

УДК 512.547.25

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

ЗОБРАЖЕННЯ ГРУП ДІЕДРА ВИЩИХ СТЕПЕНІВ НАД ДЕЯКИМИ КОМУТАТИВНИМИ ЛОКАЛЬНИМИ КІЛЬЦЯМИ.

Commutative local rings R with identity with m – an inverse element are considered. Representations $D_m \rightarrow GL(n, R)$ of an arbitrary degree $n \geq 1$ of the dihedral group $D_m = \langle a, b \mid a^m = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$, $m > 1$ over R are described. Conditions of irreducibility, indecomposability and equivalency are found. It is proved that the m -th roots of unity of the ring R form a cyclic group and up to equivalency, the representations of the group D_m , $m > 1$ over R are generated by one-dimensional representations $a \rightarrow \pm 1$, $b \rightarrow \alpha$, $\alpha^2 = 1$, two-dimensional indecomposable representations

$$a \rightarrow \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}, b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } a \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}, b \rightarrow \pm \begin{pmatrix} -1 & 0 \\ r & 1 \end{pmatrix},$$

where the element ε generates the m -th roots of unity of the ring R , k – order of ε , $r \in R$, polynomial $x^2 - rx + 1$ divides $x^m - 1$ without residue, $r \neq \varepsilon^i + \varepsilon^{-i}$, $1 \leq i < \frac{k}{2}$,

$$a \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b \rightarrow \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } a \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + J,$$

where $2 \in J(R)$, J – indecomposable matrix over the radical $J(R)$, $J(2 + J) = 0$, and also by the indecomposable representations of degree $n > 2$ $a \rightarrow E_n$, $b \rightarrow E_n + J_n$ (when $2 \in J(R)$) and $a \rightarrow a_0$, $b \rightarrow b_0$, where J_n – indecomposable matrix over the radical $J(R)$, $J_n(2 + J_n) = 0$, and a_0 – root of the polynomial $1 + x^k + \dots + x^{m-k}$, $b_0^2 = 1$, $b_0 a_0 b_0^{-1} = a_0^{-1}$.

Розглядаються комутативні локальні кільця R з 1, в яких m – оборотний елемент. Описано зображення $D_m \rightarrow GL(n, R)$ довільного степеня $n \geq 1$ групи діедрa $D_m = \langle a, b \mid a^m = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$, $m > 1$ над R . Знайдено умови їх незвідності, нерозкладності і еквівалентності. Доведено, що, корені m -го степеня із 1 кільця R утворюють циклічну групу і, з точністю до еквівалентності, зображення групи D_m , $m > 1$ над R породжуються одномірними зображеннями $a \rightarrow \pm 1$, $b \rightarrow \alpha$, $\alpha^2 = 1$, двомірними нерозкладними зображеннями

$$a \rightarrow \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}, b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ і } a \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}, b \rightarrow \pm \begin{pmatrix} -1 & 0 \\ r & 1 \end{pmatrix},$$

де елемент ε породжує корені m -го степеня із 1 кільця R , k – порядок ε , $r \in R$, тричлен $x^2 - rx + 1$ ділить без остачі двочлен $x^m - 1$, $r \neq \varepsilon^i + \varepsilon^{-i}$, $1 \leq i < \frac{k}{2}$,

$$a \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b \rightarrow \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \text{ і } a \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + J,$$

де $2 \in J(R)$, J – нерозкладна матриця над радикалом $J(R)$, $J(2 + J) = 0$, а також нерозкладними зображеннями степеня $n > 2$ $a \rightarrow E_n$, $b \rightarrow E_n + J_n$ (при $2 \in J(R)$) і $a \rightarrow a_0$, $b \rightarrow b_0$, де J_n – нерозкладна матриця над радикалом $J(R)$, $J_n(2 + J_n) = 0$, а a_0 – корінь многочлена $1 + x^k + \dots + x^{m-k}$, $b_0^2 = 1$, $b_0 a_0 b_0^{-1} = a_0^{-1}$.

У даній статті описуються всі зображення довільного степеня групи діедрa $D_m = \langle a, b \mid a^m = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$, $m > 1$ над комутативними локальними кільцями з одиницею при умові, що m –оборотний елемент кільця. Виявилось, що такі зображення зводяться до зображень близьких до відповідних зображень груп діедрa над полями і зображень груп діедрa над комутативними локальними кільцями, які не містять нетривіальних коренів m -го степеня із одиниці.

Даний підхід спирається на метод лишкових підмодулів з використанням теореми Машке.

Нехай R – комутативне локальне кільце з 1, R^* – група оборотних елементів кільця R , $m \in R^*$, ε породжує корені m -го степеня із 1 кільця R , k – порядок

ε , D_m , $m > 1$ – група діедра порядку $2m$, $\Lambda : D_m \rightarrow GL(n, R)$ – довільне зображення групи D_m у групу $GL(n, R)$, $n \geq 1$.

З'ясуємо умови нерозкладності, незвідності і еквівалентності цих зображень. Покажемо, що, з точністю до еквівалентності, такі зображення породжуються одновірними зображеннями $a \rightarrow \pm 1$, $b \rightarrow \alpha$, $\alpha^2 = 1$, $\alpha \in R$, двовірними нерозкладними зображеннями

$$a \rightarrow \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}, b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ і } a \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}, b \rightarrow \pm \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix},$$

де $r \in R$, тричлен $x^2 - rx + 1$ ділить без остачі двочлен $x^m - 1$, $r \neq \varepsilon^i + \varepsilon^{-i}$, для всіх $1 \leq i < \frac{k}{2}$,

$$a \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b \rightarrow \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \text{ і } a \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + J,$$

де $2 \in J(R)$, J – нерозкладна матриця над радикалом $J(R)$, $J(2 + J) = 0$, а також нерозкладними зображеннями степеня $n > 2$ $a \rightarrow E_n$, $b \rightarrow E_n + J_n$ при $2 \in J(R)$ і $a \rightarrow a_0$, $b \rightarrow b_0$, де J_n – нерозкладна матриця над радикалом $J(R)$, $J_n(2 + J_n) = 0$, а a_0 – корінь многочлена $1 + x^k + \dots + x^{m-k}$, $b_0^2 = 1$, $b_0 a_0 b_0^{-1} = a_0^{-1}$.

Історію питання і попередні результати можна знайти в [1–3], а деякі загальні відомості більш детально викладені в [4–9].

Якщо $n = 2$, то зображення групи D_m , $m > 1$ описані в [10]. Незважаючи на це, у даній роботі будемо вважати, що $n \geq 1$.

Нехай V – лівий R -модуль із скінченим R -базисом, $n = \dim V$, $n \geq 1$, $End(n, V)$ – кільце ендоморфізмів модуля V , $GL(n, V) = End(n, V)^*$ – група автоморфізмів модуля V . У фіксованому базисі модуля V будемо ототожнювати кільце $End(n, V)$ з R_n – кільцем всіх матриць $n \times n$ над R , $GL(n, V)$ з $GL(n, R)$ – групою всіх оборотних матриць кільця R_n . Одиничну матрицю із групи $GL(n, R)$ будемо позначати через E_n або через E або навіть через 1 , якщо із контекста буде зрозуміло про яку одиничну матрицю йде мова.

Будемо використовувати позначення $\bar{R} = R/J(R)$, $\bar{r} = \Lambda_{J(R)} r$, $r \in R$, $\bar{h} = \Lambda_{J(R)} h$, $h \in GL(n, R)$, а також $\bar{\Lambda} = \Lambda_{J(R)} \Lambda$, $\bar{g} = \bar{\Lambda} g$, де $\Lambda : G \rightarrow GL(n, R) \cong GL(n, V)$, $g \in G$, G – група.

Гомоморфізм $i_h : G \rightarrow G$, де $i_h(g) = hgh^{-1}$, $g \in G$ будемо називати внутрішнім автоморфізмом групи G з породжуючим елементом $h \in G$, а елемент $i_h(g)$ визначеним g з точністю до спряження елементом h .

Зображення $\Lambda : G \rightarrow GL(n, R) \cong GL(n, V)$ перетворює лівий R -модуль V у лівий RG -модуль за правилом $gv = \Lambda gv$ для всіх $g \in G$, $v \in V$, яке лінійно продовжується на всі елементи RG . Модуль V будемо називати модулем, у якому реалізується зображення Λ групи G .

Неважно бачити, що у фіксованому скінченому R -базисі модуля V , $n = \dim V$, $n \geq 1$ кільце ендоморфізмів $Hom_{RG}(V, V)$ RG -модуля V можна ототожнити з підкільцем централізатора $C_{R_n}(\Lambda G)$ групи ΛG у кільці R_n .

Під нетривіальними підмодулями деякого модуля будемо розуміти відмінні від нього ненульові підмодулі.

Означення 1. Зображення $\Lambda : G \rightarrow GL(n, V)$, $n \geq 1$ називається звідним, якщо існує нетривіальний RG -підмодуль модуля V із скінченим R -базисом, який можна доповнити до R -базиса модуля V . У протилежному випадку зобра-

ження Λ називається незвідним.

На матричній мові це означає, що зображення $\Lambda : G \rightarrow GL(n, R)$, $n \geq 1$ є звідним, якщо існує матриця $c \in GL(n, R)$ така, що

$$c\Lambda gc^{-1} = \begin{pmatrix} \Lambda_1 g & \Lambda_0 g \\ 0 & \Lambda_2 g \end{pmatrix},$$

де $\Lambda_i g \in GL(n_i, R)$ для всіх $g \in G$, $n = n_1 + n_2$, $n_i < n$, $1 \leq i \leq 2$. Якщо вищевказана матриця c не існує, то таке зображення Λ називається незвідним.

Означення 2. Зображення $\Lambda : G \rightarrow GL(n, V)$, $n \geq 1$ називається незвідним, якщо RG -модуль V не містить нетривіальних RG -підмодулів.

Очевидно, що незвідний модуль за означенням 2 є незвідним і за означенням 1. Навпаки не завжди вірно, хоча над тілами ці поняття співпадають. Адже, якщо зображення Λ є незвідним за означенням 2, то, згідно з лемою Шура, $\text{Hom}_{RG}(V, V)$ – тіло. Тому одномірні зображення довільної групи над кільцями, які не містять тіл, є звідними за означенням 2, хоча за означенням 1 вони є незвідними.

У подальшому під незвідним зображенням, якщо не буде обумовлено протилежне, будемо розуміти незвідне зображення у розумінні означення 1.

Лема 1. Нехай R – комутативне локальне кільце з 1, $t \in R^*$, ε породжує корені t -го степеня із 1, k – порядок ε , $\Lambda_i : D_m \rightarrow GL(2, R)$ – зображення групи діебра D_m , $m > 1$, яке визначене на породжуючих елементах a і b за правилом

$$\Lambda_i a = \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}, \Lambda_i b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1 \leq i \leq k, \varepsilon^i \neq \varepsilon^{-i}$$

і продовжене за мультиплікативністю на всю групу D_m . Тоді Λ_i – незвідне зображення і централізатор $C_{R_2}(\Lambda_i D_m) \cong R$.

Доведення. Як буде показано нижче, корені t -го степеня із 1 кільця R утворюють циклічну групу. Нехай ε – її породжуючий елемент і k – порядок ε . Також буде показано, що $\bar{\varepsilon}$ – первісний корінь k -го степеня із одиниці в полі \bar{R} . Тому $\varepsilon^i - \varepsilon^{-i} \in R^*$ при $\varepsilon^i \neq \varepsilon^{-i}$, $1 \leq i \leq k$.

Очевидно, що $\det \Lambda_i a = 1$. Якби зображення Λ_i було звідним, то існувала б матриця $c \in GL(2, R)$ така, що

$$c\Lambda_i a c^{-1} = \begin{pmatrix} \varepsilon^j & a_0 \\ 0 & \varepsilon^{-j} \end{pmatrix}, c\Lambda_i b c^{-1} = \begin{pmatrix} b_1 & b_0 \\ 0 & b_2 \end{pmatrix}, c = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix},$$

де $1 \leq j \leq k$, b_1, b_2 належать групі R^* , а $c_1, c_2, c_3, c_4, a_0, b_0$ – деякі елементи кільця R .

Неважко бачити, що тоді $c_3 \varepsilon^i = \varepsilon^{-j} c_3$, $c_4 \varepsilon^{-i} = \varepsilon^{-j} c_4$ і $c_4 = b_2 c_3$.

Якщо $c_3 \in J(R)$, то $c_4 \in J(R)$, що протирічить включенню $c \in GL(2, R)$. Тому $c_3 \in R^*$ і $c_4 \in R^*$, $\varepsilon^i = \varepsilon^{-j} = \varepsilon^{-i}$, що протирічить припущенню. Отже, Λ_i при $\varepsilon^i \neq \varepsilon^{-i}$, $1 \leq i \leq k$ є незвідним зображенням.

Легко перевірити, що матриця кільця R_2 , яка комує з $\Lambda_i a$, де $\varepsilon^i \neq \varepsilon^{-i}$ є діагональною матрицею, а діагональна матриця, яка комує з $\Lambda_i b$ є скалярною. Тому централізатор $C_{R_2}(\Lambda_i D_m)$ групи $\Lambda_i D_m$ у кільці R_2 складається із скалярних матриць і, як наслідок, може бути ототожнений з кільцем R .

Означення 3. Зображення $\Lambda : G \rightarrow GL(n, V)$ називається розкладним, якщо RG -модуль V є прямою сумою нетривіальних RG -підмодулів. В против-

ному випадку зображення Λ називається нерозкладним.

Нехай R – локальне кільце з 1, V – вільний лівий R -модуль з скінченим R -базисом, $n = \dim V \geq 1$, G – скінчена група, $\Lambda : G \rightarrow GL(n, V)$ – зображення групи G .

Якщо Λ – розкладне зображення, то за означенням 3, $V = V_1 \oplus V_2$, де V_1, V_2 – нетривіальні RG -модулі. Як відомо, проєктивні модулі над локальними кільцями вільні. Тому V_1 і V_2 – нетривіальні RG -підмодулі модуля V із скінченими R -базисами, які доповнюють R -базиси один одного до R -базиса модуля V .

Аналогічними міркуваннями доводиться, що RG -модуль V є скінченою прямою сумою нерозкладних RG -підмодулів. В такому випадку кажуть, що зображення групи G , яке реалізується у RG -модулі V , породжується нерозкладними зображеннями або по-іншому, що є сумою нерозкладних зображень групи G .

Окрім цього, вищенаведені міркування показують, що над локальними кільцями розкладні зображення звідні. Тому незвідні зображення над локальними кільцями нерозкладні.

Те, що незвідні зображення над локальними кільцями знаходяться серед нерозкладних зображень дає можливість характеризувати їх через ознаки, якими вони виділяються у класі нерозкладних зображень. Тому будемо описувати спочатку нерозкладні зображення, а потім знаходити серед них незвідні зображення.

Якщо порядок групи G є оборотним в кільці R , то, за теоремою Машке, нерозкладні зображення групи G є незвідними.

Таким чином, поняття нерозкладності і незвідності зображень скінченої групи скінченого степеня над локальними кільцями з 1, в яких порядок групи є оборотним, співпадають.

Означення незвідності і нерозкладності зображень груп аналогічним чином формулюються для будь-яких матричних відображень, а значить і для будь-яких матричних множин.

Нехай V і W – ліві вільні R -модулі із скінченими R -базисами, $n = \dim V$, $m = \dim W$.

Як і вище зображення

$$\Lambda_1 : G \rightarrow GL(n, R) \cong GL(n, V), \Lambda_2 : G \rightarrow GL(m, R) \cong GL(m, W)$$

перетворюють ліві R -модулі V і W у ліві RG -модулі.

Означення 4. Зображення Λ_1 і Λ_2 називаються еквівалентними, якщо модулі V і W , в яких вони реалізуються, ізоморфні як RG -модулі. В протилежному випадку зображення Λ_1 і Λ_2 називаються нееквівалентними.

Таким чином, еквівалентність зображень Λ_1 і Λ_2 означає, що існує ізоморфізм $f : V \rightarrow W$ R -модулів V і W такий, що $f(gv) = gf(v)$ для будь-яких $g \in G$ і $v \in V$, тобто $f\Lambda_1g = \Lambda_2gf$ для будь-яких $g \in G$.

Зрозуміло, що із еквівалентності зображень Λ_1 і Λ_2 випливає рівність $n = m$ і у фіксованих базисах V і W мають місце матричні рівності

$$c\Lambda_1gc^{-1} = \Lambda_2g, g \in G,$$

де матриця $c \in GL(n, R)$ відповідає ізоморфізму f . В такому разі будемо казати, що зображення $\Lambda_2 = {}_i c \Lambda_1$ співпадає із зображенням Λ_1 з точністю до еквівалентності.

І навпаки. Із матричної еквівалентності зображень групи G випливає ізо-

морфізм RG -модулів, в яких вони реалізуються.

Лема 2. Нехай R – комутативне локальне кільце з 1, $m \in R^*$, ε породжує корені m -го степеня із 1, k – порядок ε , $\Lambda_i : D_m \rightarrow GL(2, R)$ – зображення групи D_m , $m > 1$, які визначені за правилом

$$\Lambda_i a = \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}, \quad \Lambda_i b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Тоді Λ_i при $1 \leq i < \frac{k}{2}$ є попарно нееквівалентними незвідними зображеннями групи D_m .

Доведення. Оскільки при $1 \leq i < \frac{k}{2}$ має місце нерівність $\varepsilon^i \neq \varepsilon^{-i}$, то, згідно з лемою 1, зображення Λ_i є незвідними і, як наслідок, нерозкладними зображеннями групи D_m , $m > 1$.

Більше того, $\varepsilon^i + \varepsilon^{-i} - (\varepsilon^j + \varepsilon^{-j}) = (\varepsilon^{i+j} - 1)(\varepsilon^{-j} - \varepsilon^{-i}) \in R^*$ при $1 \leq i \neq j < \frac{k}{2}$. Тому $\varepsilon^i + \varepsilon^{-i} \neq \varepsilon^j + \varepsilon^{-j}$. Це означає, що при $1 \leq i \neq j < \frac{k}{2}$ сліди матриць $\Lambda_i a$ і $\Lambda_j a$ є різними. Тому зображення Λ_i , $1 \leq i < \frac{k}{2}$ групи D_m , $m > 1$ є попарно нееквівалентними.

Нехай V – довільний R -модуль над асоціативним кільцем R з 1, σ – довільний ендоморфізм модуля V .

Означення 5. Лишковими підмодулями модуля V ендоморфізма σ будемо називати підмодулі $R(\sigma) = (\sigma - 1)V$ і $P(\sigma) = \ker(\sigma - 1)$.

Зрозуміло, що

$$R(\sigma) = \{(\sigma - 1)v \mid v \in V\} \text{ і } P(\sigma) = \{v \in V \mid \sigma v = v\},$$

а також $R(1 - \sigma) = \sigma V$ і $P(1 - \sigma) = \ker \sigma$.

Легко бачити, що якщо σ – автоморфізм модуля V , то $R(\sigma^{-1}) = R(\sigma)$ і $P(\sigma^{-1}) = P(\sigma)$. Це випливає із рівності $\sigma^{-1} - 1 = (\sigma - 1)(-\sigma^{-1})$.

Якщо g – довільний ендоморфізм модуля V такий, що $g\sigma = \sigma^{\pm 1}g$, то $g(\sigma - 1) = (\sigma^{\pm 1} - 1)g$. Тому

$$gR(\sigma) \subseteq R(\sigma^{\pm 1}) = R(\sigma) \quad \text{і} \quad gP(\sigma) \subseteq P(\sigma^{\pm 1}) = P(\sigma).$$

Зокрема, якщо g – автоморфізм модуля V і $g\sigma = \sigma^{\pm 1}g$, то $g^{-1}\sigma = \sigma^{\pm 1}g^{-1}$ і

$$gR(\sigma) = R(\sigma), \quad gP(\sigma) = P(\sigma).$$

Цей же результат можна отримати із загальних формул

$$gR(\sigma) = R(g\sigma g^{-1}) \quad \text{і} \quad gP(\sigma) = P(g\sigma g^{-1}),$$

які із-за рівності $g\sigma g^{-1} - 1 = g(\sigma - 1)g^{-1}$, справедливі для будь-якого ендоморфізма σ і будь-якого автоморфізма g модуля V .

Мають місце важливі включення

$$R(\sigma_1\sigma_2) \subseteq R(\sigma_1) + R(\sigma_2), \quad P(\sigma_1\sigma_2) \supseteq P(\sigma_1) \cap P(\sigma_2),$$

які випливають із рівностей $\sigma_1\sigma_2 - 1 = (\sigma_1 - 1)\sigma_2 + \sigma_2 - 1 = \sigma_1(\sigma_2 - 1) + \sigma_1 - 1$.

Лема 3. Нехай R – асоціативне кільце з 1, V – лівий R -модуль (не обов'язково вільний), $\sigma \in GL(V)$, $\sigma^m = 1$, $m \in R^*$. Тоді $V = R(\sigma) \oplus P(\sigma)$, де $P(\sigma) = \{v \in V \mid (\sigma - 1)v = 0\}$ і $R(\sigma) = \{v \in V \mid (1 + \sigma + \dots + \sigma^{m-1})v = 0\}$.

Доведення. Нехай $e = (1 + \sigma + \dots + \sigma^{m-1})m^{-1}$. Оскільки $e\sigma^i = \sigma^i e = e$ для всіх $i \geq 0$, то $e^2 = e(1 + \sigma + \dots + \sigma^{m-1})m^{-1} = e$ – ідемпотент і має місце пірсонський розклад $V = eV \oplus (1 - e)V$, де $v = ev + (1 - e)v$, $v \in V$.

Очевидно, що

$$eV = \{v \in V \mid (1 - e)v = 0\} = \ker(1 - e) \text{ і } (1 - e)V = \{v \in V \mid ev = 0\} = \ker e.$$

Оскільки $e(1 - \sigma) = (1 - \sigma)e = 0$ і $1 - e = (1 - \sigma)t$, де $t \in \text{End}V$ і $\sigma t = t\sigma$,

то $eV \subseteq P(\sigma) \subseteq \ker(1 - e) \subseteq eV$ і $(1 - e)V \subseteq R(\sigma) \subseteq \ker e \subseteq (1 - e)V$.

Тим самим доведено, що

$P(\sigma) = eV = \ker(1 - e) = \{v \in V \mid (\sigma - 1)v = 0\}$, $R(\sigma) = (1 - e)V = \ker e = \{v \in V \mid (1 + \sigma + \dots + \sigma^{m-1})v = 0\}$.

Наслідок 2. Нехай R – локальне кільце з $1, 2 \in R^*$, $b \in GL(n, V)$, $b^2 = 1$. Тоді існує базис R -модуля V , в якому b має діагональний вигляд з плюс, мінус одиницями на діагоналі. Число одиниць на діагоналі визначається автоморфізмом b однозначно і дорівнює $\dim P(b)$.

Доведення. Дійсно $e = (1 + b)2^{-1}$, $1 - e = (1 - b)2^{-1}$. Тоді $V = eV \oplus (1 - e)V$, $eV = P(b) = \{v \in V \mid bv = v\}$, $(1 - e)V = \ker e = \{v \in V \mid bv = -v\}$.

Оскільки проєктивні модулі eV і $(1 - e)V$ над локальними кільцями вільні, то існує базис модуля V , який складається із базисів підмодулів eV і $(1 - e)V$, в якому b має діагональний вигляд з плюс, мінус одиницями на діагоналі. Число одиниць на діагоналі b не залежить від вибраного базису і дорівнює $\dim P(b)$. Адже, якщо $g \in GL(n, V)$, то $P(gbg^{-1}) = gP(b)$.

Лема 4. Нехай R – тіло, $\text{char} R = 2$, $b \in GL(n, R) \cong GL(n, V)$, $n \geq 1$, $b^2 = 1$. Тоді, з точністю до спряження,

$$b \sim \begin{pmatrix} E_l & 0 & E_l \\ 0 & E & 0 \\ 0 & 0 & E_l \end{pmatrix}, C_{R_n}(b) \subseteq \left\{ \begin{pmatrix} R_l & * & * \\ 0 & R_{n-2l} & * \\ 0 & 0 & R_l \end{pmatrix} \right\},$$

де E_l означає одиничну матрицю групи $GL(l, R)$, $0 \leq l \leq \frac{n}{2}$, l визначається матрицею b однозначно і дорівнює $\dim R(b)$, $C_{R_n}(b)$ – централізатор b у кільці R_n .

Доведення. Неважко бачити, що $(b - 1)^2 = 0$, $R(b) \subseteq P(b)$. Якщо $b = 1$, то лема 4 має місце при $l = 0$. Нехай $b \neq 1$. Тому $P(b) \neq V$, $R(b) \neq 0$, $P(b) \neq 0$. Нехай $V = P(b) \oplus W$. Тоді $l = \dim W = \dim V - \dim P(b) = \dim R(b)$ – визначається матрицею b однозначно. Очевидно, що

$$R(b) = (b - 1)W, 1 \leq l \leq n - l, bP(b) = P(b), bR(b) = R(b).$$

Нехай e_{n-l+1}, \dots, e_n – базис W . Тоді $e_1 = be_{n-l+1} - e_{n-l+1}, \dots, e_l = be_n - e_n$ – базис $R(b)$. Доповнимо базис e_1, \dots, e_l підпростору $R(b)$ до базиса $e_1, \dots, e_l, e_{l+1}, \dots, e_{n-l}$ простору $P(b)$. В такому разі $e_1, \dots, e_l, e_{l+1}, \dots, e_{n-l}, e_{n-l+1}, \dots, e_n$ – базис простору V , в якому b має шуканий вигляд.

Оскільки з рівності $gb = bg$, де $g \in R_n \cong \text{End}(n, V)$ випливає, що $gR(b) \subseteq R(b)$ і $gP(b) \subseteq P(b)$, то централізатор $C_{R_n}(b)$ має вищевказаний вигляд.

Тим самим лема 4 доведена.

Лема 5. Нехай R – локальне кільце з $1, 2 \in J(R)$, $b \in GL(n, R) \cong GL(n, V)$, $n \geq 1$, $b^2 = 1$. Тоді матриця b спряжена з матрицею

$$b_{l,J} = \text{diag} \left(\underbrace{\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \dots, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}}_{2l}, E + J \right)$$

де $l = \dim R(\bar{b})$, $0 \leq l \leq \frac{n}{2}$ визначається матрицею b однозначно, а J – матриця розмірів $(n - 2l) \times (n - 2l)$ над радикалом $J(R)$, $J(J + 2E) = 0$, яка визначається матрицею b з точністю до спряження.

Доведення. Згідно з лемою 4 $\bar{b} = \bar{1}$ (тоді лема 5 має місце при $l = 0$) або, з точністю до спряження, можна вважати, що

$$b = \begin{pmatrix} E_l & 0 & E_l \\ 0 & E & 0 \\ 0 & 0 & E_l \end{pmatrix} + \begin{pmatrix} J_{11} & J_{12} & J_{13} \\ J_{21} & J_{22} & J_{23} \\ J_{31} & J_{32} & J_{33} \end{pmatrix},$$

де E_l означає одиничну матрицю групи $GL(l, R)$, $1 \leq l \leq \frac{n}{2}$, $l = \dim R(\bar{b})$ визначається матрицею \bar{b} , а значить і матрицею b однозначно, а J_{ij} – матриці відповідних розмірів над $J(R)$, $1 \leq i, j \leq 3$.

Оскільки $E_l + J_{13} \in GL(l, R)$, то, з точністю до спряження матрицею

$$\begin{pmatrix} (E_l + J_{13})^{-1} & 0 & 0 \\ -J_{23}(E_l + J_{13})^{-1} & E & 0 \\ -J_{33}(E_l + J_{13})^{-1} & 0 & E_l \end{pmatrix},$$

можна вважати, що $J_{13} = 0$, $J_{23} = 0$, $J_{33} = 0$. Аналогічно, з точністю до спряження матрицею

$$\begin{pmatrix} E_l & 0 & 0 \\ 0 & E & 0 \\ 0 & J_{12} & E_l \end{pmatrix},$$

можна вважати, що $J_{12} = 0$. З рівності $b^2 = 1$ випливає, що $J_{21} = 0$, $J_{31} = 0$, $J_{32} = 0$, $E_l + J_{11} = -E_l$.

Тим самим доведено, що, з точністю до спряження,

$$b = \begin{pmatrix} -E_l & 0 & E_l \\ 0 & E + J & 0 \\ 0 & 0 & E_l \end{pmatrix}$$

Неважко бачити, що з рівності

$$g \begin{pmatrix} -E_l & 0 & E_l \\ 0 & E + J & 0 \\ 0 & 0 & E_l \end{pmatrix} = \begin{pmatrix} -E_l & 0 & E_l \\ 0 & E + J' & 0 \\ 0 & 0 & E_l \end{pmatrix} g,$$

де J, J' – матриці над $J(R)$, $g = (g_{ij}) \in R_n$, $1 \leq i, j \leq 3$ випливає, що $g_{22}J = J'g_{22}$. За лемою 4 g_{21}, g_{31}, g_{32} – матриці над $J(R)$. Тому, якщо $g \in GL(n, R)$, то $\bar{g} \in GL(n, \bar{R})$, $\overline{g_{22}} \in GL(n - 2l, \bar{R})$, $g_{22} \in GL(n - 2l, R)$. Це означає, що матриця J визначається матрицею b з точністю до спряження.

Більше того, з точністю до спряження матрицями вигляду

$$\text{diag} \left(1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1 \right),$$

матриця b спряжена з матрицею $b_{l,J}$, де l визначається матрицею b однозначно, а матриця J з точністю до спряження.

Наслідок 3. Нехай R – локальне кільце з $1, 2 \in J(R)$, $b \in GL(n, R) \cong GL(n, V)$, $n \geq 1$, $b^2 = 1$, b – нерозкладна матриця. Тоді $\bar{b} = \bar{1}$ або $n = 2$ і матриця b спряжена з нерозкладною матрицею $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$.

Доведення. Нехай $\bar{b} \neq \bar{1}$. Оскільки b – нерозкладна матриця, то, згідно з лемою 5, $l = 1$ і, з точністю до спряження, можна вважати, що $b = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$.

Очевидно, що звідна над кільцем R матриця $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ є нерозкладною над полем \bar{R} і, як наслідок, є нерозкладною над кільцем R .

Зокрема, з наслідку 3 випливає, що над локальними кільцями, в яких елемент два є необоротним, поняття нерозкладних зображень навіть циклічної групи другого порядку є ширшим від поняття їх незвідності.

Нам знадобляться деякі властивості коренів із одиниці у комутативних кільцях.

Означення 6. Нехай G – група, порядки всіх елементів якої обмежені деяким натуральним числом. Найменше спільне кратне порядків всіх елементів групи G будемо називати експонентою групи G і позначати $\exp G$.

Зрозуміло, що в тих випадках, коли мова буде йти про експоненту групи, будемо вважати, що вона існує.

Лема 6. Експонента комутативної групи є найменшим з натуральних чисел, які обмежують порядки всіх елементів групи, тобто співпадає з порядком елемента найвищого порядку групи.

Доведення. Нехай G – комутативна група, порядки всіх елементів якої обмежені деяким натуральним числом і g_0 – елемент групи G найвищого порядку, який позначимо через m_0 . Зрозуміло, що $m_0 \leq \exp G$.

Очевидно, що якщо d є дільником числа m_0 , то елемент $g_0^{\frac{m_0}{d}}$ має порядок d . Тому з існування в групі G елемента, порядок якого не ділить m_0 , випливає, що в G існує елемент h , порядок якого є степінню p^k простого числа p , яка не ділить m_0 . Нехай p^l – найбільша степінь числа p , яка ділить m_0 . Зрозуміло, що $0 \leq l < k$. В такому разі порядки елементів $g_0^{p^l}$ і h є взаємно-простими числами $\frac{m_0}{p^l}$ і p^k відповідно. Тому порядок елемента $g_0^{p^l} \cdot h$ дорівнює $\frac{m_0}{p^l} \cdot p^k \geq m_0 p > m_0$, що протирічить припущенню. Тим самим доведено, що порядки всіх елементів групи G ділять m_0 . Тому $g^{m_0} = 1$ для всіх $g \in G$, $\exp G \leq m_0$ і, як наслідок, $m_0 = \exp G$.

Відмітимо, що скінчена комутативна група G є циклічною тоді і тільки тоді, коли $|G| = m_0$, а значить тоді і тільки тоді, коли $|G| = \exp G$.

Наслідок 4. Нехай R – комутативне кільце з 1 без дільників нуля, G – підгрупа групи R^* експоненти $\exp G$. Тоді G – скінчена циклічна група, порядок якої $|G| = \exp G$.

Доведення. Нехай, як і в лемі 6, g_0 – елемент найвищого порядку m_0 групи G . Згідно з лемою 6 $m_0 = \exp G$ і $g^{m_0} = 1$ для всіх $g \in G$. Тому елементи групи G є коренями двочлена

$$x^{m_0} - 1 = (x - 1)(x - g_0) \cdots (x - g_0^{m_0-1}).$$

Оскільки в R не має дільників нуля, то $G = \langle g_0 \rangle$ – скінчена циклічна група, яка породжена елементом g_0 і $|G| = m_0 = \exp G$.

Зокрема, якщо G – група коренів m -го степеня із 1 в комутативному кільці R , яке не містить дільників нуля, то $|G| = m_0 = \exp G \leq m$.

Означення 7. Елементи кільця R , які є коренями k -го степеня із 1 і мають порядок k , називаються первісними коренями k -го степеня із 1.

Якщо ε – первісний корінь k -го степеня із 1 комутативного кільця R , яке не

містить дільників нуля, то всі елементи $1, \varepsilon, \dots, \varepsilon^{k-1}$ – різні і, згідно з наслідком 3, ε породжує всі корені k -го степеня із 1 кільця R .

Більше того, якщо a – довільний корінь m -го степеня із 1 кільця R і k ділить m , то $a^{\frac{m}{k}} \in \langle \varepsilon \rangle$.

Лема 7. Нехай R – комутативне кільце з 1, $m \in R^*$, кільце $\bar{R} = R/J(R)$ не містить дільників нуля, G – група всіх коренів m -го степеня із 1 кільця R . Тоді G – скінчена циклічна група, порядок якої $|G|$ є дільником числа m .

Доведення. Нехай G – група всіх коренів m -го степеня із 1. Тоді \bar{G} – підгрупа групи всіх коренів m -го степеня із 1 кільця \bar{R} , яка, згідно з наслідком 3, є скінченою циклічною групою. Тому $\bar{G} = \langle \bar{\varepsilon} \rangle$, де ε – деякий корінь m -го степеня із 1, $|\bar{G}| \leq m$.

Виявляється, що порядки елементів ε і $\bar{\varepsilon}$ співпадають. Адже, якщо $\bar{\varepsilon}^l = \bar{1}$, то $\varepsilon^l = 1 + j$, де $j \in J(R)$. З рівності $\varepsilon^m = 1$ випливає, що $(1 + j)^m = 1$. Тому $mj + j^2r = 0$, де r – деякий елемент кільця R . За умовою $m + jr \in R^*$. Тому $j = 0$, $\varepsilon^l = 1$. Отже, з $\bar{\varepsilon}^l = \bar{1}$ випливає, що $\varepsilon^l = 1$. Навпаки очевидно. Тим самим доведено, що порядки елементів ε і $\bar{\varepsilon}$ рівні.

Доведемо, що $G = \langle \varepsilon \rangle$. Дійсно, якщо a – довільний корінь m -го степеня із 1 кільця R , то $\bar{a} = \bar{\varepsilon}^i$, де $1 \leq i \leq |\bar{G}|$. Тому $a\varepsilon^{-i}$ – корінь m -го степеня із 1, який належить $1 + J(R)$. Згідно з вищедоведеним, $a\varepsilon^{-i} = 1$. Тому $a = \varepsilon^i$. Це означає, що $G = \langle \varepsilon \rangle$ і $|G| = |\bar{G}| \leq m$.

Нехай k – порядок елемента ε . Зрозуміло, що k ділить m і ε – первісний корінь k -го степеня із 1, який породжує всі корені m -го степеня із 1 кільця R .

Тому, якщо k' – довільний дільник числа m , то будь-який корінь k' -го степеня із 1 є коренем m -го степеня із 1 і, як наслідок, коренем k -го степеня із 1.

Оскільки k – порядок елемента $\bar{\varepsilon}$, то $\bar{\varepsilon}$ – первісний корінь k -го степеня із 1 і $\varepsilon^i - \varepsilon^j \notin J(R)$ для всіх $1 \leq i \neq j \leq k$.

Зокрема, якщо R – комутативне локальне кільце з 1, $m \in R^*$, ε породжує корені m -го степеня із 1 кільця R , k – порядок ε , то k ділить m і $\varepsilon^i - \varepsilon^j \in R^*$ для всіх $1 \leq i \neq j \leq k$.

Зауважимо, що в будь-якому полі тільки ± 1 є коренями другого степеня із 1. Тому, якщо в комутативному локальному кільці R з 1 елемент $2 \in R^*$, то -1 породжує всі корені 2-го степеня із 1 кільця R .

Лема 8. Нехай R – комутативне локальне кільце з 1, $m \in R^*$, ε породжує корені m -го степеня із 1 кільця R , k – порядок ε , $\sigma \in GL(n, R) \cong GL(n, V)$, $n \geq 1$, $\sigma^m = 1$. Тоді, з точністю до спряження, σ – діагональний елемент з степенями ε на діагоналі, кратність входження яких визначається σ однозначно і елемента σ_0 , що є коренем многочлена $1 + x^k + \dots + x^{m-k}$ і будь-яка степінь $\bar{\sigma}_0$, показник якої є взаємно-простим з числом m , не має власних значень над полем \bar{R} .

Якщо $g \in GL(n, R) \cong GL(n, V)$ і $g\sigma g^{-1} = \sigma^{-1}$, то мають місце рівності $gP(\varepsilon^{-i}\sigma) = P(\varepsilon^{-(k-i)}\sigma)$, $gR(\varepsilon^{-i}\sigma) = R(\varepsilon^{-(k-i)}\sigma)$ для всіх $0 \leq i \leq k$.

Доведення. Індукцією по l покажемо, що при $1 \leq l \leq k$ має місце розклад

$$V = P(\varepsilon^{-1}\sigma) \oplus \dots \oplus P(\varepsilon^{-l}\sigma) \oplus R(\varepsilon^{-1}\sigma) \bigcap \dots \bigcap R(\varepsilon^{-l}\sigma).$$

При $l = 1$ даний розклад $V = P(\varepsilon^{-1}\sigma) \oplus R(\varepsilon^{-1}\sigma)$ випливає із леми 3. Припу-

стимо, що розклад модуля V має місце при $l < k$ і доведемо його при $l + 1$.

Як відмічалось вище, лишкові підмодулі елементів $\varepsilon^{-i}\sigma$, $1 \leq i \leq k$ інваріантні відносно σ і, згідно з лемою 3, має місце розклад підмодуля

$$W = R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-l}\sigma) = P(\varepsilon^{-l-1}\sigma) \cap W \oplus R(\varepsilon^{-l-1}\sigma) \cap W.$$

Доведемо, що має місце включення $P(\varepsilon^{-l-1}\sigma) \subseteq W$. Адже, якщо v_0 – довільний елемент підмодуля $P(\varepsilon^{-l-1}\sigma)$, то $\sigma v_0 = \varepsilon^{l+1}v_0$. Неважко бачити, що $1 \leq -i + l + 1 \leq l < k$ для всіх $1 \leq i \leq l$. Тому $1 - \varepsilon^{-i+l+1} \in R^*$, $1 + \varepsilon^{-i+l+1} + \dots + (\varepsilon^{-i+l+1})^{m-1} = 0$, $(1 + \varepsilon^{-i}\sigma + \dots + (\varepsilon^{-i}\sigma)^{m-1})v_0 = 0$, $v_0 \in W$.

Тим самим доведено, що $P(\varepsilon^{-l-1}\sigma) \cap W = P(\varepsilon^{-l-1}\sigma)$, а з нею і твердження індукції. Зокрема, при $l = k$ має місце розклад

$$V = P(\varepsilon^{-1}\sigma) \oplus \dots \oplus P(\varepsilon^{-k}\sigma) \oplus R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma).$$

Оскільки проективні модулі над локальними кільцями вільні, то $P(\varepsilon^{-1}\sigma)$, \dots , $P(\varepsilon^{-k}\sigma)$, $R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma)$ – вільні підмодулі модуля V .

Зафіксуємо базис модуля V , який складається із базисів підмодулів

$$P(\varepsilon^{-1}\sigma), \dots, P(\varepsilon^{-k}\sigma), R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma).$$

У цьому базисі елемент σ має вигляд

$$\sigma = \text{diag} \left(\underbrace{\varepsilon, \dots, \varepsilon}_{n_1}, \dots, \underbrace{\varepsilon^k, \dots, \varepsilon^k}_{n_k}, \sigma_0 \right),$$

де $n_i = \dim P(\varepsilon^{-i}\sigma)$, $1 \leq i \leq k$, $n_0 = \dim R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma)$, $n = n_0 + n_1 + \dots + n_k$ і σ_0 – звуження σ на $R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma)$.

Безпосередньою перевіркою встановлюємо, що

$$1 + \varepsilon^{-i}\sigma + \dots + (\varepsilon^{-i}\sigma)^{m-1} = \left(1 + \varepsilon^{-i}\sigma + \dots + (\varepsilon^{-i}\sigma)^{k-1}\right) (1 + \sigma^k + \dots + \sigma^{m-k})$$

для всіх $1 \leq i \leq k$. Покажемо, що $1 + \sigma_0^k + \dots + \sigma_0^{m-k} = 0$. Нехай v' – довільний елемент підмодуля $R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma)$, $v = (1 + \sigma^k + \dots + \sigma^{m-k})v'$. За припущенням

$$\begin{cases} (1 + \varepsilon^{-1}\sigma + \dots + (\varepsilon^{-1}\sigma)^{m-1})v' = 0 \\ \dots \\ (1 + \varepsilon^{-k}\sigma + \dots + (\varepsilon^{-k}\sigma)^{m-1})v' = 0 \end{cases},$$

Дану систему можна записати у вигляді матричної рівності $TL = 0$, де

$$T = \begin{pmatrix} 1 & \varepsilon^{-1} & \dots & (\varepsilon^{-1})^{k-1} \\ \dots & \dots & \dots & \dots \\ 1 & \varepsilon^{-k} & \dots & (\varepsilon^{-k})^{k-1} \end{pmatrix}, L = \begin{pmatrix} v \\ \vdots \\ \sigma^{k-1}v \end{pmatrix}.$$

Оскільки визначник матриці T є визначником Вандермонда $\det T = \prod_{1 \leq i < j \leq k} (\varepsilon^{-j} - \varepsilon^{-i}) \in$

R^* , то $L = 0$, $v = 0$. Тим самим доведено, що

$$1 + \sigma_0^k + \dots + \sigma_0^{m-k} = (1 + \sigma^k + \dots + \sigma^{m-k})|_{R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma)} = 0.$$

Покажемо, що $\bar{\sigma}_0$ не має власних значень над полем \bar{R} .

Припустимо, що $\bar{\lambda}$ – деяке власне значення елемента $\bar{\sigma}_0$ над полем \bar{R} . Тоді $\bar{\lambda}$ – корінь m -го степеня із $\bar{1}$, який породжується коренем k -го степеня із $\bar{1}$. Тому $\bar{\lambda}^k = \bar{1}$. Оскільки $m - k = \left(\frac{m}{k} - 1\right)k$, то сума $1 + \sigma_0^k + \dots + \sigma_0^{m-k}$ містить $\frac{m}{k}$ доданків. Це означає, що $\frac{m}{k} \cdot \bar{1} = \bar{0}$, що протирічить включенню $\frac{m}{k} \in R^*$.

Тим самим доведено, що $\overline{\sigma}_0$ не має власних значень над полем \overline{R} . Зокрема σ_0 не є одномірною матрицею, а також звідною двомірною або тримірною матрицею.

Якщо m' – натуральне число, яке взаємно-просте з числом m , то $\overline{\sigma}_0$ породжується $\overline{\sigma}_0^{m'}$. Тому $\overline{\sigma}_0^{m'}$ не має власних значень над полем \overline{R} .

Характеристичний многочлен матриці σ має вигляд $f(x) = \prod_{i=1}^k (x - \varepsilon^i)^{n_i} f_0(x)$, де $n_i = \dim P(\varepsilon^{-i}\sigma)$, $1 \leq i \leq k$ – кратність входження кореня ε^i в розкладі σ , матриця σ_0 і, як наслідок, $f_0(x) = \det(xE - \sigma_0)$ – характеристичний многочлен матриці σ_0 , визначаються σ однозначно, степінь многочлена $f_0(x)$ співпадає з n_0 .

Зрозуміло, що n_0, n_1, \dots, n_k – невід'ємні цілі числа і якщо деяке з них дорівнює нулю, то відповідний підмодуль у розкладі модуля V і, як наслідок, відповідна складова у розкладі елемента σ , відсутні.

Нехай g – автоморфізм модуля V такий, що $g\sigma g^{-1} = \sigma^{-1}$. Неважко бачити, що

$$gP(\varepsilon^{-i}\sigma) = P(\varepsilon^{-i}\sigma^{-1}) = P((\varepsilon^{-i}\sigma^{-1})^{-1}) = P(\varepsilon^i\sigma) \text{ для всіх } 1 \leq i \leq k.$$

Аналогічно $gR(\varepsilon^{-i}\sigma) = R(\varepsilon^i\sigma)$ для всіх $1 \leq i \leq k$. З рівності $\varepsilon^i = \varepsilon^{-(k-i)}$ випливає, що

$$P(\varepsilon^i\sigma) = P(\varepsilon^{-(k-i)}\sigma) \text{ і } R(\varepsilon^i\sigma) = R(\varepsilon^{-(k-i)}\sigma).$$

$$\text{Тому } gP(\varepsilon^{-i}\sigma) = P(\varepsilon^{-(k-i)}\sigma) \text{ для всіх } 1 \leq i \leq k \text{ і } g(R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma)) = R(\varepsilon\sigma) \cap \dots \cap R(\varepsilon^k\sigma) = R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma).$$

З вищедоведеного випливає, що $n_i = n_{k-i}$ для всіх $1 \leq i < k$.

У зафіксованому базисі модуля V елементи σ і g мають вигляд

$$\sigma = \text{diag} \left(\underbrace{\varepsilon, \dots, \varepsilon}_{n_1}, \dots, \underbrace{\varepsilon^k, \dots, \varepsilon^k}_{n_k}, \sigma_0 \right), \quad g = \begin{pmatrix} & & & g_{k-1} \\ & & \ddots & \\ & & & \\ g_1 & & & \\ & & & g_k \\ & & & \\ & & & g_0 \end{pmatrix},$$

де $g_i \in GL(n_i, R)$ – матриці ізоморфізмів $g_i : P(\varepsilon^{-i}\sigma) \rightarrow P(\varepsilon^{-(k-i)}\sigma)$, $1 \leq i \leq k$, які індуковані автоморфізмом g , $g_0 = g|_{R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma)} \in GL(n_0, R)$.

Відмітимо, що комутативне локальне кільце R з 1, $m \in R^*$ не містить нетривіальних коренів m -го степеня із 1 тоді і тільки тоді, коли $k = 1$. Якщо $k = 1$, то, з точністю до спряження,

$$\sigma = \text{diag} \left(\underbrace{1, \dots, 1}_{n_1}, \sigma_0 \right), \quad g = \text{diag}(g_1, g_0),$$

де $1 + \sigma_0 + \dots + \sigma_0^{m-1} = 0$, $g_0\sigma_0g_0^{-1} = \sigma_0^{-1}$.

З другого боку комутативне кільце R з 1 містить первісний корінь m -го степеня із 1 тоді і тільки тоді, коли $k = m$. Якщо $k = m$ і ε – первісний корінь m -го степеня із 1, то $1 + \sigma_0^k + \dots + \sigma_0^{m-k} = 1$, $R(\varepsilon^{-1}\sigma) \cap \dots \cap R(\varepsilon^{-k}\sigma) = 0$ і елементи σ_0 , g_0 у відповідних розкладах елементів σ і g відсутні.

Наслідок 5. В умовах лема 8, елемент σ , з точністю до спряження, є діагональним елементом з матрицями на діагоналі, будь-яка степінь яких є скалярною матрицею або коренем многочлена $1 + x^k + \dots + x^{m-k}$.

якщо k – непарне число, а також

$$\Lambda a = \text{diag} \left(\underbrace{\varepsilon, \dots, \varepsilon}_{n_1}, \dots, \underbrace{\varepsilon^k, \dots, \varepsilon^k}_{n_k}, a_0 \right),$$

$$\Lambda b = \begin{pmatrix} & & & & E_{n_{k-1}} \\ & & & \dots & \\ & & & \dots & \\ & & & b_{\frac{k}{2}} & \\ & & \dots & & \\ E_{n_1} & & & & \\ & & & & b_k \\ & & & & b_0 \end{pmatrix},$$

якщо k – парне число.

Спряженням матрицями вигляду $\text{diag} \left(1, \dots, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, 1, \dots, 1 \right)$ неважко добитися, щоб при непарному k

$$\Lambda a = \text{diag} \left(\underbrace{\varepsilon, \varepsilon^{-1}, \dots, \varepsilon, \varepsilon^{-1}}_{2n_1}, \dots, \underbrace{\varepsilon^t, \varepsilon^{-t}, \dots, \varepsilon^t, \varepsilon^{-t}}_{2n_t}, \underbrace{1, \dots, 1}_{n_k}, a_0 \right),$$

$$\Lambda b = \text{diag} \left(\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{n-n_k-n_0}, b_k, b_0 \right),$$

а при парному k

$$\Lambda a = \text{diag} \left(\underbrace{\varepsilon, \varepsilon^{-1}, \dots, \varepsilon, \varepsilon^{-1}}_{2n_1}, \dots, \underbrace{\varepsilon^t, \varepsilon^{-t}, \dots, \varepsilon^t, \varepsilon^{-t}}_{2n_t}, \underbrace{\varepsilon^{\frac{k}{2}}, \dots, \varepsilon^{\frac{k}{2}}}_{n_{\frac{k}{2}}}, \underbrace{1, \dots, 1}_{n_k}, a_0 \right),$$

$$\Lambda b = \text{diag} \left(\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{n-n_{\frac{k}{2}}-n_k-n_0}, b_{\frac{k}{2}}, b_k, b_0 \right).$$

Тим самим доведено, що

$$\Lambda = n_1 \Lambda_1 + \dots + n_t \Lambda_t + \Lambda_{\frac{k}{2}} + \Lambda_k + \Lambda_0,$$

де n_i , $1 \leq i \leq t$ і степені зображень $\Lambda_{\frac{k}{2}}$ (при парному k), Λ_k і Λ_0 визначаються матрицею Λa і, як наслідок, зображенням Λ однозначно. Адже, n_i – це кратність кореня ε^i , $1 \leq i \leq t$, а степені зображень $\Lambda_{\frac{k}{2}}$ (при парному k) і Λ_k – це кратність коренів $\varepsilon^{\frac{k}{2}}$ і $\varepsilon^k = 1$ у розкладі матриці Λa відповідно, степінь зображення Λ_0 – число n_0 однозначно визначається рівністю $n = 2(n_1 + \dots + n_t) + n_{\frac{k}{2}} + n_k + n_0$.

Деякі з чисел n_1, \dots, n_t і степенів зображень $\Lambda_{\frac{k}{2}}$ (при парному k), Λ_k і Λ_0 можуть бути нульовими. В такому разі відповідні зображення у розкладі зображення Λ відсутні.

Зокрема, якщо в теоремі 1 $k = 1$ (тобто коли R не містить нетривіальних коренів m -го степеня із 1) або коли $k = m$ (тобто коли R містить первісний корінь m -го степеня із 1), то $\Lambda_1, \dots, \Lambda_t, \Lambda_{\frac{k}{2}}$ і відповідно Λ_0 у розкладі зображення Λ відсутні.

Наслідок 6. В умовах теореми 1 зображення Λ є незвідним (нерозкладним) тоді і тільки тоді, коли Λ , з точністю до еквівалентності, співпадає з зображенням типу Λ_i , $1 \leq i \leq t$ або з одним із незвідних (нерозкладних) зображень типу $\Lambda_{\frac{k}{2}}$ (при парному k), Λ_k , Λ_0 (при $1 \leq k < t$).

Доведення. Нехай Λ – незвідне зображення. Тоді Λ – нерозкладне зображення і всі числа n_1, \dots, n_t і степені зображень $\Lambda_{\frac{k}{2}}$ (при парному k), Λ_k і Λ_0 дорівнюють нулеві, за винятком одного з них. Зрозуміло, що якщо $n_i \neq 0$, $1 \leq i \leq t$, то $n_i = 1$, а якщо степені зображення $\Lambda_{\frac{k}{2}}$ (при парному k) або степені зображення Λ_k відмінна від нуля, то $\Lambda_{\frac{k}{2}}b$ або $\Lambda_k b$ є відповідно незвідними (нерозкладними) матрицями.

Незвідність (нерозкладність) зображень Λ_i , $1 \leq i \leq t$ впливає із леми 1, а зображень $\Lambda_{\frac{k}{2}}$ і Λ_k з того, що $\Lambda_{\frac{k}{2}}a$ і $\Lambda_k a$ є скалярними матрицями, а $\Lambda_{\frac{k}{2}}b$ і $\Lambda_k b$ є відповідно незвідними (нерозкладними) матрицями.

Вивчення питання про вигляд, існування, нерозкладність і незвідність зображень типу Λ_0 є значно складнішим і потребує окремого дослідження. Тому в даній роботі ці питання розглядаються тільки при $n = 2$.

Нехай $\Lambda_{k,n} : D_m \rightarrow GL(n, R)$ – зображення групи D_m , $m > 1$ степеня $n \geq 1$, яке задається за правилом

$$\Lambda_{k,n}a = E_n, \quad \Lambda_{k,n}b = E_n + J_n,$$

де J_n – матриця $n \times n$ над радикалом $J(R)$, $J_n(2 + J_n) = 0$.

Зрозуміло, що зображення $\Lambda_{k,n}$ знаходяться серед зображень типу Λ_k і $J_n = 0$ при $2 \in R^*$. Тому зображення $\Lambda_{k,n}$ будемо розглядати виключно при $2 \in J(R)$.

Має місце

Теорема 2. Нехай R – комутативне локальне кільце з 1 , $m \in R^*$, ε – порядок корені m -го степеня із 1 , k – порядок ε , $D_m = \langle a, b \mid a^m = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$ – група діедра. Нерозкладними попарно-нееквівалентними зображеннями групи D_m , $m > 1$, з точністю до еквівалентності, є одномірні зображення типу $\Lambda_{\frac{k}{2}}$ (при парному k) і Λ_k

$$\Lambda_{\frac{k}{2}}a = \varepsilon^{\frac{k}{2}}, \quad \Lambda_{\frac{k}{2}}b = \pm 1 \quad \text{і} \quad \Lambda_k a = 1, \quad \Lambda_k b = \alpha, \quad \alpha^2 = 1,$$

двомірні зображення типу Λ_i , $1 \leq i < \frac{k}{2}$ і Λ_k , $\Lambda_{k,2}$, Λ_0 (при $1 \leq k < m$),

$$\Lambda_i a = \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}, \quad \Lambda_i b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{і} \quad \Lambda_0 a = \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}, \quad \Lambda_0 b = \pm \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix},$$

де $r \in R$, тричлен $x^2 - rx + 1$ ділить без остачі двочлен $x^m - 1$, $r \neq \varepsilon^i + \varepsilon^{-i}$ для всіх $1 \leq i < \frac{k}{2}$,

$$\Lambda_k a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \Lambda_k b = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{і} \quad \Lambda_{k,2} a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \Lambda_{k,2} b = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + J_2,$$

де $2 \in J(R)$, J_2 – нерозкладна матриця над радикалом $J(R)$, $J_2(2 + J_2) = 0$, а також нерозкладні зображення степеня $n > 2$ типу $\Lambda_{k,n}$ і типу Λ_0 (при $1 \leq k < m$)

$$\Lambda_{k,n}a = E_n, \quad \Lambda_{k,n}b = E_n + J_n \quad \text{і} \quad \Lambda_0 a = a_0, \quad \Lambda_0 b = b_0,$$

де J_n – нерозкладна матриця над радикалом $J(R)$, $J_n(2 + J_n) = 0$, a_0 – корінь многочлена $1 + x^k + \dots + x^{m-k}$, $b_0^2 = 1$, $b_0 a_0 b_0^{-1} = a_0^{-1}$.

Незвідними серед вищеописаних нерозкладних зображень групи D_m , $m > 1$ є одномірні зображення, а також двомірні зображення типу Λ_i , $1 \leq i < \frac{k}{2}$, зображення типу $\Lambda_{k,n}$, де $n \geq 2$, J_n – незвідна матриця і незвідні зображення

типу Λ_0 .

Доведення. Згідно з теоремою 1 і її наслідком 5, нерозкладні зображення групи D_m , $m > 1$ слід шукати серед нерозкладних зображень типу

$$\Lambda_i, 1 \leq i < \frac{k}{2}, \Lambda_{\frac{k}{2}} \text{ (при парному } k), \Lambda_k \text{ і } \Lambda_0 \text{ (при } 1 \leq k < m).$$

Зображення типу Λ_i , $1 \leq i < \frac{k}{2}$, згідно з лемами 1 і 2, є незвідними і, як наслідок, нерозкладними попарно-нееквівалентними між собою зображеннями групи D_m , $m > 1$.

Більше того, $\Lambda_i a$, $1 \leq i < \frac{k}{2}$ – нескалярні діагональні матриці, елементи $\Lambda_{\frac{k}{2}} a$ (при парному k) і $\Lambda_k a$ є різними скалярними матрицями, а матриця $\Lambda_0 a$ не має власних значень в кільці R . Тому зображення

$$\Lambda_i, 1 \leq i < \frac{k}{2}, \Lambda_{\frac{k}{2}} \text{ (при парному } k), \Lambda_k \text{ і } \Lambda_0 \text{ (при } 1 \leq k < m)$$

є попарно-нееквівалентними.

Зрозуміло, що зображення $\Lambda_{\frac{k}{2}}$ і Λ_k є нерозкладними і незвідними тоді і тільки тоді, коли матриці $\Lambda_{\frac{k}{2}} b$ і $\Lambda_k b$ є відповідно нерозкладними і незвідними.

Нехай $2 \in R^*$. Тоді -1 породжує корені 2-го степеня із 1, $\varepsilon^{\frac{k}{2}} = \pm 1$. Згідно з наслідком 1, нерозкладні матриці $\Lambda_{\frac{k}{2}} b$ (при парному k) і $\Lambda_k b$ є одномірними плюс, мінус одиницями. Тому нерозкладні зображення типу $\Lambda_{\frac{k}{2}}$ (при парному k) і Λ_k є одномірними зображеннями і $\Lambda_{\frac{k}{2}} a = \varepsilon^{\frac{k}{2}} = \pm 1$, $\Lambda_{\frac{k}{2}} b = \pm 1$, $\Lambda_k a = 1$, $\Lambda_k b = \pm 1$.

Таким чином, у випадку $2 \in R^*$, група D_m , $m > 1$ має нерозкладними (а значить незвідними із-за $|D_m| = 2m \in R^*$) чотири одномірні зображення типу $\Lambda_{\frac{k}{2}}$ і Λ_k при парному k (що має місце тільки при парному m) і два одномірні зображення типу Λ_k при непарному k . Решту нерозкладних зображень складають двомірні зображення типу Λ_i , $1 \leq i < \frac{k}{2}$ і незвідні зображення степеня $n \geq 2$ типу Λ_0 .

Нехай $2 \in J(R)$. Оскільки $m \in R^*$, то m і, як наслідок, k – непарні числа. Тому зображення $\Lambda_{\frac{k}{2}}$ не існує. З'ясуємо умови, при яких $\Lambda_k b$ – нерозкладна і незвідна матриця.

Згідно з лемою 5 і її наслідком 2, достатньо розглянути випадки, коли

$$\Lambda_k \bar{b} = \overline{E_n} \text{ або } \Lambda_k b = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

У першому з них Λ_k співпадає із зображенням типу $\Lambda_{k,n}$, $n \geq 1$, де J_n – нерозкладна матриця над $J(R)$.

У другому випадку Λ_k є двомірним зображенням, яке задається за правилом

$$\Lambda_k a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \Lambda_k b = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Зрозуміло, що, із-за $\overline{\Lambda_k b} \neq \bar{1}$, елемент $\Lambda_k b$ є нерозкладною, хоча і звідною матрицею.

Таким чином, при $2 \in J(R)$ група D_m , $m > 1$ має нерозкладними одномірні зображення типу $\Lambda_{k,1}$, двомірні зображення типу Λ_i , $1 \leq i < \frac{k}{2}$ і типу $\Lambda_{k,2}$, Λ_k і Λ_0 . Решту нерозкладних зображень складають нерозкладні зображення степеня $n > 2$ типу $\Lambda_{k,n}$ і Λ_0 .

Незвідними серед них є одномірні зображення і двомірні зображення типу Λ_i , $1 \leq i < \frac{k}{2}$, $\Lambda_{k,2}$, якщо J_2 – незвідна матриця, а також незвідні зображення типу Λ_0 . Решту незвідних зображень степеня $n > 2$ складають незвідні зобра-

ження типу $\Lambda_{k,n}$ і Λ_0 .

Опишемо, з точністю до еквівалентності, двомірні зображення групи D_m , $m > 1$ типу Λ_0 . Згідно з лемою 8 матриця $\Lambda_0 a$ не має власних значень і тому є нескаларною матрицею. Всі двомірні зображення, які відображають елемент a в нескаларну за модулем радикалу матрицю, описані в [7].

Оскільки $m \in R^*$, то $2 \in R^*$ або m – непарне число. В обох випадках, згідно з [7], з точністю до еквівалентності, мають місце рівності

$$\Lambda_0 a = \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}, \quad \Lambda_0 b = \pm \begin{pmatrix} -1 & 0 \\ r & 1 \end{pmatrix},$$

де r – деякий елемент кільця R такий, що тричлен $x^2 - rx + 1$ ділить без остачі двочлен $x^m - 1$.

Нехай $r = \varepsilon^i + \varepsilon^{-i}$ для деякого $1 \leq i < \frac{k}{2}$. Оскільки $\bar{\varepsilon}^i \neq \bar{\varepsilon}^{-i}$, то $x - \bar{\varepsilon}^i$ – взаємно-прості лінійні двочлени, які ділять без остачі двочлен $x^k - \bar{1}$. Тому тричлен $x^2 - \bar{r}x + \bar{1} = (x - \bar{\varepsilon}^i)(x - \bar{\varepsilon}^{-i})$ ділить без остачі двочлен $x^k - \bar{1}$. Це означає, що $\overline{\Lambda_0 a^k} = \bar{1}$ і, як наслідок, $\frac{m}{k} \cdot \bar{1} = \bar{0}$, що протирічить включенню $\frac{m}{k} \in R^*$. Тим самим доведено, що $r \neq \varepsilon^i + \varepsilon^{-i}$ для всіх $1 \leq i < \frac{k}{2}$.

Вірно і навпаки. Нехай $r \neq \varepsilon^i + \varepsilon^{-i}$ для всіх $1 \leq i < \frac{k}{2}$. Нескалярна матриця $\Lambda_0 a$, через накладені на $r = \text{tr} \Lambda_0 a$ умови, не є спряженою з матрицею вигляду $\text{diag}(\varepsilon^i, \varepsilon^{-i})$ для будь-якого $1 \leq i < \frac{k}{2}$. Оскільки $\det \Lambda_0 a = 1$, то $\Lambda_0 a$ є незвідною матрицею і, згідно з лемою 8, є коренем многочлена $1 + x^k + \dots + x^{m-k}$. Тому зображення $\Lambda_0 a$ є незвідним, а значить і нерозкладним.

Зауважимо, що умови, які визначають при $m \in R^*$ двомірні зображення типу Λ_0 , існують. Наприклад, при $m = 6$, $k = 3$, $r = 1$. Адже, тоді $\varepsilon^3 = 1$, $\varepsilon + \varepsilon^{-1} = \varepsilon + \varepsilon^2 = -1 \neq 1$, тричлен $x^2 - x + 1$ ділить без остачі двочлен $x^6 - 1$.

Теорема 3. *Нехай R -комутативне локальне кільце з 1, $m \in R^*$, ε породжує корені m -го степеня із 1 кільця R , k - порядок ε . Зображення $\Lambda : D_m \rightarrow GL(n, R)$, $\Lambda' : D_m \rightarrow GL(n, R)$ вигляду*

$\Lambda = n_1 \Lambda_1 + \dots + n_t \Lambda_t + \Lambda_{\frac{k}{2}} + \Lambda_k + \Lambda_0$, $\Lambda' = n'_1 \Lambda_1 + \dots + n'_t \Lambda_t + \Lambda'_{\frac{k}{2}} + \Lambda'_k + \Lambda'_0$ еквівалентні тоді і тільки тоді, коли $n_i = n'_i$ для всіх $1 \leq i \leq t$ і матриці $\Lambda_{\frac{k}{2}} b$ і $\Lambda'_{\frac{k}{2}} b$ (при парному k), $\Lambda_k b$ і $\Lambda'_k b$ є відповідно спряженими, а зображення Λ_0 і Λ'_0 еквівалентними.

Доведення. Нехай зображення Λ і Λ' еквівалентні. Це означає, що існує матриця $c \in GL(n, R)$ така, що $i_c \Lambda = \Lambda'$, тобто

$$c \Lambda a c^{-1} = \Lambda' a \quad \text{і} \quad c \Lambda b c^{-1} = \Lambda' b.$$

Оскільки $c P(\varepsilon^{-i} \Lambda a) = P(\varepsilon^{-i} \Lambda' a)$ і $c R(\varepsilon^{-i} \Lambda a) = R(\varepsilon^{-i} \Lambda' a)$, $1 \leq i \leq k$, то кратності входження степенів первісного кореня ε у розкладах матриць Λa і $\Lambda' a$ співпадають. Тоді $n'_1 = n_1, \dots, n'_t = n_t$, степені зображень $\Lambda_{\frac{k}{2}}$ і $\Lambda'_{\frac{k}{2}}$ (при парному k), Λ_k і Λ'_k і, як наслідок, Λ_0 і Λ'_0 відповідно співпадають. Це означає, що $P(\varepsilon^{-i} \Lambda' a) = P(\varepsilon^{-i} \Lambda a)$, $1 \leq i \leq k$ і $R(\varepsilon^{-1} \Lambda a) \cap \dots \cap R(\varepsilon^{-k} \Lambda a) = R(\varepsilon^{-1} \Lambda' a) \cap \dots \cap R(\varepsilon^{-k} \Lambda' a)$. Більше того, з рівності $c \Lambda a c^{-1} = \Lambda' a$ випливає, що $c = \text{diag}(c', c_0)$, де $c_0 \in GL(n_0, R)$ і на підмодулі $P(\varepsilon^{-1} \Lambda a) \oplus \dots \oplus P(\varepsilon^{-k} \Lambda a) = P(\varepsilon^{-1} \Lambda' a) \oplus \dots \oplus P(\varepsilon^{-k} \Lambda' a)$ мають місце рівності $\Lambda a = \Lambda' a$, $c' \Lambda a c'^{-1} = \Lambda' a$, $c' \Lambda b c'^{-1} = \Lambda' b$. Зрозуміло, що при цьому $i_{c_0} \Lambda_0 = \Lambda'_0$.

Неважко бачити, що підмодулі $P(\varepsilon^{-i} \Lambda a) \oplus P(\varepsilon^i \Lambda a) = P(\varepsilon^{-i} \Lambda' a) \oplus P(\varepsilon^i \Lambda' a)$ інваріантні відносно c' , Λb і $\Lambda' b$ для всіх $1 \leq i \leq t$, а також $i = \frac{k}{2}$ (при

парному k) і $i = k$. Тому $c' = \text{diag} (c_1, \dots, c_t, c_{\frac{k}{2}}, c_k)$, де $c_i \in GL(2n_i, R)$, $1 \leq i \leq t$, $c_{\frac{k}{2}} \in GL(n_{\frac{k}{2}}, R)$, $c_k \in GL(n_k, R)$. При цьому c_i комутують з елементами $n_i \Lambda_i a = n_i \Lambda'_i a$, $n_i \Lambda_i b = n_i \Lambda'_i b$ для всіх $1 \leq i \leq t$, $c_{\frac{k}{2}} \Lambda_{\frac{k}{2}} b c_{\frac{k}{2}}^{-1} = \Lambda'_{\frac{k}{2}} b$ (при парному k), $c_k \Lambda_k b c_k^{-1} = \Lambda'_k b$.

Таким чином, необхідність в теоремі 3 доведена. Достатність очевидна.

Зауважимо, що, згідно з лемою 1, матриці c_i , можна ототожнити з матрицями групи $GL(n_i, R)$ за допомогою гомоморфізма $R \rightarrow R_2$, який визначається за правилом $r \rightarrow \text{diag}(r, r)$, $r \in R$.

За побудовою $\Lambda_{\frac{k}{2}} a$ (існує тільки при парному k) – скалярна матриця з $\varepsilon^{\frac{k}{2}}$ на діагоналі, $\Lambda_k a$ – одинична матриця. Тому на матриці $\Lambda_{\frac{k}{2}} b$ і $\Lambda_k b$, $\Lambda'_{\frac{k}{2}} b$ і $\Lambda'_k b$ жодних умов, окрім того, що вони елементи другого порядку, не накладається.

Наслідок 7. В умовах теореми 3 зображення Λ і Λ' еквівалентні тоді і тільки тоді, коли виконуються умови

при $2 \in R^*$ $n_i = n'_i$ для всіх $1 \leq i \leq t$, зображення Λ_0 і Λ'_0 еквівалентні, $\dim P(\Lambda_k b) = \dim P(\Lambda'_k b)$ і $\dim P(\Lambda b) = \dim P(\Lambda' b)$,

при $2 \in J(R)$ $n_i = n'_i$ для всіх $1 \leq i \leq t$, зображення Λ_0 і Λ'_0 еквівалентні, $l = l'$ і матриці J і J' спряжені, де, з точністю до спряження, $\Lambda_k b = b_{l,J}$, а $\Lambda'_k b = b_{l',J'}$.

Доведення. Нехай $2 \in R^*$. Згідно з наслідком 1 матриці $\Lambda_{\frac{k}{2}} b$ і $\Lambda'_{\frac{k}{2}} b$ (при парному k) спряжені тоді і тільки тоді, коли

$$\dim P(\Lambda_{\frac{k}{2}} b) = \dim P(\Lambda'_{\frac{k}{2}} b)$$

Аналогічно матриці $\Lambda_k b$ і $\Lambda'_k b$ спряжені тоді і тільки тоді, коли

$$\dim P(\Lambda_k b) = \dim P(\Lambda'_k b)$$

Неважко бачити, що

$$\dim P \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 2 - \dim R \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1.$$

Нехай Λ і Λ' еквівалентні зображення групи D_m , $m > 1$. Згідно з теоремою 2 $n_i = n'_i$, для всіх $1 \leq i \leq t$, зображення Λ_0 і Λ'_0 еквівалентні і матриці $\Lambda_{\frac{k}{2}} b$ і $\Lambda'_{\frac{k}{2}} b$ (при парному k), а також $\Lambda_k b$ і $\Lambda'_k b$ спряжені. Тому

$$\dim P(\Lambda_{\frac{k}{2}} b) = \dim P(\Lambda'_{\frac{k}{2}} b), \dim P(\Lambda_k b) = \dim P(\Lambda'_k b) \text{ і}$$

$$\dim P(\Lambda b) = n_1 + \dots + n_t + \dim P(\Lambda_{\frac{k}{2}} b) + \dim P(\Lambda_k b) + \dim P(\Lambda_0 b) =$$

$$= n'_1 + \dots + n'_t + \dim P(\Lambda'_{\frac{k}{2}} b) + \dim P(\Lambda'_k b) + \dim P(\Lambda_0 b) = \dim P(\Lambda' b).$$

Навпаки. Нехай $n_i = n'_i$ для всіх $1 \leq i \leq t$, зображення Λ_0 і Λ'_0 еквівалентні, $\dim P(\Lambda_k b) = \dim P(\Lambda'_k b)$ і $\dim P(\Lambda b) = \dim P(\Lambda' b)$. Тоді $\dim P(\Lambda_{\frac{k}{2}} b) = \dim P(\Lambda'_{\frac{k}{2}} b)$ (при парному k). Згідно з наслідком 1 матриці $\Lambda_k b$ і $\Lambda'_k b$, а також матриці $\Lambda_{\frac{k}{2}} b$ і $\Lambda'_{\frac{k}{2}} b$ є відповідно спряженими. Згідно з теоремою 3, Λ і Λ' еквівалентні.

Нехай $2 \in J(R)$. Тоді m – непарне число. Згідно з теоремою 3 зображення Λ і Λ' еквівалентні тоді і тільки тоді, коли $n_i = n'_i$ для всіх $1 \leq i \leq t$, зображення Λ_0 і Λ'_0 еквівалентні і матриці $\Lambda_k b$ і $\Lambda'_k b$ є спряженими. За лемою 5, з точністю до спряження, $\Lambda_k b = b_{l,J}$, $\Lambda'_k b = b_{l',J'}$, де

$$b_{l,J} = \text{diag} \left(\underbrace{\left(\begin{array}{cc} -1 & 1 \\ 0 & 1 \end{array} \right), \dots, \left(\begin{array}{cc} -1 & 1 \\ 0 & 1 \end{array} \right)}_{2l}, E + J \right),$$

$$b_{l',J'} = \text{diag} \left(\underbrace{\left(\begin{array}{cc} -1 & 1 \\ 0 & 1 \end{array} \right), \dots, \left(\begin{array}{cc} -1 & 1 \\ 0 & 1 \end{array} \right)}_{2l'}, E + J' \right),$$

де $l = \dim R(\overline{\Lambda_k b})$, $l' = \dim R(\overline{\Lambda'_k b})$, а J і J' – матриці над $J(R)$.

Якщо матриці $\Lambda_k b$ і $\Lambda'_k b$ спряжені, то матриці $\overline{\Lambda_k b}$ і $\overline{\Lambda'_k b}$ також спряжені. Тому $l = l'$. Згідно з лемою 5 матриці J і J' спряжені. Навпаки очевидно.

Теорема 3 дає можливість встановлювати еквівалентність довільних зображень групи діедра D_m , $m > 1$ над комутативними локальними кільцями R з 1, в яких m – оборотний елемент. Нехай

$$\Lambda_1 : D_m \rightarrow GL(n, R), \quad n \geq 2 \quad \text{і} \quad \Lambda_2 : D_m \rightarrow GL(n, R), \quad n \geq 2$$

довільні зображення групи діедра D_m , $m > 1$. За теоремою 1 існують зображення Λ і Λ' групи D_m такого ж вигляду як в теоремі 3, що є еквівалентними до зображень Λ_1 і Λ_2 відповідно. За теоремою 3 встановлюється еквівалентність або нееквівалентність зображень Λ і Λ' , а значить і зображень Λ_1 і Λ_2 .

Теорема 4. Нехай R – комутативне локальне кільце з 1, $m \in R^*$, ε – породжує корені m -го степеня із 1 кільця R , k – порядок ε , $k > 1$, $\Lambda : D_m \rightarrow GL(n, R) \cong GL(n, V)$, $n \geq 1$ – довільне зображення групи діедра D_m , $m > 1$. Тоді, з точністю до еквівалентності,

$$\Lambda a = \text{diag} \left(\underbrace{a_1, a_1^{-1}}_{2n_1}, \dots, \underbrace{a_t, a_t^{-1}}_{2n_t}, a_{\frac{k}{2}}, a_k \right),$$

$$\Lambda b = \text{diag} \left(\left(\begin{array}{cc} 0 & E_{n_1} \\ E_{n_1} & 0 \end{array} \right), \dots, \left(\begin{array}{cc} 0 & E_{n_t} \\ E_{n_t} & 0 \end{array} \right), b_{\frac{k}{2}}, b_k \right),$$

де $a_i^{\frac{m}{k}} = \varepsilon^i E_{n_i}$, $1 \leq i \leq t < \frac{k}{2}$, $a_{\frac{k}{2}}^{\frac{m}{k}} = \varepsilon^{\frac{k}{2}} E_{n_{\frac{k}{2}}}$, $b_{\frac{k}{2}}^2 = E_{n_{\frac{k}{2}}}$ (при парному k), $a_k^{\frac{m}{k}} = E_{n_k}$, $b_k^2 = E_{n_k}$.

Доведення. Розглянемо групу діедра

$$D_k = \left\langle a^{\frac{m}{k}}, b \mid \left(a^{\frac{m}{k}}\right)^k = a^m = 1, b^2 = 1, bab^{-1} = a^{-1} \right\rangle, \quad k > 1$$

і зображення $\tilde{\Lambda} : D_k \rightarrow GL(n, R) \cong GL(n, V)$, $n \geq 1$, яке визначене за правилом $\tilde{\Lambda} a^{\frac{m}{k}} = \Lambda a^{\frac{m}{k}}$ і $\tilde{\Lambda} b = \Lambda b$.

Оскільки $k \in R^*$ і ε – первісний корінь k -го степеня із 1, то, згідно з теоремою 1, з точністю до еквівалентності, $\tilde{\Lambda} = n_1 \Lambda_1 + \dots + n_t \Lambda_t + \Lambda_{\frac{k}{2}} + \Lambda_k$, де

$$\Lambda_i : a^{\frac{m}{k}} \rightarrow \begin{pmatrix} \varepsilon^i & \\ & \varepsilon^{-i} \end{pmatrix}, \quad \Lambda_i : b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$1 \leq i \leq t < \frac{k}{2}$, n_i – кратність входження Λ_i в $\tilde{\Lambda}$, $\Lambda_{\frac{k}{2}} : a^{\frac{m}{k}} \rightarrow \varepsilon^{\frac{k}{2}} E_{n_{\frac{k}{2}}}$, $\Lambda_{\frac{k}{2}} : b \rightarrow b_{\frac{k}{2}}$

(при парному k) і $\Lambda_k : a^{\frac{m}{k}} \rightarrow E_{n_k}$, $\Lambda_k : b \rightarrow b_k$.

Без обмеження загальності, можна вважати, що зображення $n_i \Lambda_i : D_k \rightarrow GL(2n_i, R)$,

$$n_i \Lambda_i : a^{\frac{m}{k}} \rightarrow \text{diag} \left(\underbrace{\begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}, \dots, \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix}}_{2n_i} \right),$$

$$n_i \Lambda_i : b \rightarrow \text{diag} \left(\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{2n_i} \right)$$

співпадають з еквівалентними до них зображеннями

$$a^{\frac{m}{k}} \rightarrow \begin{pmatrix} \varepsilon^i E_{n_i} & 0 \\ 0 & \varepsilon^{-i} E_{n_i} \end{pmatrix}, b \rightarrow \begin{pmatrix} 0 & E_{n_i} \\ E_{n_i} & 0 \end{pmatrix}.$$

Тому, без обмеження загальності, можна вважати, що

$$\tilde{\Lambda} a^{\frac{m}{k}} = \text{diag} \left(\varepsilon E_{n_1}, \varepsilon^{-1} E_{n_1}, \dots, \varepsilon^t E_{n_t}, \varepsilon^{-t} E_{n_t}, \varepsilon^{\frac{k}{2}} E_{n_{\frac{k}{2}}}, E_{n_k} \right),$$

$$\tilde{\Lambda} b = \text{diag} \left(\begin{pmatrix} 0 & E_{n_1} \\ E_{n_1} & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & E_{n_t} \\ E_{n_t} & 0 \end{pmatrix}, b_{\frac{k}{2}}, b_k \right).$$

Матриця Λa комутує з матрицею $\tilde{\Lambda} a^{\frac{m}{k}}$. Враховуючи, що $\varepsilon^i - \varepsilon^{\pm j}$, $\varepsilon^{-i} - \varepsilon^{\pm j}$, $\varepsilon^i - \varepsilon^{-i}$, $\varepsilon^{\pm i} - \varepsilon^{\frac{k}{2}}$ (при парному k), $\varepsilon^{\pm i} - 1$ належать R^* при будь-яких $1 \leq i \neq j < \frac{k}{2}$ отримуємо, що, з точністю до еквівалентності,

$$\Lambda a = \text{diag} \left(a_1, a_1^{-1}, \dots, a_t, a_t^{-1}, a_{\frac{k}{2}}, a_k \right).$$

Із співвідношення $bab^{-1} = a^{-1}$ випливає, що $a'_i = a_i^{-1}$ для всіх $1 \leq i \leq t$.
Тому

$$\Lambda a = \text{diag} \left(\underbrace{a_1, a_1^{-1}}_{2n_1}, \dots, \underbrace{a_t, a_t^{-1}}_{2n_t}, a_{\frac{k}{2}}, a_k \right),$$

$$\Lambda b = \text{diag} \left(\begin{pmatrix} 0 & E_{n_1} \\ E_{n_1} & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & E_{n_t} \\ E_{n_t} & 0 \end{pmatrix}, b_{\frac{k}{2}}, b_k \right),$$

де $a_i \in GL(n_i, R)$, $a_i^{\frac{m}{k}} = \varepsilon^i E_{n_i}$, $1 \leq i \leq t$, $a_{\frac{k}{2}}, b_{\frac{k}{2}} \in GL\left(n_{\frac{k}{2}}, R\right)$, $a_{\frac{k}{2}}^{\frac{m}{k}} = \varepsilon^{\frac{k}{2}} E_{n_{\frac{k}{2}}}$, $b_{\frac{k}{2}}^2 = E_{n_{\frac{k}{2}}}$ (при парному k), $a_k, b_k \in GL(n_k, R)$, $a_k^{\frac{m}{k}} = E_{n_k}$, $b_k^2 = E_{n_k}$.

Нерозкладні (незвідні) зображення групи дієдра D_m , $m > 1$ над комутативним локальним кільцем R з 1, в якому $m \in R^*$, ε породжує корені m -го степеня із 1, k – порядок ε , $k > 1$, з точністю до еквівалентності, знаходяться серед зображень вигляду

$$a \rightarrow \begin{pmatrix} a_i & 0 \\ 0 & a_i^{-1} \end{pmatrix}, b \rightarrow \begin{pmatrix} 0 & E_{n_i} \\ E_{n_i} & 0 \end{pmatrix}$$

або $a \rightarrow a_{\frac{k}{2}}$, $b \rightarrow b_{\frac{k}{2}}$ (при парному k) або $a \rightarrow a_k$, $b \rightarrow b_k$, де $a_i^{\frac{m}{k}} = \varepsilon^i E_{n_i}$, $1 \leq i < \frac{k}{2}$, $a_{\frac{k}{2}}^{\frac{m}{k}} = \varepsilon^{\frac{k}{2}} E_{n_{\frac{k}{2}}}$, $b_{\frac{k}{2}}^2 = E_{n_{\frac{k}{2}}}$, $a_k^{\frac{m}{k}} = E_{n_k}$, $b_k^2 = E_{n_k}$. Теорема 4 доведена.

Для повноти описання нагадаємо, що при $k = 1$, згідно з теоремою 1, з точністю до еквівалентності, $\Lambda = \Lambda_1 + \Lambda_0$, тобто $\Lambda a = \text{diag} \left(\underbrace{1, \dots, 1}_{n_1}, a_0 \right)$ і

$\Lambda b = \text{diag}(b_1, b_0)$, де a_0 – корінь многочлена $1 + x + \dots + x^{m-1}$ і $b_0^2 = 1$, $b_0 a_0 b_0^{-1} = a_0^{-1}$.

Нерозкладні (незвідні) зображення групи D_m , $m > 1$ над R при $k = 1$ знаходяться серед одномірних зображень $a \rightarrow 1$, $b \rightarrow \alpha$, де $\alpha^2 = 1$ або двомірних зображень $a \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}$, $b \rightarrow \pm \begin{pmatrix} -1 & 0 \\ r & 1 \end{pmatrix}$, де $r \in R$ і тричлен $x^2 - rx + 1$ ділить без остачі двочлен $x^m - 1$ або степеня $n > 2$ вигляду $a \rightarrow a_0$, $b \rightarrow b_0$, де a_0 – корінь многочлена $1 + x + \dots + x^{m-1}$ і $b_0^2 = 1$, $b_0 a_0 b_0^{-1} = a_0^{-1}$.

1. Бондаренко В.М., Дрозд Ю.А. Представленческий тип конечных групп // Записки науч. семинаров Ленингр. отд. мат. ин-та АН СССР. – 1977. – 71. – С.24-41.
2. Гудивок П.М. Представления конечных групп над коммутативными локальными кольцами. – Ужгород: Ужгородский национальный университет. 2003. – 119 с.
3. Тимлицяк О.А. Зображення 2-го степеня групи діедра порядку $2p$ над деякими комутативними локальними кільцями // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2008. – Вип. 16. – С.188-192.
4. Винберг Э.Б. Курс алгебры. – 2-е изд. испр. и доп. – Москва: Факториал Пресс., 2001. – 544 с.
5. Дроботенко В.С., Рудько В.П. Элементы теории колец. – Ужгород: Ужгородський національний університет. 2004. – 128 с.
6. Дрозд Ю.А., Кириченко В.В. Конечномерные алгебры. – Киев: Изд. объедин. «Вища школа», 1980. – 192 с.
7. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. – 3-е изд. перероб. и доп. – Москва: Наука, 1982. – 288 с.
8. Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр. – Москва: Наука, 1969. – 668 с.
9. Фейт У. Теория представлений конечных групп: Пер. с англ. – М.: Наука. Гл. ред. физ.-мат., 1990. – 464 с.
10. Петечук Ю. В. Двомірні зображення груп діедра над комутативними локальними кільцями. Частина 1. // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2009. – Вип. 19. – С.112–120.

Одержано 20.04.2010