваних елементів, то в кільці $Q(R)[x]$ множини цих елементів співпадають і кожний з них входить в добутки із однаковим показником степеня. Після відповідного скорочення рівних елементів кільця $R[x]$ залишаються рівні добутки простих елементів кільця R, множини яких в силу факторіальності кільця R, співпадають і кожний з множників входить в добутки з однаковим показником степеня.

Тому $R[x]$ - факторіальне кільце, якщо R -факторіальне кільце. Зокрема, $R[x_1, \ldots, x_n]$, $n \geq 1$ - факторіальне кільце, якщо R - поле або R - факторіальне кільце.

Лема Круля. *Нехай R - комутативне ньотерове кільце з $1 \neq 0$, I - ненульовий ідеал R. Тоді $\bigcap I^t = 0$ для всіх $t \geq 1$ має місце тоді і тільки тоді, коли*

$1-I$ *не має дільників нуля в* R.

Доведення. Якщо $r \in R$, $i \in I$, $r(1-i)=0$, то $r = ri = ri^2 = \ldots \in \bigcap I^t$. Тому з умови $\bigcap I^t = 0$ випливає, що $r = 0$, $1-I$ не має дільників нуля в R. Навпаки. Нехай $1-I$ не має дільників нуля в R, але $J = \bigcap I^t \neq 0$. Оскільки R - ньотерове кільце, то $I =< r_1, ..., r_l >_R$.

Нехай j - довільний елемент J. Оскільки $j \in \bigcap I^t$, $t \geq 1$, то $j = F_t(r_1, ..., r_l)$, $F_t(r_1, ..., r_l)$ - деякий однорідний многочлен степеня t кільця $R[x_1, \ldots, x_l]$.

Ідеал $< F_t(r_1, ..., r_l) | t \geq 1 >$ за теоремою Гільберта про базис в ньотеровому кільці $R[x_1, \ldots, x_l]$ є скінченнопородженим ідеалом. Нехай $P_1, ..., P_s$ - породжуючі його елементи. Тоді $F_t = \sum\limits_i u_i P_i$, $1 \leq i \leq s$. Якщо t більше від степенів многочленів $P_1, ..., P_s$, то можна вважати, що $u_1, ..., u_s$ - многочлени без вільних членів. Тому після заміни $x_1, ..., x_l$ на $r_1, ..., r_l$ відповідно, отримуємо що $j \in Ij$ і, як наслідок, $J = IJ$.

Нехай $J =< e_1, ..., e_k >_R$. Згідно з вище доведеним $e_i = \sum a_{ij} e_j$, де $a_{ij} \in I$, $1 \leq i, j \leq k$. Нехай $A = (a_{ij})$. Тоді $\det(E-A)\, e_i = 0$ для всіх $1 \leq i \leq k$. Оскільки елемент $\det(E-A)\, e_i \in 1-I$ не має дільників нуля в R, то $e_i = 0$ для всіх $1 \leq i \leq k$ і, як наслідок, $J = 0$. Це, однак, протирічить припущенню. Тим самим доведено, що $J = 0$.

Застосуємо теорему Гільберта про базис і лему Круля, яка з неї випливає, до деяких матриць скінченного порядку над комутативними кільцями.

Теорема 4. *Нехай* R *- комутативне кільце з* $1 \neq 0$, $J(R)$ *- радикал Джекобсона кільця* R, v *- матриця кільця матриць* R_m, $m \geq 1$ *елементи якої належать* $J(R)$, n *- натуральне число, таке що* $(E+v)^n = E$ *і існує натуральне число* l, *яке взаємно-просте з* n *і належить* $J(R)$. *Тоді* $v = 0$.

Доведення. Якщо $v = 0$, то все доведено. Припустимо, що $v \neq 0$. Нехай R_v - підкільце R, яке породжене елементом 1 та v_{ij}, $1 \leq i, j \leq m$ матриці $v = (v_{ij})$. За теоремою Гільберта про базис R_v - ньотерове кільце з $1 \neq 0$. За умовою $1 = xl + yn$, де $x, y \in Z$.

Нехай $I = R_v \bigcap J(R)$. Неважко бачити, що I - ненульовий ідеал кільця R_v, який містить l і елементи матриці v. Тому елементи матриць xlv і v^2 належать I^2 і

$$E + v = (E+v)^{xl} = E + v' = (E+v')^{xl} = E + v'' = \ldots,$$

де $v = v'$ - матриця над I^2. Аналогічно $v' = v''$ - матриця над I^3 і т.д. Це означає, що $v_{ij} \in \bigcap I^t$ для всіх $1 \leq i, j \leq m$. Із включення $1+I \subset 1+J(R) \subset R^*$ випливає, що $1-I$ не має дільників нуля в кільці R. За лемою Круля $\bigcap I^t = 0$, $v_{ij} = 0$, $1 \leq i, j \leq m$. Отримане протиріччя показує, що $v = 0$.

Наслідок 10. *Нехай* R *- комутативне кільце з* $1 \neq 0$, $J(R)$ *- радикал* R, $v \in (J(R))_m$, $m \geq 1$ *і існують числа* l *і* n *такі, що* $(l, n) = 1$, $l \in J(R)$ *і* $(E+v)^{ln} = E$. *Тоді* $(E+v)^l = E$.

Доведення. Нехай $v_0 = (E+v)^l - E$. Тоді $(E+v_0)^n = E$. За теоремою 4 $v_0 = 0$.

9. Матриці скінченного порядку над кільцями головних ідеалів. Нехай R - кільце головних ідеалів, V - лівий вільний R -модуль скінченного рангу, W - ненульовий підпростір $Q(R)V$. Оскільки будь-який R -підмодуль модуля V є вільним, то $V \bigcap W$ - ненульовий вільний R -підмодуль V, $V/V \bigcap W$-

скінченнопороджений без кручення, а тому вільний R -модуль. Це означає, що R -базис модуля $V \bigcap W$ доповнюється до R -базиса модуля V.

Нехай $G \subset EndV$, V - RG -модуль і W - ненульовий, інваріантний відносно G підпростір $Q(R)V$. Як було показано вище $V \bigcap W$ - інваріантний відносно G ненульовий прямий доданок R -модуля V.

Якщо V - незвідний RG -модуль, то $V \bigcap W = V$, $V \subset W$, $Q(R)V \subset W$, $W = Q(R)V$. Це означає, що V - незвідний $Q(R)G$ -модуль.

Тим самим доведено, що із незвідності RG -модуля V випливає його незвідність над полем $Q(R)$. Навпаки очевидно.

Нехай $G = \langle a \,|a^n = 1\rangle$, V - незвідний RG -модуль скінченного рангу над R, $v \neq 0 \in V$. В такому разі існує найбільше натуральне число $m \leq n$, таке що елементи $v, av, \ldots, a^{m-1}v$ - лінійно незалежні над $Q(R)$, $m = \dim Q(R)V$. Із незвідності V над полем $Q(R)$ випливає, що $Q(R)V = \langle v, av, \ldots, a^{m-1}v\rangle_{Q(R)}$. Оскільки $(a^n - 1)v = 0$, то існує многочлен $f(x)$ найменшого степеня кільця $R[x]$, такий, що $f(a)v = 0$. Ясно, що $\deg f(x) = m$, $f(a)V = 0$, $f(x)$ - дільник $x^n - 1$ над полем $Q(R)$.

З наслідку 9 леми Гауса слідує, що, без обмеження загальності, можна вважати $f(x)$ унітарним многочленом кільця $R[x]$.

Якщо $f(x)$ - добуток взаємно-простих многочленів позитивного степеня $f_1(x)$ і $f_2(x)$ кільця $R[x]$, то цей добуток повний і, згідно з наслідком 5, $V = V_1 \oplus V_2$ і $f_1(a)V_1 = f_2(a)V_2 = 0$. Із незвідності V випливає, що $V = V_i$, $f_i(a)V = 0$, де $i = 1$ або $i = 2$, що протирічить мінімальності степеня многочлена $f(x)$. Тим самим доведено, що $f(x)$ - деяка степінь незвідного унітарного многочлена $p(x) \in R[x]$, який, згідно з наслідком 8 леми Гауса, є незвідним многочленом і над полем $Q(R)$.

Нехай ξ - елемент алгебраїчного замикання поля $Q(R)$, такий що $p(\xi) = 0$ і $Q(R)(\xi)$ - поле, яке утворене приєднанням до поля $Q(R)$ елемента ξ. Підкреслимо, що поле $Q(R)(\xi)$ перетворюється в незвідний $Q(R)G$ -модуль, якщо дію a задати як оператор множення на ξ. Тому в базисі $1, \xi, \ldots, \xi^{n-1}$ матриця a задається кліткою Фробеніуса з коефіцієнтами многочлена $p(x)$.

Відображення $\Lambda_{Q(R)} : V \to Q(R)(\xi)$ за правилом $v \to \xi$ індукує ізоморфізм $Q(R)G$ -модулів V і $Q(R)(\xi)$, а його звуження RG -гомоморфізм $\Lambda_R : V \to I$, де I -ненульовий скінченнопороджений $R[\xi]$ -підмодуль поля $Q(R)(\xi)$.

Нехай $v_0 \in V$, такий що $\Lambda_R(v_0) = 0$. Оскільки $v_0 \in Q(R)V$, то існує $r_0 \neq 0 \in R$ і $g(x) \in R[x]$, такі що $r_0 v_0 = g(a)v$. Тому $0 = r_0\Lambda_R(v_0) = \Lambda_R(r_0 v_0) = g(\xi)\xi$, $g(\xi) = 0$, $p(x)$ ділить $g(x)$ в кільці $R[x]$. Це означає, що $v_0 \in p(a)Q(R)V$. Тим самим доведено, що $\ker \Lambda_R = p(a)Q(R)V \bigcap V$.

Ненульовий скінченнопороджений модуль над областю цілісності, який належить його полю відношень, прийнято називати дробовим ідеалом області цілісності.

Тому I - дробовий ідеал кільця $R[\xi]$, який належить його полю відношень $Q(R)(\xi)$. Очевидно, що I - скінченнопороджений R -модуль без кручення, а тому вільний R -модуль, який як $Q(R)G$ -модуль співпадає з полем $Q(R)(\xi)$ і тому є незвідним RG -модулем.

Неважко бачити, що αI для будь-якого $\alpha \neq 0 \in Q(R)(\xi)$ також дробовий ідеал $R[\xi]$, який як $Q(R)G$ -модуль ізоморфний $Q(R)(\xi)$. Прийнято казати, що дробові ідеали I та αI належать одному класу дробових ідеалів кільця $R[\xi]$.

Відображення $\Lambda : I \to \alpha I$ за правилом $\Lambda(r) = \alpha r$, $r \in I$ задає RG - ізоморфізм. Адже,

$$\Lambda\left((\sum \alpha_i a^i)r\right) = \alpha\left(\sum \alpha_i \xi^i r\right) = \left(\sum \alpha_i \xi^i\right)(\alpha r) = (\sum \alpha_i a^i)\Lambda(r).$$

Вірно і навпаки. Адже, якщо $\Lambda : I \to \Lambda(I)$ є RG -ізоморфізмом дробових ідеалів кільця $R[\xi]$, то для довільних ненульових елементів r і r_1 дробового ідеала I існує ненульовий елемент $\gamma \in I$, такий, що γr^{-1} і γr_1^{-1} належать $R[\xi]$. Тому $\Lambda(\gamma) = \gamma r^{-1}\Lambda(r) = \gamma r_1^{-1}\Lambda(r_1)$. Нехай $\alpha = r^{-1}\Lambda(r) = r_1^{-1}\Lambda(r_1)$. З вищесказаного випливає, що $\Lambda(r) = \alpha r$, де α не залежить від r.

Таким чином дробові ідеали кільця $R[\xi]$ належать одному класу дробових ідеалів тоді і тільки тоді, коли вони ізоморфні як RG -модулі.

Незвідні RG -модулі V скінченного рангу над кільцем головних ідеалів R групи $G = \langle a \,|a^n = 1\rangle$, які як $Q(R)G$ -модулі ізоморфні полю $Q(R)(\xi)$, де ξ - корінь незвідного над R дільника $p(x)$ двочлена $x^n - 1$, породжують ізоморфізми RG-модулів ${}^{V}\!/_{p(a)Q(R)V \bigcap V}$ з дробовими ідеалами фіксованих класів дробових ідеалів кільця $R[\xi]$. Число незвідних RG -модулів V скінченного рангу над R не менше від числа класів дробових ідеалів кільця $R[\xi]$.

Нехай $n \neq 0$ в R. Тоді $n \in Q(R)^*$, $x^n - 1$ не має кратних дільників в $R[x]$. Тому $p(a)V = 0$, $\ker \Lambda_R = 0$.

Тим самим доведено, що має місце

Наслідок 11. *Незвідні RG -модулі скінченного рангу над кільцем головних ідеалів R групи $G = \langle a \,|a^n = 1\rangle$, при $n \neq 0$ в R, ізоморфні дробовим ідеалам кільця $R[\xi]$. Їх число дорівнює числу класів дробових ідеалів кільця $R[\xi]$.*

Доведення. Довільний RG -модуль V скінченного рангу над R перетворюється в $Q(R)G$ - модуль скінченної розмірності над полем $Q(R)$. За теоремою Машке $Q(R)V$ є прямою сумою незвідних $Q(R)G$ -модулів $W_1, ..., W_t$, $t \geq 1$. Тому V є прямою сумою вільних над R незвідних RG -модулів, які ізоморфні дробовим ідеалам кільця $R[\xi_i]$, $1 \leq i \leq t$, де W_i ізоморфний як $Q(R)G$ -модуль з $Q(R)(\xi_i)$.

Тому a, з точністю до спряження, задається діагональною матрицею з матрицями на діагоналі, які визначаються дією a на дробові ідеали кілець $R[\xi_i]$, $1 \leq i \leq t$.

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 університет, 2003. - 119 с.
3. *Гудивок П.М., Рудько В.П., Бовді В.А.* Кристалографічні 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: Изд. объед. "Вища школа 1980. - 192 с.
6. *Каргаполов М.И., Мерзляков Ю.И.* Основы теории групп. - 3-е изд. перероб. и доп. - Москва: Наука, 1982. - 288 с.
7. *Петечук В.М.* Стабильность колец // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. - 2009. Вип. 19. - с. 87 - 111.
8. *Фейт У.* Теория представлений конечных групп: Пер. с англ. - М.: Наука. Гл. ред. физ.-мат., 1990. - 464 с.

Одержано 25.04.2013