

Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

Тилищак Олександр Андрійович

УДК 512.547.25:512.64:512.552.7:519.725

ДИСЕРТАЦІЯ
МАТРИЧНІ ЗОБРАЖЕННЯ СКІНЧЕННИХ ГРУП
НАД КОМУТАТИВНИМИ ЛОКАЛЬНИМИ
КІЛЬЦЯМИ ТА ЇХ ЗАСТОСУВАННЯ

01.01.06 – алгебра та теорія чисел

Подається на здобуття наукового ступеня
доктора фізико-математичних наук

Дисертація містить результати власних досліджень. Використання
ідей, результатів і текстів інших авторів мають посилання на відповідне
джерело _____ О. А. Тилищак

Науковий консультант
Бондаренко Віталій Михайлович,
доктор фізико-математичних наук,
професор

Київ – 2020

АНОТАЦІЯ

Тилищак О. А. Матричні зображення скінченних груп над комутативними локальними кільцями та їх застосування. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.06 – алгебра та теорія чисел. – Київський національний університет імені Тараса Шевченка, Міністерство освіти і науки України, Київ, 2020.

Дисертаційна робота присвячена вивченню матричних зображень скінченних груп над комутативними кільцями, дослідженню мономіальних матриць пов'язаних із зображеннями над тими ж кільцями та різноплановими застосуваннями методів теорії матричних зображень скінченних груп над комутативними кільцями в теорії лінійних груп, групових кілець та теорії кодування. У роботі в основному розглядаються модулярні зображення скінченних p -груп над комутативними кільцями характеристики p^s ($s > 0$, p — просте число), що не є полями. Описати, з точністю до еквівалентності, всі такі зображення в більшості випадків не можна із за охоплення цією задачею іншої класичної нерозв'язної задачі лінійної алгебри про пару матриць. В таких випадках актуальними стають дослідження зображень певного вигляду, зокрема, незвідних та нерозкладних.

Було встановлено критерій скінченності множини нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи над комутативним нетеровим локальним кільцем характеристики p^s , яке не є напівпервісним, з нескінченним полем лишків. Показано, що множина нееквівалентних незвідних матричних зображень наперед за-

даного степеня скінченної p -групи над цим кільцем або нескінченна, або порожня. Показано нескінченність числа всіх нееквівалентних незвідних матричних зображень наперед заданого степеня $n > 1$ скінченної p -групи G порядку $|G| > 2$ над комутативним нетеровим локальним напівпервісним нецілісним кільцем характеристики p , з нескінченним полем лишків. Також показано нескінченність числа всіх нееквівалентних незвідних матричних зображень наперед заданого степеня $n > 1$ скінченної 2-групи G порядку $|G| > 1$ над комутативним локальним напівпервісним нецілісним кільцем, яке містить неголовний анулятор деякого з своїх елементів характеристики p , поле класів лишків якого нескінченне.

Доведено, що всі матричні зображення непарного степеня групи другого порядку над локальною областю цілісності характеристики 2, будь-який скінченно породжений ідеал якої володіє мінімальною системою з не більше ніж двох твірних елементів, звідні.

Описано всі, з точністю до еквівалентності, матричні зображення 2-го степеня групи діедра порядку $2p$ (p — непарне просте число) над комутативними локальними кільцями довжини 2 характеристики 2, та з'ясовано критерій їх незвідності.

Розглянуто такі види мономіальних матриць: канонічних циклічних, t -циклічних, бімономіальних. Встановлено одну достатню умову спадкової звідності t -циклічних матриць над комутативним кільцем. Аналогічне встановлено для бімономіальних матриць над комутативним кільцем. А саме доведено, що така матриця спадково звідна, коли її розмір і кількість одиниць у вигляді не є взаємно прості. Показано незвідність яка, зокрема, означає спадкову незвідність, всіх бімономіальних 7×7 -матриць над комутативним локальним кільцем довжини $l > 2$. Раніше були відомі спадково звідні бімономіальні 7×7 -матриці (коли їх розмір

і кількість одиниць у вигляді взаємно прості) над комутативним локальним кільцем довжини $l = 2$.

Описане дослідження матриць було застосоване до дослідження потужності множини нерозкладних та множини незвідних унімономіальних зображень з точністю до еквівалентності циклічної p -групи над комутативним локальним кільцем скінченної довжини характеристики p^s . Побудовано серію нерозкладних унімономіальних зображень циклічної p -групи, що відповідають двозв'язним циклам, над комутативним локальним кільцем скінченної довжини характеристики p^s , та оцінюється знизу число побудованих зображень заданого степеня з точністю до еквівалентності для груп з деяким достатньо великим порядком. Була побудована серія нерозкладних унімономіальних зображень циклічної p -групи над скінченним комутативним локальним кільцем скінченної довжини характеристики p , та підраховується число побудованих зображень заданого степеня з точністю до еквівалентності для кожної групи та кільця, зі скінченним полем лишків, окремо.

Введено поняття $*$ -еквівалентності зображень циклічної групи над комутативним локальним кільцем головних ідеалів, що дозволило абстрагуватися від деяких оборотних параметрів у серіях нерозкладних зображень побудованих раніше. Була побудована нова серія нерозкладних унімономіальних зображень циклічної p -групи над довільним комутативним локальним кільцем скінченної довжини характеристики p та підраховується число побудованих зображень заданого степеня з точністю до $*$ -еквівалентності для кожної групи та кільця окремо.

Також була побудована нова серія спадково незвідних унімономіальних зображень циклічної p -групи над скінченним комутативним локальним кільцем головних ідеалів характеристики p , та підраховується число

побудованих зображень заданого степеня з точністю до еквівалентності для кожної групи та кільця, зі скінченним полем лишків, окремо.

Методи теорії матричних зображень скінченних груп над комутативним кільцем K природно знаходять застосування при дослідженні матричних груп над тим же кільцем. Було показано, що всі максимальні уніпотентні підгрупи повної лінійної групи над кільцем K попарно спряжені, якщо його фактор-кільце $K/\text{rad } K$ за первісним радикалом $\text{rad } K$ є скінченною прямою сумою кілець Безу. Також показано, що всі максимальні уніпотентні підгрупи спеціальної лінійної групи над кільцем K попарно спряжені, якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу. Результати про максимальні уніпотентні підгрупи повної та спеціальної лінійної групи над комутативним кільцем застосовуються до вивчення силовських p -підгрупи повної та спеціальної лінійної групи над тим же кільцем характеристика якого p^s .

Класичним прикладом застосування теорії зображень класичної та модулярної при дослідженні одиниць скінченного порядку цілочислового групового кільця скінченної групи є метод Лутара – Пасі. Цим методом встановлено, що в цілочисловому груповому кільці скінченної простої групи $PSL(3, 4)$ показника 420, який має 23 нетривіальні дільники, можуть бути тільки нетривіальні одиниці порядку: 2, 3, 4, 5, 7 і 6 (відомо, що порядок розглядуваних одиниць завжди ділить показника 420), а для одиниць порядку 2 та 3 виконується гіпотеза Цассенхауза.

Було побудовано з використанням регулярного зображення групових кілець низку самодуальних кодів над деякими скінченними комутативними фробеніусовими кільцями в тому числі й бінарні самодуальні коди, багато з яких є екстремальними. Зокрема, розглянуто один метод побудови розширених бінарних кодів Галея за груповим кільцем групи 24-го

порядку. Встановлено, що з 15 відомих неізоморфних груп 24-го порядку таким способом можна побудувати код тільки для груп

$$D_{24}, (C_6 \times C_2) \rtimes C_2, C_3 \times D_8, S_4, C_2 \times A_4.$$

Для трьох з цих груп $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$ такі коди будувались вперше. Крім того, відома конструкція коду, що використовувала дію регулярного зображення на певних елементах групового кільця, як частини породжуючої матриці коду, була поширена для побудови нових самодуальних кодів над полем з двох елементів та над деякими скінченними комутативними фробеніусовими кільцями.

Результати дисертаційної роботи мають здебільшого теоретичний характер. Побудовані серії незвідних та нерозкладних зображень скінченних груп над комутативними локальними кільцями можуть знайти своє застосування при описанні, з точністю до еквівалентності, окремих серій зображень тих же груп над локальними та довільними комутативними кільцями. Результати дисертаційної роботи про мономіальні матриці над комутативними локальними кільцями знайшли (і можуть знайти нові) застосування при дослідженні модулярних матричних зображень скінченних груп над тими ж кільцями, а також можуть знайти застосування при описанні, з точністю до подібності, окремих серій квадратних матриць над локальними та довільними комутативними кільцями. Розроблені методи також застосовувались (і можуть далі застосовуються) при дослідженні уніпотентних підгруп лінійних груп над комутативним кільцем, при побудові самодуальних кодів над фробеніусовими кільцями. Результати дисертаційної роботи про самодуальні коди носять пряме практичне значення. Зокрема побудовані бінарні екстремальні самодуальні коди можуть застосовуватися при кодуванні інформації, для виправлення помилок під час передачі даних каналами зв'язку.

Ключові слова: комутативне кільце, радикал кільця, ступінь нільпотентності, локальне кільце, матричне зображення, незвідне зображення, нерозкладне зображення, мономіальна матриця, унімономіальне зображення, уніпотентна група, лінійна група, цілочислове групове кільце, одиниця скінченного порядку, самодуальний код, розширений бінарний код Голя.

ABSTRACT

Tylyshchak A. A. Matrix representations of finite groups over commutative local rings and their applications. – Qualifying scientific paper on the rights of the manuscript.

The thesis for obtaining the Doctor of Physical and Mathematical Sciences degree on the speciality 01.01.06 — «algebra and number theory». – Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine, Kyiv, 2020.

The thesis is devoted to the studying of matrix representations of finite groups over commutative rings, the studying of monomial matrices connected with representations over same rings and to the diversified applications of methods of theory of matrix representations of finite groups over commutative rings in the linear group theory, in group rings, and in the coding theory. The paper deals mainly with modular representations of finite p -groups over commutative rings of characteristic p^s ($s > 0$, p is a prime), which are not fields. In most cases the problem of classifying up to equivalence all such representations is impossible because this problem include the problem of pair of matrices. This is another classical unsolvable problem of linear algebra. In such situation, an important place is occupied by particular kind of matrices, in particular, irreducible and indecomposable representations over rings.

In paper it has been found the criterion of finiteness of the set of non-equivalent irreducible matrices representations of given degree of finite p -group over a commutative Noetherian local ring of characteristics p^s , which is not semi-primitive ring, with infinite residue class field. It has been shown that the set of non-equivalent irreducible matrix representations of given degree of finite p -group over such ring are either infinite or empty. It has been shown the infiniteness of the set of non-equivalent irreducible matrix representations of given degree $n > 1$ of finite p -group G of order $|G| > 2$ over a commutative Noetherian local semi-primordial non-integer ring of characteristic p , with infinite residue class field. It has also been shown infiniteness of the set of non-equivalent irreducible matrices representations of given degree $n > 1$ of finite 2-group G of order $|G| > 1$ over a commutative local semiprime non-integral ring containing a non-principle annihilator of some of its elements of characteristic p , whose residue class field is infinite.

It has been proved that all matrix representations of odd degree of group of the second order over a local integral domain of characteristic 2 are reducible if any finitely generated ideal of ring has a generator system of no more than two elements.

All matrix representations of the second degree of the dihedral group of order $2p$ (p be a odd prime) over a commutative local rings of length 2 of characteristic 2 up to equivalence are described. The criterion of their irreducibility also was founded.

The following types of monomial matrices: canonical cyclic, t -cyclic, binomial are considered. It has been established one sufficient condition of its hereditary reducibility over a commutative ring. A similar result was set for binomial matrices over the commutative ring. Namely, it has been proved that such matrix is hereditarily reducible when number of units in the form

is not relatively prime to matrix size. It has been shown irreducibility which also mean hereditary irreducibility of all binomial 7×7 -matrices over a commutative local ring of length $l > 2$. Previously it is known hereditary reducibility of binomial 7×7 -matrices (number of units is not relatively prime to matrix size) over a commutative local ring of length $l = 2$.

The described matrix studding was applied to the investigation of cardinality of the set of indecomposable and set of irreducible unimonomial representations up to equivalence of a cyclic p -group over a commutative local ring of finite length of characteristic p^s . It has been constructed a series of indecomposable unimonomial representations of a cyclic p -group corresponding to two-loop cycles over a commutative local ring of finite length of characteristic p^s , and it has been estimated below the number of constructed representations of a given degree up to equivalence for groups with some large enough order. A series of indecomposable unimonomial representations was constructed for a cyclic p -group over a finite commutative local ring of finite length of characteristic p , and it was counted the number of constructed representations of a given degree up to equivalence separately for each group and ring with the finite residue class field.

It has been introduced the notation of $*$ -equivalence of representations of a cyclic group over a commutative local principle ideals ring, which allowed us to abstract from some of the invertible parameters in a series of representations constructed earlier. It has been constructed a new series of irreducible unimonomial representations of a cyclic p -group over an arbitrary commutative local ring of finite length of characteristic p and it was counted the number of constructed representations of given degree up to $*$ -equivalence separately for each group and ring.

A new series of hereditary irreducible unimonomial representations of

a cyclic p -group over a finite commutative local principle ideals ring of the characteristic p was also constructed. The number of constructed representations of a given degree up to equivalence was counted separately for each group and ring with the finite residue class field.

Methods of matrix representation theory of finite groups over a commutative ring K naturally find application in the investigation of matrix groups over the same ring. It has been shown that all maximal unipotent subgroups of the general linear group over the ring K are pairwise conjugated if factor-ring $K/\text{rad } K$ by its primitive radical $\text{rad } K$ is a finite direct sum of Bezou domain. It is also shown that all maximal unipotent subgroups of the special linear group over the ring K are pairwise conjugated if $K/\text{rad } K$ is a finite direct sum of Bezou domain. Results on the maximum unipotent subgroups of the general and special linear groups over the commutative ring are applied to the investigation of the Sylow p -subgroup of the general and special linear group over the same ring of characteristic p^s .

A classic example of applying of classical and modular representation theory to investigation of torsion units of the integer group ring the finite group is the Luthar–Passi method. It has been shown by this method that in the integer group ring of the finite simple group $PSL(3, 4)$ of exponent 420, which has 23 non-trivial divisors, can be only non-trivial torsion units of order: 2, 3, 4, 5, 7 and 6 (it is known that order of torsion units divides 420), and for torsion units of order 2 and 3 the Zassenhaus conjecture is satisfied.

Using the regular representation of group rings make it possible to construct some self-coded codes over a finite commutative Frobenius rings. Some of them are binary self-dual codes, which are extreme. In particular, it has been considered one method of constructing extended Binary Golay code by the group ring of group of order 24. It is known that there are 15

non-isomorphic groups of order 24. It has been shown that by this way one can construct extended Binary Golay code only from groups

$$D_{24}, (C_6 \times C_2) \rtimes C_2, C_3 \times D_8, S_4, C_2 \times A_4.$$

For three of these groups $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$ such codes were constructed first. Moreover, it is known codes of form, which used the regular representation on some elements of a group ring as part of a generating matrices of codes. Method of construction of this codes was extended to constructing new self-dual codes over the field of two element and over some finite commutative Frobenius rings.

The results of the work are mainly theoretical. Constructed series of irreducible representations of finite groups over commutative local rings can be applied in the describing up to equivalence individual series of representations of the same groups over local and arbitrary commutative rings. The results of the thesis on monomial matrices over commutative local rings have found (and can find new) applications in the investigations of modular matrix representations of finite groups over the same rings, and can also find applications to the descriptions up to similarity of individual series of square matrices over local and arbitrary commutative rings. The methods proposed in the thesis had been applied (and may continue to apply) in the study of unipotent subgroups of linear groups over a commutative ring, at constructing of self-dual codes over Frobenius rings. The results included to the thesis on self-dual codes have direct practical importance. In particular binary extreme self-dual codes can be effectively used when encoding information to correct errors during data transmission by communication channels.

Keywords: commutative ring, radical of a ring, degree of nilpotency, local ring, matrix representation, irreducible representation, indecomposable

representation, monomial matrix, unimonomial representation, unipotent group, linear group, integral group ring, torsion unit, selfdual cod, extended binary Golay code.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації, в яких опубліковано основні наукові результати дисертації

1. Тилищак О. А. Про незвідні модулярні зображення даного степеня скінченної p -групи над комутативним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2002. Вип. 7. С. 108–114.
2. Тилищак О. А. Про незвідні модулярні зображення даного степеня скінченної p -групи над напівпервісним комутативним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2003. Вип. 8. С. 156–159.
3. Тилищак О. А. Про незвідні модулярні зображення 2-групи даного степеня над напівпервісним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2004. Вип. 9. С. 103–106.
4. Тилищак О. А. Про модулярні зображення циклічної 2-групи над локальною областю цілісності. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2005. Вип. 10–11. С. 137–141.
5. Тилищак О. А. Зображення 2-го степеня групи діедра порядку $2p$ над деякими комутативними локальними кільцями. *Наук. вісник*

- Ужгород. ун-ту. Серія математики і інформатики. 2008. Вип. 16. С. 188–192.
6. Tylyshchak A. A. On maximal unipotent subgroups of the general linear group over commutative rings. *Bulletin of University of Kyiv. Ser.: Phys. & Math.* 2010. Vol. No 3. P. 115–117.
 7. Динис Р. Ф., Тилищак О. А. Про звідність матриць деякого вигляду над комутативними локальними кільцями головних ідеалів. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики.* 2012. Вип. 23, № 1. С. 57–62.
 8. Bondarenko V. M., Bortos M. Yu., Dinis R. F., Tylyshchak A. A. Reducibility and Irreducibility of Monomial Matrices over Commutative Rings. *Algebra Discret Math.* 2013. Vol. 16, No 2. P. 171–187.
 9. Бортош М. Ю., Тилищак О. А. Приводимость некоторых мономимальных матриц над коммутативными локальными кольцами. *Науковий часопис НПУ ім. М. П. Драгоманова. Серія 1. Фіз.-мат. науки.* Київ. : НПУ ім. М. П. Драгоманова. 2013. № 14. С. 68–78.
 10. Bondarenko V. M., Tylyshchak A. A., Stoika M. V. On the equivalence of matrices over commutative rings modulo ideals. *Algebra and Discrete Math.* 2014. Vol. 17, No 1. P. 12–19.
 11. Динис Р., Тилищак О. Про звідність деяких мономіальних матриць над комутативними кільцями. *Вісник Київ. нац. ун-ту ім. Т. Шевченка. Серія: математики і механіки.* 2014. Вип. 2 (32). С. 20–23.
 12. Gildea J., Tylyshchak A. Torsion units in the integral group ring of $PSL(3, 4)$. *J. Algebra Appl.* 2016. Vol. 15, No 1, 1650013. 9 p.

13. Bondarenko V. M., Bortos M. Yu., Dinis R. F., Tylyshchak A. A. Indecomposable and irreducible t -monomial matrices over commutative rings. *Algebra and Discrete Math.* 2016. Vol. 22, No 1. P. 11–20.
14. Dougherty S. T., Gildea J., Taylor R., Tylyshchak A. Group rings, G -codes and constructions of self-dual and formally self-dual codes. *Designs, Codes and Cryptography.* 2018. Vol. 86, Is. 9. P. 2115–2138.
15. Тилищак О. А. Про число нерозкладних модулярних зображень циклічної p -групи над скінченним локальним кільцем. *Прикл. проблеми механіки і математики.* 2018. Вип. 16. С. 19–29.
16. Тилищак О. А. Про незвідність мономіальних матриць 7-го порядку над локальними кільцями. *Вісник Київ. нац. ун-ту ім. Т. Шевченка. Серія: фіз.-мат. науки.* 2018. Вип. № 3. С. 37–44.
17. Bondarenko V. M., Gildea J., Tylyshchak A. A., Yurchenko N. V. On hereditary reducibility of 2-monomial matrices over commutative rings. *Algebra and Discrete Math.* 2019. Vol. 27, No 1. P. 1–11.
18. Dougherty S., Gildea J., Korban A., Kaya A., Tylyshchak A., Yildiz B. Bordered Constructions of Self-Dual Codes from Group Rings and New Extremal Binary Self-Dual Codes. *Finite Fields and Their Applications.* 2019. Vol. 57. P. 108–127.
19. Тилищак О. А. Про максимальні уніпотентні підгрупи спеціальної лінійної групи над комутативним кільцем. *Укр. мат. журн.* 2019. Т. 71, № 8. С. 1150–1156.
20. Тилищак О. А. Про спадково незвідні унімономіальні зображення циклічних p -груп над локальними кільцями характеристики p .

Наук. вісник Ужгород. ун-ту. Серія математики і інформатики.
2019. Вип. № 1 (34). С. 52–59.

21. Тилищак О. А. Про число нерозкладних модулярних зображень циклічної p -групи над локальним кільцем скінченної довжини. *Мат. методи та фіз.-мех. поля.* 2019. Вип. 62, № 1. С. 74–82.

Публікації, які додатково відображають наукові результати дисертації

22. Тилищак О. А., Юрченко Н. В., Цімболинець Р. Ф. Нерозкладність однієї матриці довільного порядку над локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики.* 2016. Вип. № 1 (28). С. 135–139.
23. Dougherty St., Gildea J., Taylor R., Tylyshchak A. Constructions of Self-Dual and Formally Self-Dual Codes from Group Rings. ArXiv preprint arXiv:1604.07863v1, 2016. 20 p. URL: <https://arxiv.org/abs/1604.07863v1> (date of appeal: 28.03.2020).

Публікації, які засвідчують апробацію матеріалів дисертації

24. Tylyshchak O. Irreducible modular representation of the given degree of finite p -group over commutative local ring of characteristic p^s . *IV International Algebraic Conference in Ukraine*: abstracts, L'viv, August 4–9, 2003. L'viv : Ivan Franko National University of L'viv, 2003. P. 222–223.
25. Tylyshchak A. On maximal unipotent subgroups of the general linear group over commutative ring. *XI International Mathematical Kravchuk*

- Conference* : conference materials, Kyiv, May 18–20, 2006. Kyiv. : TOV «Zadruha», 2006. P. 616.
26. Tylyshchak A. A. On Irreducible Modular Representations of Given Degree of Finite Group over Commutative Local Ring. *International Conference of Humboldt-Kolleg Series in Kyiv «Humboldt Cosmos: Science and Society», Kyiv, November 19-22, 2009* : abstracts, Kyiv, November 19–22, 2009. Kyiv : Embassy of the Federal Republic of Germany Kyiv, 2009. P. 45.
 27. Динис Р. Ф., Тилищак О. А. Про еквівалентність матриць деякого вигляду над локальними областями головних ідеалів. *Десята наукова відкрита конф. інституту прикладної математики та фундаментальних наук ІМФН* : зб. матеріалів та програма конф. [«PSC-IMFS-10»] (Львів, 17–18 травня 2012 р.). Львів : Видавництво Львівської політехніки, 2012. С. А31.
 28. Tylyshchak A., Bortosh M. On Reducibility of Monomial Matrixes over Commutative Local Rings. *IX International Algebraic Conference in Ukraine* : abstracts of reports, L'viv, July 8–13, 2013. L'viv : Ivan Franko National University of L'viv, 2013. P. 201.
 29. Bondarenko V., Dinis R., Tylyshchak A. On irreducibility of some matrices over p -adic integers. *Fifth International Conference on Analytic Number Theory and Spatial Tessellations* : abstracts, Kiev, September 16–20, 2013. Kyiv : Institute of Mathematics of NAS of Ukraine, 2013. P. 6.
 30. Dinis R. F., Tylyshchak A. A., Yurchenko N. V. On indecomposability of some monomial matrices over local rings. *X International*

- Algebraic Conference in Ukraine dedicated to the 70th anniversary of Yu. A. Drozd* : abstracts, Odessa, August 20–27, 2015. Odessa : TES, 2015. P. 32.
31. Stoika M. V., Tylyshchak A. A. On classifying the matrices over commutative rings up to equivalence. *International Conference of Young Mathematicians* : book of abstracts, Kyiv, June 3–6, 2015. Kyiv : Institute of Mathematics of NAS of Ukraine, 2015. P. 23.
 32. Динис Р. Ф., Тилищак О. А., Юрченко Н. В. Про нерозкладність мономіальних матриць спеціального вигляду над локальними кільцями. *Міжнар. мат. конф. «Методика викладання та методи досліджень в математиці»* : матеріали конф., Берегове, 21–23 квітня 2016. Ужгород : ТОВ «PIK-Y», 2016. С. 28.
 33. Tylyshchak A. A. On the estimation of the number of indecomposable representations of given degree of a cyclic group. *XI International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko* : abstracts, Kyiv, July 3–7, 2017. Kyiv : Institute of Mathematics of NAS of Ukraine, 2017. P. 137.
 34. Bondarenko V., Gildea J., Salim M., Tylyshchak A. On the number of indecomposable representations of given degree of a cyclic group over local rings of finite length. *The Second International Conference on Groups, Group Rings and Related Topics* : abstracts [electronic resource], Khorfakkan (UAE), November 19–22, 2017. Khorfakkan (UAE), 2017. P. 10. URL: https://conferences.uaeu.ac.ae/ggrrt2017/en/abstracts_ggrrt.pdf (date of appeal: 28.03.2020).

35. Тилищак О. Деякі нерозкладні модулярні зображення циклічної p -групи над локальним кільцем скінченної довжини. *Міжнар. наукова конф. «Сучасні проблеми механіки та математики»* : збірник наукових праць : у 3-х т. / за заг. ред. А. М. Самойленка та Р. М. Кушніра [Електронний ресурс] (Львів, 22–25 травня 2018). Львів, 2018. Т. 3. С. 237. URL: http://www.iapmm.lviv.ua/mpmm2018/Volume_3.pdf (дата звернення 28.03.2020).
36. Tylyshchak A. A. On irreducibility of monomial matrices of order 7 over local rings. *XII International Algebraic Conference in Ukraine dedicated to the 215th anniversary of V. Bunyakovsky* : abstracts, 2019, July 02-06, Vinnytsia, Ukraine. Vinnytsia : Vasyl' Stus Donetsk National University, 2019. P. 117–118.

ЗМІСТ

Список умовних позначень	24
Вступ	26
1. Попередні відомості	60
1.1 Зображення скінченних груп над комутативними кільцями .	60
1.2 Мономіальні матриці	67
1.3 Застосування теорії зображень при вивченні лінійних груп .	72
1.4 Групові кільця	81
1.4.1 Одиниці скінченного порядку цілочислових групових кільць	82
1.4.2 Застосування зображень групових кільць для побудо- ви самодуальних кодів.	89
1.5 Висновки до розділу	99
2. Незвідні та звідні модулярні зображення p-груп над ко- мутативними локальними кільцями	101
2.1 Вступ	102
2.2 Зображення скінченних p -груп над кільцями характеристики p^s	104
2.3 Зображення скінченних p -груп над напівпервісними кільця- ми характеристики p	121
2.4 Зображення скінченних 2-груп над областями цілісності ха- рактеристики 2	138
2.5 Зображення дієдральних груп порядку $2p$ над кільцями ха- рактеристики 2	144

2.6	Висновки до розділу	157
-----	-------------------------------	-----

3. Мономіальні матриці над комутативними кільцями 159

3.1	Означення і позначення	159
3.2	Спадкова звідність t -циклічних матриць	160
3.3	Спадкова звідність бімономіальних матриць	167
3.4	Незвідність бімономіальних матриць 7-го порядку	177
3.5	Висновки до розділу	203

4. Унімономіальні зображення груп над локальними кільцями скінченної довжини 205

4.1	Означення та елементарні властивості унімономіальних зображень	206
4.2	Про число нерозкладних унімономіальних зображень для двозв'язних циклів циклічних p -груп над локальним кільцем характеристики p^s з точністю до еквівалентності	210
4.3	Про число нерозкладних унімономіальних зображень циклічних p -груп над локальним кільцем характеристики p з точністю до еквівалентності	214
4.4	Про число нерозкладних унімономіальних зображень циклічних p -груп над локальним кільцем характеристики p з точністю до $*$ -еквівалентності	222
4.5	Про число спадково незвідних унімономіальних зображення циклічних p -груп над локальним кільцем характеристики p з точністю до еквівалентності	234
4.6	Висновки до розділу	240

5. Уніпотентні підгрупи лінійних груп над комутативними

кільцями	242
5.1 Вступ	242
5.2 Максимальні уніпотентні підгрупи повної лінійної групи . . .	244
5.3 Максимальні уніпотентні підгрупи спеціальної лінійної групи	252
5.4 Силовські p -підгрупи повної та спеціальної лінійної групи над кільцем характеристики p^s	256
5.5 Висновки до розділу	258
6. Еквівалентність матриць за модулем ідеалів	260
6.1 Еквівалентність пар матриць над полем	260
6.2 Еквівалентність матриць та пар матриць над кільцем	262
6.3 Еквівалентність матриць над факторіальним кільцем	265
6.4 Висновки до розділу	269
7. Застосування в теорії групових кілець і теорії кодів	270
7.1 Одиниці скінченного порядку цілочислового групового кільця групи $PSL(3, 4)$	270
7.2 Побудова розширених бінарних кодів Голея за груповим кільцем скінченних груп порядку 24	287
7.2.1 Група $SL(2, 3)$	289
7.2.2 Група $C_4 \times S_3$	296
7.2.3 Група $(C_6 \times C_2) \rtimes C_2$	300
7.2.4 Група $C_3 \times D_8$	305
7.2.5 Група $C_2 \times A_4$	309
7.2.6 Група $C_2 \times C_2 \times S_3$	315
7.3 Одна конструкція самодуальних кодів	319
7.4 Висновки до розділу	324

Висновки	326
-----------------	------------

Список використаних джерел	328
-----------------------------------	------------

Додаток А. Обчислення числових характеристик множини унімономіальних зображень над локальними кільцями скінченної довжини	356
--	------------

A.1 Підрахунок числа нерозкладних нееквівалентних унімономіальних зображень	356
A.2 Підрахунок числа нерозкладних *-нееквівалентних унімономіальних зображень	370
A.3 Підрахунок числа спадково незвідних нееквівалентних унімономіальних зображень	376

Додаток Б. Обчислення одиниць скінченного порядку цілочислового групового кільця групи $PSL(3, 4)$	386
--	------------

Додаток В. Обчислення розширених бінарних кодів Голя за груповим кільцем скінчених груп порядку 24	393
---	------------

V.1 Знаходження кодів за групою $SL(2, 3)$	395
V.2 Знаходження кодів за групою $C_4 \times S_3$	403
V.3 Знаходження кодів за групою $(C_6 \times C_2) \rtimes C_2$	410
V.4 Знаходження кодів за групою $C_3 \times D_8$	419
V.5 Знаходження кодів за групою $C_2 \times A_4$	427
V.6 Знаходження кодів за групою $C_2 \times C_2 \times S_3$	436

Додаток Г. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації	444
---	------------

Додаток Д. Апробація результатів дисертації	451
--	------------

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

$\mathbb{N}$ — множина натуральних чисел;

$\mathbb{Z}$ — кільце цілих чисел;

$\mathbb{Q}$ — поле раціональних чисел;

$\mathbb{Z}_m$ — кільце класів лишків за модулем m ;

$\mathbb{Z}[\lambda]$ — кільце цілочислових поліномів від невідомої λ ;

C_m^r — число сполучень з m елементів по r ;

$|G|$ — порядок скінченної групи G ;

$|g|$ — порядок елемента g деякої групи;

$x^g = g^{-1}xg$ — спряжений елемент до x за допомогою елемента g ;

$x^G = \{x^g | g \in G\}$ — клас спряжених елементів до елемента x у групі G ;

$A \cong B$ — ізоморфізм груп (кілець, модулів) A і B ;

$A \times B$ — прямий добуток груп A і B ;

$A \rtimes B$ — напівпрямий добуток груп A і B ;

$A \oplus B$ — внутрішня пряма сума кілець (адитивних груп) A і B ;

$\langle a \rangle$ — циклічна група, породжена елементом a ;

$a|b$ — елемент a комутативного кільця K ділить його елемент b ;

$\text{Rad } K$ — радикал Джекобсона комутативного кільця K ;

$\text{rad } K$ — первісний радикал комутативного кільця K ;

$\text{Ann } t = \{w \in K | wt = 0\}$ — анулятор елемента t в комутативному кільці K ;

K^* — мультиплікативна група кільця K з одиницею;

K/V — фактор-кільце комутативного кільця K за ідеалом V ;

$\bar{z} = z + \text{Rad } K$ — елемент поля лишків $K/\text{Rad } K$ комутативного локального кільця K , де $z \in K$;

$\tilde{z} = z + \text{rad } K$ — елемент фактор-кільця $K/\text{rad } K$ комутативного кільця

K , де $z \in K$;

$\overline{T} = \|t_{ij} + \text{Rad } K\|$ — матриця над полем лишків $K/\text{Rad } K$ комутативного локального кільця K , де $T = \|t_{ij}\|$ — деяка матриця над кільцем K ;

$\widetilde{T} = \|t_{ij} + \text{rad } K\|$ — матриця над фактор-кільцем $K/\text{rad } K$ комутативного кільця K , де $T = \|t_{ij}\|$ — деяка матриця над кільцем K ;

$\text{diag}[\alpha_1, \alpha_2, \dots, \alpha_n]$ — діагональна матриця порядку n з діагональними елементами $\alpha_1, \alpha_2, \dots, \alpha_n$;

$\det A$ — детермінант квадратної матриці A ;

$J_n(\lambda)$ — жорданова $n \times n$ -клітка з діагональним елементом λ ;

$\text{tr } A$ — слід квадратної матриці A ;

$A \circ B = A + B + AB$ — приєднаний добуток квадратних матриць A і B однакових порядків;

$M(n, K)$ — повне матричне кільце степеня n над комутативним кільцем K з одиницею;

$T(n, K)$ — кільце верхніх трикутних матриць порядку n комутативним кільцем K з одиницею з нулями на головній діагоналі;

E_n — одинична $n \times n$ -матриця;

$GL(n, K)$ — повна лінійна група степеня n над комутативним кільцем K з одиницею;

$SL(n, K)$ — спеціальна лінійна група степеня n над комутативним кільцем K з одиницею;

$PSL(n, K)$ — проективна спеціальна лінійна група степеня n над комутативним кільцем K з одиницею;

$UT(n, K)$ — унітрикутна група степеня n над комутативним кільцем K з одиницею.

ВСТУП

Актуальність теми. Теорія зображень скінченних груп займається вивченням гомоморфізмів абстрактної скінченної групи в групу лінійних операторів чи групу матриць. Перенесення обчислень з абстрактної групи в групу матриць виявилася ефективною ідеєю як при вивченні матричних груп так при вивченні абстрактних груп. Починаючи з 80-х років XIX століття, завдяки роботам Ф. Г. Фробеніуса та У. Бернсайда (див. [130]), які займалися переважно зображеннями скінченної групи над полем характеристики 0, теорія зображень груп посіла значне місце в теорії абстрактних скінченних груп. Серед її застосувань цікавими є дві відомі теореми теорії груп: Бернсайда та Фейта — Томпсона про розв'язність скінченних груп порядку $p^\alpha q^\beta$, де p, q — різні прості числа, та довільного непарного порядку відповідно [129, 144]. Завдяки роботам Е. Ньотер [179] було встановлено тісний зв'язок теорії зображень з теорією модулів над кільцями. Теорія зображень знайшла численні застосування майже у всіх областях алгебри і не тільки а й, наприклад, у квантовій механіці [57, 169].

Природним продовженням теорії зображень скінченних груп над полями є перехід до вивчення матричних зображень скінченних груп над комутативними кільцями, які почали активно досліджуватися в 40-х роках XX століття. З того часу вони також знайшли застосування в тому числі й за межами алгебри, наприклад, у кристалографії [92, 197].

При дослідженні матричних зображень скінченної групи над комутативним кільцем (як і над полем) виникають 3 основні задачі.

- 1) Розкласти довільне зображення в пряму суму нерозкладних.
- 2) Описати нерозкладні зображення з точністю до еквівалентності на

основі незвідних зображень.

3) Описати незвідні зображення з точністю до еквівалентності.

Відомий результат Машке (див. [37]) твердить, що якщо порядок $|G|$ групи G є оборотним елементом кільця K , то будь-яке нерозкладне матричне зображення над кільцем K є незвідним, що означає повну тотожність задач 2 та 3. Якщо $|G|$ є оборотним елементом кільця K , то характеристика кільця K є 0 або є взаємно простою з $|G|$. В останньому випадку говорять про *класичну теорію зображень*, а в іншому — про *модулярну*.

Над полем у класичному і модулярному випадках першу задачу розв'язати можна і розклади на нерозкладні зображення однозначні, з точністю до порядку слідування доданків і їх еквівалентності (теорема Крулля – Шмідта [61, 135]). Твердження поширюється також на деякі класи комутативних кілець. Воно справедливе для матричних зображень скінченних груп над кільцем цілих чисел $\mathbb{Z}$ (див. [200]). Г. Азумая, З. І. Боревиц, Д. К. Фаддєєв Р. Суон і І. Райнер [15, 100, 202, 211]) довели його над повними дискретно нормованими кільцями, яким, зокрема, є кільце $\mathbb{Z}_p$ цілих p -адичних чисел. Однак, навіть, для кільця цілих алгебраїчних чисел скінченного розширення поля $\mathbb{Q}$, яке не є областю головних ідеалів (яким є $\mathbb{Z}$), (див. [200]) теорема Крулля – Шмідта завжди не виконується. Подібно П. М. Гудивок і Є. Я. Погоріляк [25, 34] показали, що для матричних зображень скінченної p -групи G над дискретно нормованим кільцем K характеристики нуль з полем лишків характеристики p тоді і тільки тоді справедлива теорема Крулля – Шмідта, коли кожне незвідне матричне F -зображення групи G незвідне і над полем F_P , де F — поле відношень кільця K , P — максимальний ідеал кільця

K і F_P — P -адичне замикання поля F .

В класичному випадку над полем розв'язані і однакові за змістом задачі 2 та 3 а кількість незвідних (нерозкладних) зображень є завжди скінченною і не перевищує порядок групи (див. [61,135]). Не зважаючи на розв'язання задачі 2 чи 3 в класичному випадку при переході від полів до довільних комутативних кілець, розв'язання задач сильно ускладнюється. В теорії цілочислових зображень груп перші результати були отримані С. Д. Берманом, П. М. Гудивком і А. Джоунсом [4,8,167], які показали, що число нееквівалентних нерозкладних матричних $\mathbb{Z}$ -зображень скінченної групи G скінченне тоді і тільки тоді, коли для довільного простого числа p , яке ділить порядок групи G , силовська p -підгрупа групи G є циклічною групою порядку p^n ($n \leq 2$). Л. Назарова описала цілочислові зображення абелевої групи типу $(2, 2)$ [64], А. Яковлев — циклічної групи порядку 8 [96]. С. Д. Берман, П. М. Гудивок, А. Хеллер і І. Райнер [3, 5, 156, 157] довели, що число нееквівалентних нерозкладних матричних зображень скінченної групи G над кільцем цілих p -адичних чисел $\mathbb{Z}_p$ скінченне тоді і тільки тоді, коли силовська p -підгрупа групи G циклічна група порядку p^r ($r \leq 2$). У часткових випадках цей результат раніше був одержаний З. І. Боровичем, Д. К. Фадєєвим [15] і А. В. Ройтером [71].

Майже одночасно з початком досліджень зображень над кільцями в 30-х роках ХХ століття починається систематичне дослідження модулярної теорії зображень скінченних груп над полями з робіт Р. Брауера. В модулярному випадку над полем задача 3, яка тепер відрізняється від задачі 2, була розв'язана Р. Брауером, Е. Віттом і С. Д. Берманом [10,125,223]. Кількість незвідних зображень теж виявилася скінченною, яка не перевищує порядок групи. Число ж нерозкладних нееквіва-

лентних зображень скінченної групи скінченне тоді і тільки тоді, коли її силовська p -підгрупа циклічна. Цей результат був отриманий Д. Хігманом [164]. Однак задачу 2 в модулярному випадку в цілому розв'язати не можна.

Задача описання зображення скінченної групи G над полем характеристики p у випадку, коли p ділить порядок групи G (тут і далі ми завжди будемо припускати, що p — просте число), як виявилось, часто містить у собі нерозв'язну задачу про класифікацію з точністю до подібності пар квадратних матриць довільного розміру над деяким полем. Такі задачі називали *дикими*. В. М. Бондаренко і Ю. А. Дрозд [12] показали, що задача описання з точністю до еквівалентності зображень скінченної групи G з силовською p -підгрупою H над полем характеристики p , не є дикою тоді і тільки тоді, коли H є циклічна або коли фактор-група H/H' є абелевою групою типу $(2, 2)$, де H' — комутант групи H . Часткові випадки результату раніше розглядалися В. А. Башевим [2], С. А. Кругляком [60], Ш. Бреннер [127], В. М. Бондаренком [14] і К. Рінгелем [203].

Детальні дослідження зображень скінченних груп над багатьма комутативними кільцями показали, зокрема, що основним випадком є випадок, коли група є p -групою, а кільце є локальним. В дисертаційній роботі розглядаються в основному проблематика модулярної теорії зображень скінченних груп над комутативними локальними кільцями стосовно задач 2, 3. Зрозуміло, що при переході від полів до довільних комутативних кілець у модулярному випадку, розв'язання задачі 3 теж сильно ускладнюється, а сподіватися на розв'язання задачі 2 в загальному не приходить (див., наприклад, [13, 27, 32, 35]). Однак є багато результатів, що досліджують ці задачі для вузьких класів груп, кілець та деяких обмежень на зображення.

В [28] показано, що число нееквівалентних нерозкладних матричних зображень довільного степеня $n > 1$ скінченної нециклічної p -групи ($p \neq 2$) над нескінченним полем характеристики p нескінченне. В [42] аналогічне твердження доведено для матричних зображень скінченної нециклічної p -групи ($p \neq 2$) над комутативним локальним кільцем K характеристики p^s ($s > 0$), якщо K — нескінченне кільце характеристики p або поле лишків кільця K нескінченне. Далі Rad позначає радикал Джекобсона комутативного кільця K . П. М. Гудивок і І. Б. Чухрай [46, 152] довели такі теореми:

- 1) Нехай G — скінченна p -група порядку $|G| > 2$, K — комутативне локальне кільце характеристики p^s ($s > 0$), $\text{Rad } K \neq 0$ і $K/\text{Rad } K$ — нескінченне поле. Тоді число нееквівалентних нерозкладних матричних K -зображень довільного степеня $n > 1$ групи G нескінченне.
- 2) Нехай G — скінченна p -група порядку $|G| > 2$, K — комутативна локальна область цілісності характеристики p , яка не є полем. Тоді число нееквівалентних нерозкладних матричних K -зображень довільного степеня $n > 1$ групи G нескінченне.

П. М. Гудивок [38] показав, що множина степенів всіх нерозкладних матричних зображень скінченної p -групи H порядку $|H| > 1$ над областю K головних ідеалів характеристики p скінченна тоді і тільки тоді, коли група H циклічна і виконується одна із таких умов: 1) K — поле характеристики p ; 2) $|H| = 2$. П. М. Гудивок, В. Й. Погоріляк показали [31, 35, 36], що скінченна p -група G порядку $|G| > 1$ над комутативним локальним кільцем K характеристики p^s ($s \geq 1$), що не є полем, має скінченну множину степенів нерозкладних матричних зображень тоді і тільки тоді, коли $|G| = 2$ і K є кільцем Безу характеристики 2.

Добре відомо [61, 135], що довільне матричне зображення скінченної групи G незвідне над областю головних ідеалів тоді і тільки тоді, коли воно незвідне над її полем відношень F , а число незвідних нееквівалентних зображень групи G над полем F не перевищує порядок групи G .

Крім того, оскільки тривіальне зображення першого степеня — єдине незвідне матричне зображення скінченної p -групи над полем характеристики p [37, 135], то тривіальне зображення першого степеня — єдине незвідне матричне зображення скінченної p -групи над областю головних ідеалів характеристики p .

П. М. Гудивок, Є. Я. Погоріляк та В. М. Орос [33, 66] показали, що над нетеровим факторіальним кільцем характеристики p , яке не є областю головних ідеалів, існує нескінченна кількість нееквівалентних незвідних матричних зображень скінченної p -групи G порядку $|G| > 1$ довільного наперед заданого степеня $n > 1$. В [51, 155] описано всі, з точністю до еквівалентності, незвідні матричні зображення скінченної групи порядку p над комутативним локальним кільцем K характеристики p^s ($s > 0$), де pK — максимальний ідеал кільця K . В [22, 44, 80] з'ясовується, коли множина степенів всіх незвідних матричних зображень скінченної p -групи над нецілісним комутативним нетеровим локальним кільцем характеристики p^s скінченна. В [80] також показано існування незвідних матричних зображень скінченної p -групи G як завгодно високого степеня над цілісним комутативним нетеровим локальним кільцем характеристики p , яке не є областю головних ідеалів, у випадку, коли $|G| > 2$.

Внесок здобувача в розвиток цієї тематики полягає в побудові нових серій незвідних та нерозкладних зображень над деякими комутативними кільцями в модулярному випадку, дослідження еквівалентності побудованих зображень та оцінка їх кількості. Крім того, було знайдено засто-

сування, розроблених методів і, взагалі, методів теорій зображень над комутативними кільцями (в класичному і модулярному випадках) в теорії лінійних груп над комутативними кільцями, цілочислових групових кілець, кодів над скінченними комутативними фробеніусовими кільцями.

Застосування теорії зображень при дослідженні матричних груп виникають природно. Максимальні уніпотентні підгрупи повної лінійної групи $GL(n, F)$ довільного натурального степеня n над полем F довільної характеристики методами теорії зображень були описали з точністю до спряження Мальцев А. І. та Колчин Е. Р. Ними показано (див. [63, 74, 174]), що в цьому випадку всі, з точністю до спряженості, максимальні уніпотентні підгрупи групи $GL(n, F)$ вичерпуються унітрикутною підгрупою. Для поля F характеристики $p > 0$, це негайно означає, що довільна силовська p -підгрупа групи $GL(n, F)$ спряжена з унітрикутною підгрупою. П. М. Гудивок, Є. Я. Погоріляк і В. П. Рудько показали [33, 40], що силовські p -підгрупи повної лінійної групи степеня $n > 1$ над нетеровою локальною областю цілісності L характеристики p попарно спряжені тоді і тільки тоді, коли L — область головних ідеалів. В [33] також описано всі, з точністю до спряженості, силовські p -підгрупи повної лінійної групи над довільною областю головних ідеалів характеристики p . Вони вичерпуються унітрикутною групою.

Логічним продовженням наведених результатів було встановлення здобувачем попарної спряженості максимальних уніпотентних підгруп повної та спеціальної лінійних груп над комутативним кільцем, фактор-кільце якого за первісним радикалом є пряма сума областей Безу.

Ще одним застосуванням теорії зображень виступають дослідження одиниць групових кілець скінченних груп. Поняття групового кільця вперше використали Ф. Г. Фробеніус та І. Шур (див. [1]) як корисний

допоміжний засіб при вивченні зображень скінченних груп. Природно виникає обернений вплив результатів теорії зображень на дослідження в групових кільцях. Дослідження одиниць групового кільця проводили, наприклад, Д. Хігман та С. Д. Берман [1, 7], які мали значний доробок у теорії зображень. Відома гіпотеза Цассенхауза про одиниці цілочислового групового кільця скінченної групи G активно досліджується останнім часом методом Лутара — Пасі [177], який передбачає наявність інформації про незвідні зображення групи G над алгебраїчно замкнутим полем як характеристики 0 так і характеристики p , що ділить порядок групи G . Здобувачем було використано метод Лутара — Пасі, для описання можливих порядків та перевірки гіпотези Цассенхауза для одиниць цілочислового групового кільця групи $PSL(3, 4)$.

Потужні алгебраїчні методи модулярної теорії зображень скінченних груп систематично застосовуються до дослідження лінійних кодів (див. [62, 141, 225]). Зокрема, піонерський підхід С. Д. Бермана [6] розглядав односторонні ідеали в групових алгебрах скінченних груп над скінченними полями, як коди над тими ж полями. Таким способом Ф. Бергард, П. Ландрок, О. Манз [102] побудували розширені коди Галея за групою алгеброю симетричної групи 4 степеня (24-го порядку) над полем з двох елементів, Т. Харлей та І. Маклоглін [185, 186] — за групою алгеброю групи діедра 24-го порядку. Здобувачем, зокрема, було розглянуто цю ж можливість для всіх груп 24-го порядку. Також розглядалися деякі методи побудови інших самодуальних кодів над довільними скінченними фробеніусовими кільцями.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертації пов'язана з науковими дослідженнями на механіко-математичному факультеті Київського національного університету імені

Тараса Шевченка — тема «Застосування алгебро-геометричних методів у теоріях груп, напівгруп, кілець, зображень до задач прикладної алгебри та захисту інформації» (номер державної реєстрації 0111U005264), а також виконувалась у рамках бюджетної дослідницької наукової теми «Зображення скінченних груп та їх застосування» (номер державної реєстрації 0115U007026) кафедри алгебри ДВНЗ «Ужгородського національного університету».

Мета і задачі дослідження. *Метою* дисертаційної роботи є дослідження властивостей модулярних матричних зображень скінченних груп над локальними кільцями, властивостей мономіальних матриці над локальними кільцями, властивостей уніпотентних підгруп лінійних груп над комутативними кільцями та побудова нових самодуальних кодів над фробеніусовими кільцями.

Об'єктом дослідження є модулярні матричні зображення скінченних груп над локальними кільцями, мономіальні матриці над тими ж кільцями, уніпотентні підгрупи лінійних груп над комутативними кільцями одиниці скінченного порядку цілочислових групових кілець та самодуальні коди над фробеніусовими кільцями.

Предметом дослідження є звідність і розкладність матричних зображень скінченних груп і мономіальних матриць, максимальність та спряженість уніпотентні підгрупи лінійних груп порядки одиниць цілочислових групових кілець та їх спряженість та вигляд самодуальних кодів над фробеніусовими кільцями.

Методи дослідження. У дисертаційній роботі використовуються переважно класичні і сучасні методи теорії матриць, методи теорії зображень, комбінаторні методи та методи структурного, функціонального програмування системи комп'ютерної алгебри GAP.

Наукова новизна одержаних результатів. У дисертації автором отримано такі нові результати:

- Встановлено критерій скінченності множини нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи над комутативним нетеровим локальним кільцем характеристики p^s ($s > 0$), яке не є напівпервісним, з нескінченним полем лишків. Показано, що множина нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи над цим кільцем або нескінченна, або порожня.
- Показано нескінченність числа всіх нееквівалентних незвідних матричних зображень наперед заданого степеня $n > 1$ скінченної p -групи G порядку $|G| > 2$ над комутативним нетеровим локальним напівпервісним нецілісним кільцем характеристики p , з нескінченним полем лишків.
- Описано всі, з точністю до еквівалентності, матричні зображення 2-го степеня групи діедра порядку $2p$ (p — непарне просте число) над комутативними локальними кільцями довжини 2 характеристики 2, та з'ясовано критерій їх незвідності.
- Встановлено достатню умову спадкової звідності t -циклічних матриць над комутативним кільцем.
- Встановлено достатню умову спадкової звідності бімономіальних матриць над комутативним кільцем.
- Показана незвідність всіх бімономіальних матриць 7-го порядку над комутативним локальним кільцем довжини $l > 2$.
- Побудована серія нерозкладних унімономіальних зображень циклічної p -групи над скінченним комутативним локальним кільцем скін-

ченної довжини характеристики p , та підраховано число побудованих зображень заданого степеня з точністю до еквівалентності для кожної групи та кільця, зі скінченним полем лишків, окремо.

- Побудована серія нерозкладних унімономіальних зображень циклічної p -групи над довільним комутативним локальним кільцем скінченної довжини характеристики p та підраховано число побудованих зображень заданого степеня з точністю до $*$ -еквівалентності для кожної групи та кільця окремо.
- Побудована серія спадково незвідних унімономіальних зображень циклічної p -групи над скінченним комутативним локальним кільцем головних ідеалів характеристики p , та підраховано число побудованих зображень заданого степеня з точністю до еквівалентності для кожної групи та кільця, зі скінченним полем лишків, окремо.
- Показано, що всі максимальні уніпотентні підгрупи повної лінійної групи над кільцем K попарно спряжені, якщо фактор-кільце кільця K за первісним радикалом є скінченною прямою сумою кілець Безу.
- Показано, що всі максимальні уніпотентні підгрупи спеціальної лінійної групи над кільцем K попарно спряжені, якщо фактор-кільце кільця K за первісним радикалом є скінченною прямою сумою кілець Безу.
- Показано дикийсть за модулем радикалу Джекобсона задачі про описання, з точністю до еквівалентності за модулем головного ідеалу породженого будь-яким елементом довжини більше 2, матриць над локальним факторіальним кільцем, що не є областю головних ідеалів.
- Встановлено, що в цілочисловому груповому кільці скінченної групи

$PSL(3, 4)$ показника 420, який має 23 нетривіальні дільники, можуть бути тільки нетривіальні одиниці порядку: 2, 3, 4, 5, 7 і 6, а для елементів порядку 2 та 3 виконується гіпотеза Цассенхауза.

- Вперше побудовано розширені бінарні коди Галея за груповим кільцем груп $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$ порядку 24 над полем з двох елементів, та підраховано їх кількість. Також показано, що крім вже відомих побудовами для груп D_{24} , S_4 це всі можливі групи 24-го порядку з яких будуються розширені бінарні коди Галея розглядуваним методом.

Теоретичне та практичне значення одержаних результатів.

Побудовані нові серії незвідних та нерозкладних зображень скінченних груп над комутативними локальними кільцями можуть знайти застосування при описанні, з точністю до еквівалентності, окремих серій зображень тих же груп над локальними та довільними комутативними кільцями. Результати дисертаційної роботи про мономіальні матриці над комутативними локальними кільцями знайшли (і можуть знайти нові) застосування при дослідженні модулярних матричних зображень скінченних груп над тими ж кільцями, а також можуть знайти застосування при описанні, з точністю до подібності, окремих серій квадратних матриць над локальними та довільними кільцями. Розроблені методи також застосовувалися (і можуть далі застосовуватися) при дослідженні уніпотентних підгруп лінійних груп над комутативним кільцем, при побудові самодуальних кодів над фробеніусовими кільцями. Результати дисертаційної роботи про самодуальні коди носять пряме практичне значення оскільки побудовані екстремальні коди можуть застосовуватися при кодуванні інформації, для виправлення помилок під час передачі даних каналами зв'язку.

Особистий внесок здобувача. Усі результати дисертаційної роботи, які виносяться на захист, отримано автором самостійно. З результатів робіт, що виконані в співавторстві, на захист виносяться лише положення, що отримано здобувачем. 11 з 21 наукової статі, опублікованих за темою дисертації, є одноосібними.

У статтях [17,48,49] здобувачу належить постановка задачі та загальні ідеї доведення звідності розглядуваних матриць, у статті [106] здобувачу належить загальні ідеї доведення звідності розглядуваних матриць. Отримані результати ввійшли в дисертації на здобуття наукового ступеня кандидата фізико-математичних наук М. Ю. Бортош та Р. Ф. Цімболинець (Динис) [16,93]. Ідеї було розвинуто і узагальнено до альтернативного доведення звідності розглядуваних матриць опублікованого в [107]. В цій статті здобувачу належить доведення основного результату — теореми 2. В. М. Бондаренку належить постановка задачі та загальні ідеї доведення, Й. Гілдеа — перевірка в окремих випадках засобами електронного числення загальних висновків отриманих теоретичним шляхом, Н. В. Юрченко — спрощення викладок доведень допоміжних тверджень 1 та 4.

У статті [108] здобувачу належить результат, про еквівалентність матриць за модулем ідеалу над факторіальним кільцем (теореми 4). Результати про еквівалентність матриць за модулем ідеалу над областями цілісності (теореми 1–3) та над нетеровими областями (теореми 5–7) у випадку, коли ідеал є максимальним належать Стойці М. В. і ввійшли в його дисертаційну роботу на здобуття наукового ступеня кандидата фізико-математичних наук [73].

У статті [105] здобувачу належить підрозділ 1.4 в якому дослідження мономіальних матриць з 2-однорідними послідовностями застосовується для побудови нерозкладних модулярних зображень. У статті [90] здо-

бувачу належить підрозділ 3 в якому нерозкладна мономіальна $n \times n$ -матриця, побудована співавторами в розділі 2, застосовується для побудови нерозкладних модулярних зображень довільного степеня $n \geq 4$.

У статті [149] з Й. Гілдеа останньому належать постановки задач та загальне керування дослідженнями а практична реалізація та ряд конкретних ідей належать здобувачеві. У статті [142] здобувачу належить розділ 3 присвячений побудові розширеним бінарних кодів Голея. У статті [140] здобувачу належить обчислення рангів при доведенні теореми 3.1.

Апробація результатів дисертації. Результати дисертаційної роботи оприлюднено на таких конференціях та семінарах.

- Четверта міжнародна алгебраїчна конференція в Україні (Львів, 4–9 серпня 2003р.).
- Одинадцята міжнародна наукова конференція імені академіка Михайла Кравчука (Київ, 18–20 травня 2006 р.).
- Міжнародна конференція Humboldt-Kolleg Series in Kyiv (Київ, 19–22 листопада 2009).
- Десята відкрита науковій конференція інституту прикладної математики та фундаментальних наук (Львів, 17–18 травня 2012 р.).
- Дев'ята міжнародна алгебраїчна конференція в Україні (Львів, 8–13 липня 2013 р.).
- П'ята міжнародна конференція з аналітичної теорії чисел та просторових мозаїк (Київ, 16–20 вересня 2013 р.)
- Десята міжнародна алгебраїчна конференція в Україні, присвячена 70-річчю Ю. А. Дрозда (Одеса, 20–27 серпня 2015 р.).

- П'ятнадцята міжнародна науковій конференція імені академіка Михайла Кравчука (Київ, 15–17 травня 2014 р.).
- Міжнародна алгебраїчна конференції, присвячена 100-річчю від дня народження Л. А. Калужніна (Київ, 7–12 липня 2014 р.).
- Міжнародна мат. конференція «Методика викладання та методи досліджень в математиці» (Берегове, 21–23 квітня 2016 р.).
- Одинадцята міжнародна алгебраїчна конференція в Україні, присвячена 75-річчю В. В. Кириченка (Київ, 3–7 липня 2017 р.).
- Друга міжнародна конференція про групи, групові кільця і пов'язані теми (Хорфаккан (ОАЕ), 19–22 листопада 2017 р.).
- Міжнародна наукова конференція «Сучасні проблеми механіки та математики» (Львів, 22–25 травня 2018 р.)
- Дванадцята міжнародна алгебраїчна конференція в Україні, присвячена 215-й річниці з дня народження В. Буняковського (Вінниця, 2–6 липня 2019 р.).
- Семінари кафедри алгебри Ужгородського національного університету (Ужгород, 2003–2019).
- Алгебраїчний семінар Інституту математики ім. А. Ренні Угорської академії наук (Будапешт (Угорщина), 2005).
- Науковий семінар відділення інженерії факультету механіки та електронної інженерії Технологічного інституту Сліго (Сліго (Ірландія), 2012).
- Наукові семінари відділення комп'ютерних наук та математики Університету Честер (Честер (Великобританія), 2013, 2019).

- Алгебраїчні семінари Інституту математики Кошицького університету ім. П. Й. Шафарика (Кошице (Словаччина), 2019).
- Алгебраїчний семінар Інституту математики НАН України (Київ, 2019).
- Підсумковий семінар кафедри алгебри та мат. логіки Київського національного університету ім. Т. Шевченка (Київ, 2020).

Публікації. Основні результати дисертації опубліковано в 36 наукових роботах, у тому числі

- 21 статті у фахових наукових виданнях [17, 48, 49, 77–79, 81–84, 87–89, 105–108, 140, 142, 149, 219], 8 із них індексуються в міжнародних наукометричних базах [78, 105–108, 140, 142, 149],
 - 18 статтях у вітчизняних виданнях [17, 48, 49, 77–79, 81–84, 87–89, 105–108, 219],
 - 3 статтях у закордонних виданнях [140, 142, 149];
- 2 статтях інших видань [90, 143];
- 13 тезах наукових конференцій [47, 50, 91, 103, 104, 136, 210, 215–218, 220, 221].

Структура та обсяг дисертації. Дисертаційна робота складається з анотацій українською та англійською мовами, списку публікацій за темою дисертації, переліку умовних позначень, вступу, семи розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації складає 355 сторінки, з яких основний зміст роботи викладено на 303 сторінках. Список використаних джерел містить 225 найменування та займає 28 сторінок.

Автор висловлює щирю вдячність своєму науковому консультанту — доктору фізико-математичних наук, професору Бондаренку Віталію Михайловичу за цікаві ідеї, корисні поради, змістовні дискусії, а також всіляку підтримку та допомогу при підготовці дисертаційної роботи.

Основний зміст роботи

У вступі обґрунтовано актуальність теми дисертації, визначено мету, задачі, об'єкт і предмет дослідження, вказано наукову новизну й теоретичне та практичне значення результатів роботи, наведено інформацію про особистий внесок здобувача та апробацію результатів дослідження, охарактеризовано зміст роботи.

У першому розділі «Попередні відомості» вводяться необхідні поняття і позначення та наводяться відомі результати, які використовуються далі в дисертації. У тому числі наводиться виклад базових понять теорії характерів Фробеніуса, характерів Брауера та результатів про числа нееквівалентних незвідних зображень скінченної групи над полем довільної характеристики. Також наведено результати про числа незвідних зображень скінченних p -груп над комутативними кільцями характеристики p^s в окремих випадках. При побудові серії незвідних нерозкладних зображень скінченних груп над комутативними кільцями використовувалися мономіальні матриці. Було наведено означення мономіальної матриці та її видів канонічно циклічної, бімономіальної, t -циклічної, разом з попередніми результатами досліджень їх подібності, звідності та розкладності. Серія напрямків: уніпотентні підгрупи лінійних груп над комутативними кільцями, дослідження одиниць цілочислового групового кільця, побудова самодуальних кодів над фробеніусовими кільцями де можна використати методи теорії зображень скінчен-

них груп над комутативними кільцями і отримані раніше в цих напрямках результати та розроблені методи описано в заключних підрозділах розділу. Окремо відмічено метод доведення того, що унітрикутна група є силовською p -підгрупою групи повної лінійної групи над напівпервісним комутативне кільце характеристики p . Також було описано метод Лутара — Пасі перевірки гіпотези Цассенхауза для одиниць цілочислового групового кільця. Було введено означення фробеніусового кільця, та описано методи побудов деяких самодуальних кодів над цим кільцем за груповими кільцями.

Другий розділі «Незвідні та звідні модулярні зображення p -груп над комутативними локальними кільцями» присвячено пошуку нових серій незвідних зображень скінченних груп над комутативними локальними кільцями в модулярному випадку.

У підрозділі 2.1 «Вступ» наведено загальні означення для матричних зображень скінченних груп над комутативними кільцями та окреслено спрямованість досліджень розділу.

У підрозділі 2.2 «Зображення скінченних p -груп над кільцями характеристики p^s » з'ясовується, коли є скінченною множина нееквівалентних незвідних зображень заданого степеня скінченної p -груп над комутативним кільцями характеристики p^s , яке не є напівпервісним. Завдання було повністю розв'язане для нетерових кілець, з нескінченним полем лишків та для артінових кілець.

Теорема 2.10. *Нехай G — скінченна p -група порядку $|G| > 1$ і K — комутативне нетерове локальне кільце характеристики p^s ($s > 0$), яке не є напівпервісним, з нескінченним полем лишків. Множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня $n > 1$ скінченна тоді і тільки тоді, коли виконується одна з*

таких умов:

- 1) $|G| = 2$, $s = 1$, $(\text{Rad } K)^2 = 0$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;
- 2) $|G| = 3$, $s = 1$, $(\text{Rad } K)^2 = 0$, $n = 2$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня 2 звідні;
- 3) $|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \notin (p-1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;
- 4) $|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \in (p-1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n та $\frac{n}{p-1}$ звідні.

Зауважимо, що множина нееквівалентних незвідних зображень групи G над кільцем K степеня n або нескінченна, або порожня.

Теорема 2.11. Нехай G — скінченна p -група порядку $|G| > 1$ і K — комутативне артінове локальне кільце характеристики p^s ($s > 0$), яке не є полем. Множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня $n > 1$ скінченна тоді і тільки тоді, коли виконується одна з таких умов:

- 1) поле $K/\text{Rad } K$ скінченне;
- 2) $|G| = 2$, $s = 1$, $(\text{Rad } K)^2 = 0$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;
- 3) $|G| = 3$, $s = 1$, $(\text{Rad } K)^2 = 0$, $n = 2$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня 2 звідні;
- 4) $|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \notin (p-1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;

- 5) $|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \in (p-1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n та $\frac{n}{p-1}$ звідні.

У підрозділі 2.3 «Зображення скінченних p -груп над напівпервісними кільцями характеристики p » з'ясовується, коли є скінченною множина нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи G над комутативним нетеровим локальним напівпервісним нецілісним кільцем характеристики p , поле класів лишків якого нескінченне. Основні результати підрозділу описуються такими двома теоремами.

Теорема 2.12. *Нехай G — скінченна p -група порядку $|G| > 1$ і K — комутативне нетерове локальне напівпервісне кільце характеристики p , яке не є цілісним, з нескінченним полем лишків. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K довільного наперед заданого парного степеня n .*

Теорема 2.13. *Нехай G — скінченна p -група порядку $|G| > 2$ і K — комутативне нетерове локальне напівпервісне кільце характеристики p , яке не є цілісним, з нескінченним полем лишків. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K довільного наперед заданого степеня $n > 1$.*

Цікавим є твердження 2.14 яке встановлює комутативне локальне напівпервісне кільце характеристики 2, яке не є цілісним, всі матричні зображення скінченної групи порядку 2 над яким довільного непарного степеня $n > 1$ звідні.

У підрозділі 2.4 «Зображення скінченних 2-груп над областями цілісності характеристики 2» досліджуються матричні зобра-

ження непарного степеня групи другого прядку над локальною областю цілісності характеристики 2. В підрозділі доведено теорему.

Теорема 2.17. *Нехай K — локальна область цілісності характеристики 2, будь-який скінченно породжений ідеал якої володіє мінімальною системою з не більше ніж двох твірних елементів, $G = \langle a \rangle$ — циклічна група порядку 2. Всі матричні зображення групи G над кільцем K непарного степеня n звідні.*

Раніше здобувачем було показано [80, ст. 110, теорема 2] існування незвідних матричних зображень скінченної p -групи G як завгодно високого степеня над цілісним комутативним нетеровим локальним кільцем характеристики p , яке не є областю головних ідеалів, у випадку, коли $|G| > 2$. Для доведення при цьому будувались незвідні зображення групи G довільного парного степеня вище 6 або довільного степеня кратного 4.

У підрозділі 2.5 «Зображення дієдральних груп порядку $2p$ над кільцями характеристики 2» описуються, з точністю до еквівалентності, матричні зображення 2-го степеня групи дієдра порядку $2p$ (p — непарне просте число) над комутативними локальними кільцями головних ідеалів характеристики 2, радикали Джекобсона яких є нільпотентними ідеалами другого степеня.

Теорема 2.21. *Нехай K — комутативне локальне кільце характеристики 2, $\text{Rad } R = tR$, $t \in K$, $t^2 = 0$, $t \neq 0$, $G = \langle a, b | a^2 = b^p = (ab)^2 = e \rangle$ — група дієдра порядку $2p$ (p — непарне просте число). Γ — матричне зображення 2-го степеня групи G над кільцем K . Якщо поле лишків кільця K містить тільки один корінь p -го степеня з одиниці, то виконується одна з умов:*

1) зображення Γ еквівалентне зображенню вигляду

$$\Gamma_{\overline{F}} : a \rightarrow E_2 + tF, \quad b \rightarrow E_2,$$

де E_2 — одинична матриця порядку 2, F — будь-яка 2×2 -матриця над кільцем K ;

2) зображення Γ еквівалентне зображенню вигляду

$$\Delta : a \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow E_2;$$

3) зображення Γ еквівалентне зображенню вигляду

$$\Lambda_{\alpha} : a \rightarrow \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix},$$

де α — будь-який елемент кільця K такий, що многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$.

Два зображення різних виглядів не еквівалентні над кільцем K . Два зображення $\Gamma_{\overline{F}_1}, \Gamma_{\overline{F}_2}$ (F_1, F_2 — 2×2 -матриці над кільцем K) еквівалентні над кільцем K тоді і тільки тоді, коли матриці $\overline{F}_1, \overline{F}_2$ подібні над полем лишків кільця K . Два зображення $\Lambda_{\alpha_1}, \Lambda_{\alpha_2}$ ($\alpha_1, \alpha_2 \in K$, многочлени $x^2 + \alpha_1 x + 1$ та $x^2 + \alpha_2 x + 1$ ділять $x^p + 1$ у кільці $K[x]$) еквівалентні над кільцем K тоді і тільки тоді, коли $\alpha_1 = \alpha_2$.

Доведена теорема дозволяє також виділити всі, з точністю до еквівалентності, незвідні зображення (наслідок 2.22) групи G над кільцем K якими будуть зображення $\Gamma_{\overline{F}}$ вигляду 1, якщо матриця F після редукції за модулем радикала Джекобсона кільця K є супровідна 2×2 -матриця незвідного многочлена $f(x)$ над полем лишків кільця K , та зображення Λ_{α} вигляду 3.

У третьому розділі «Мономіальні матриці над комутативними кільцями» уточнено результати про звідність мономіальних матриць деяких виглядів та розширено обсяг досліджених мономіальних матриць малих розмірів на предмет звідності.

У підрозділі 3.1 «Означення і позначення» приведено початкові менш загальні означення для розглядуваних квадратних матриць над комутативним кільцем (з одиницею): мономіальної матриці, канонічно циклічної матриці, циклічної матриці, t -циклічної матриці. Зокрема, остання матриця має вигляд

$$M(t, s_1, \dots, s_n) = \begin{pmatrix} 0 & \dots & 0 & t^{s_n} \\ t^{s_1} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & t^{s_{n-1}} & 0 \end{pmatrix}$$

для деякого елемента t розглядуваного кільця.

У підрозділі 3.2 «Спадкова звідність t -циклічних матриць» вводиться поняття спадкової звідності для t -циклічних матриць, яке, зокрема, означає також звичайну звідність матриць, та запропоновано новий підхід до доведення теореми.

Теорема 3.3 ([17, 106]). *Нехай K — комутативне кільце, $t \in K$. t -циклічна матриця $M(t^{s_1}, \dots, t^{s_n})$, де $s_i \geq 0$ ($i = 1, \dots, n$), є спадково звідна, якщо $\sum_{i=1}^n s_i$ і n не є взаємно простими.*

Попереднє доведення було реалізовано в термінах лінійного оператора скінченно вимірного лінійного простору визначеного λ -циклічною матрицею над полем відношень кільця цілочислових многочленів від невідомої λ . Було запропоновано доведення матричним численням, що не спирається на аналіз лінійного оператора скінченно вимірного лінійного

простору над полем, яке буде також застосоване до питання про спадкову звідність біноміальних матриць.

У підрозділі 3.3 «Спадкова звідність біноміальних матриць» вводиться поняття біноміальних матриць та їх спадкової звідності. Біноміальна матриця, з точністю до переставної подібності, має вигляд $M(t, k, n) = M(t, \underbrace{1, \dots, 1}_k, 0, \dots, 0)$ для деякого елемента t розглядуваного кільця, $0 < k < n$. Основним результатом розділу є теорема.

Теорема 3.9. *Нехай K — комутативне кільце, $t \in K$. Біноміальна матриця $M(t, k, n)$ є спадково звідна, якщо k і n не є взаємно простими.*

У підрозділі 3.4 «Незвідність біноміальних матриць 7-го порядку» доведено, що всі матриці $M(t, k, 7)$ ($0 < k < 7$) незвідні над комутативним локальним кільцем K , радикал Джекобсона якого $\text{Rad } K = tK$, $t^2 \neq 0$ ($t \in K$). В [49] Р. Ф. Цімболинець (Динис) одержала, що для $n < 7$, $(n, k) = 1$ матриця $M(t, k, n)$ — незвідна над комутативним локальним кільцем K , радикал Джекобсона якого $\text{Rad } K = tK \neq 0$ ($t \in K$). Якщо $t^2 = 0$ Р. Ф. Цімболинець (Динис) [49, 106] показала, що матриці $M(t, 3, 7)$, $M(t, 4, 7)$ звідні над кільцем K .

Четвертий розділ «Уніноміальні зображення груп над локальними кільцями скінченної довжини» присвячено пошуку нових серій незвідних та нерозкладних уніноміальних зображень скінченних груп над комутативними локальними кільцями в модулярному випадку на основі результатів дослідження мономіальних матриць.

У підрозділі 4.1 «Означення та елементарні властивості уніноміальних зображень» вводиться поняття уніноміальних зображень скінченно породжених груп над комутативними локальними

кільцями. Для побудови незвідних та нерозкладних унімономіальних зображень циклічної p -групи $G = \langle a \rangle$ над комутативним локальним кільцем характеристики p скінченної довжини використовуються зображення вигляду

$$\Gamma: a \rightarrow \Gamma(a) = E_n + M,$$

де E_n — одинична $n \times n$ -матриця, M — канонічно циклічна матриця. Для перевірки відображень заданого вигляду на предмет визначення зображень встановлена теорема.

Теорема 4.4. *Нехай $H = \langle a \rangle$ — циклічна p -група, K — комутативне локальне кільце характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l > 1$, E_n — одинична $n \times n$ -матриця, $s_i \in \mathbb{N} \cup \{0\}$ і $\varepsilon_i \in K^*$ ($i = 1, \dots, n$). Відображення*

$$\Gamma: a \rightarrow E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}),$$

де $\varepsilon_i \in K^$, $s_i \geq 0$ ($i = 1, \dots, n$) є зображенням групи H тоді і тільки тоді, коли*

$$\sum_{j=0}^{|H|-1} s_{i+j} \geq l(i = 1, \dots, n).$$

Тут індекси $i + j$ треба замінити на індекси $i + j - kp$ якщо $i + j > kp$, де k — максимально можливе натуральне число (тобто тут індекси розглядаються за модулем n).

У підрозділі 4.2 «Про число нерозкладних унімономіальних зображень для двозв'язних циклів циклічних p -груп над локальним кільцем характеристики p^s з точністю до еквівалентності» наведено означення двозв'язних циклів та описано результат про нерозкладність канонічно циклічних матриць, що їм відповідають. Було побудовано серію нерозкладних зображень циклічної p -групи G над комутативним локальним кільцем характеристики p довжини 2.

Теорема 4.6. *Нехай K — комутативне локальне кільце характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = 2$. Тоді для будь-якої циклічної p -групи G і $n \geq |G|$, потужність нееквівалентних нерозкладних унімономіальних зображень фіксованого степеня n не менша, ніж $|G| - 2$.*

Також було побудовано серію нерозкладних зображень циклічної p -групи G достатньо великого порядку над комутативним локальним кільцем характеристики p^s довжини $l > 1$.

Теорема 4.7. *Нехай K — комутативне локальне кільце характеристики p^s , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l > 1$. Тоді для циклічної p -групи G деякого порядку N (отже, і більшого порядку), потужність нееквівалентних нерозкладних унімономіальних зображень фіксованого степеня n не менша, ніж $n - 1$ для будь-якого $n > 1$.*

У підрозділі 4.3 «Про число нерозкладних унімономіальних зображень циклічних p -груп над локальним кільцем характеристики p з точністю до еквівалентності» встановлено, що відображення

$$\Gamma: a \rightarrow E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}),$$

де $\varepsilon_i \in K^*$, $0 \leq s_i < l$ ($i = 1, \dots, n$) є нерозкладним унімономіальним зображенням циклічної p -групи $H = \langle a \rangle$ над комутативним локальним кільцем характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l > 1$, коли

- 1) $\sum_{j=0}^{|H|-1} s_{i+j} \geq l$ ($i = 1, \dots, n$),
- 2) послідовність $(s_1, \dots, s_n)$ неперіодична.

Крім того, зображення вказаного вигляду еквівалентні тоді і тільки тоді, коли відповідні послідовності $(s_1, \dots, s_n)$ циклічно еквівалентні а елементи $\prod_{i=1}^n \varepsilon_i$ кільця K рівні за модулем $\text{Ann}(t^s) = \{x \in K \mid t^s x = 0\}$, де s — найбільший член вагової послідовності $\bar{w}$.

Засобами програмування в GAP була обчислена кількість $W(k, l, m, n)$ побудованих нерозкладних зображень, з точністю до еквівалентності, що залежить від порядку k поля відношень кільця K , довжини l локального кільця K , порядку m групи H , тепіні n зображень. Залежність від k подано аналітично, а залежність від інших параметрів — перебором їх малих значень.

У підрозділі 4.4 «Про число нерозкладних унімономіальних зображень циклічних p -груп над локальним кільцем характеристики p з точністю до *-еквівалентності» введене поняття *-еквівалентності зображень циклічних груп, що дозволяє над локальними кільцями абстрагуватися від структури поля лишків і оцінювати потужність побудованих зображень, навіть, коли поле нескінченне.

Було встановлено, що відображення

$$\Gamma: a \rightarrow E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}),$$

де $\varepsilon_i \in K^*$, $0 \leq s_i < l$ ($i = 1 \dots, n$) є нерозкладним унімономіальним зображенням циклічної p -групи $H = \langle a \rangle$ над комутативним локальним кільцем характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l > 1$, коли

- 1) $\sum_{j=0}^{|H|-1} s_{i+j} \geq l$ ($i = 1, \dots, n$),
- 2) послідовність $(s_1, \dots, s_n)$ неперіодична.

Крім того, зображення вказаного вигляду *-еквівалентні тоді і тільки тоді, коли відповідні послідовності $(s_1, \dots, s_n)$ циклічно еквівалентні.

Засобами програмування в GAP була обчислена кількість $X(l, m, n)$ побудованих нерозкладних зображень, з точністю до $*$ -еквівалентності, що залежить від довжини l локального кільця K , порядку m групи H , степені n зображень. Залежність від параметрів подано перебором їх малих значень.

У підрозділі 4.5 «Про число спадково незвідних унімономіальних зображення циклічних p -груп над локальним кільцем характеристики p з точністю до еквівалентності» встановлено, що відображення

$$\Gamma: a \rightarrow E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}),$$

де $\varepsilon_i \in K^*$, $0 \leq s_i < l$ ($i = 1, \dots, n$) є спадково незвідним унімономіальним зображенням циклічної p -групи $H = \langle a \rangle$ над комутативним локальним кільцем характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l > 1$, коли

- 1) $\sum_{j=0}^{|H|-1} s_{i+j} \geq l$ ($i = 1, \dots, n$),
- 2) $(s, n) = 1$, $t^s \neq 0$, де $s = \sum_{i=1}^n s_i$.

Крім того, зображення вказаного вигляду еквівалентні тоді і тільки тоді, коли відповідні послідовності $(s_1, \dots, s_n)$ циклічно еквівалентні а елементи $\prod_{i=1}^n \varepsilon_i$ кільця K рівні за модулем $\text{Ann}(t^s)$, де s — найбільший член вагової послідовності $\overline{w}$.

Засобами програмування в GAP була обчислена кількість $Y(k, l, m, n)$ побудованих спадково незвідних зображень, з точністю до еквівалентності, що залежить від порядку k поля відношень кільця K , довжини l локального кільця K , порядку m групи H , тепіні n зображень. Залежність від k подано аналітично, а залежність від інших параметрів — перебором їх малих значень.

У п'ятому розділі «Уніпотентні підгрупи лінійних груп над комутативними кільцями» встановлюються нові класи повної та спеціальної лінійних груп, що максимальні уніпотентні підгрупи попарно спряжені. Отримані результати застосовуються до вивчення силовських p -підгруп тих же груп над кільцем K , якщо характеристика кільця K рівна p^s ($s \in \mathbb{N}$).

У підрозділі 5.1 «Вступ» описано базові поняття теорії лінійних груп над комутативними кільцями та окреслено напрям досліджень розділу.

У підрозділі 5.2 «Максимальні уніпотентні підгрупи повної лінійної групи» одержано класифікацію максимальних уніпотентних підгруп повної лінійної групи над комутативним кільцем з одиницею, для якого фактор-кільце за первісним радикалом $\text{rad } K$ є скінченна пряма сума кілець Безу.

Теорема 5.4. *Нехай K — комутативне кільце з одиницею, для якого $K/\text{rad } K$ — скінченна пряма сума кілець Безу. Тоді будь-яка максимальна уніпотентна підгрупа групи $GL(n, K)$ спряжена до групи*

$$P = \{X \in GL(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

Тут $\widetilde{T} = (t_{ij} + \text{rad } K)$ — матриця над фактор-кільцем $K/\text{rad } K$ для довільної матриці $T = (t_{ij})$ над кільцем K .

У підрозділі 5.3 «Максимальні уніпотентні підгрупи спеціальної лінійної групи» застосовуються результати досліджень уніпотентних підгруп повної лінійної групи над комутативним кільцем до

повної класифікації з точністю до спряження максимальних уніпотентних підгруп спеціальної лінійної групи над комутативним кільцем з одиницею, для якого фактор-кільце за первісним радикалом $\text{rad } K$ є скінченною прямою сумою кілець Безу. Наводиться розширене формулювання раніше отриманої здобувачем теореми, що описує одну максимальну уніпотентну підгруп повної лінійної групи над довільним комутативним кільцем.

Теорема 5.6. *Нехай K — комутативне кільце.*

$$P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$$

є максимальною уніпотентною підгрупою групи $GL(n, K)$.

Застосовуючи цю теорему та результати попереднього підрозділу показано такі дві теореми.

Теорема 5.7. *Нехай K — комутативне кільце. Тоді*

$$P \cap SL(n, K), \text{ де } P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$$

є максимальною уніпотентною підгрупою групи $SL(n, K)$.

Теорема 5.9. *Нехай K — комутативне кільце. Якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу, то будь-яка максимальна уніпотентна підгрупа групи $SL(n, K)$ спряжена до групи*

$$P \cap SL(n, K), \text{ де } P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

У підрозділі 5.4 «Силовські p -підгрупи повної та спеціальної лінійної групи над кільцем характеристики p^s » застосовано доведені твердження для уніпотентних підгруп до дослідження силовських p -підгруп повної та спеціальної лінійної групи над комутативним кільцем K характеристики p^s . Нехай $P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$.

- P є силовською p -підгрупою групи $GL(n, K)$.
- Якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу, то будь-яка силовська p -підгрупа групи $GL(n, K)$ спряжена до групи P .
- $P \cap SL(n, K)$ є силовською p -підгрупою групи $SL(n, K)$.
- Якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу, то будь-яка силовська p -підгрупа групи $SL(n, K)$ спряжена до групи $P \cap SL(n, K)$.

У шостому розділі «Еквівалентність матриць за модулем ідеалів» досліджується зв'язок між дикістю задачі про описання матриць над факторіальним кільцем з точністю до еквівалентності за модулем ідеалу, і властивостями простих елементів даної області.

У підрозділі 6.1 «Еквівалентність пар матриць над полем» та 6.2 «Еквівалентність матриць та пар матриць над кільцем» описано результати та загальні ідеї пов'язаними з окресленими дослідженнями.

У підрозділі 6.3 «Еквівалентність матриць над факторіальним кільцем» одержано такий результат.

Теорема 6.7. *Нехай K — факторіальне кільце, а $J \neq K$ — його ідеал, що має щонайменше два неасоційовні прості елементи. Тоді для будь-якого елемента $v \in J$, принаймні три з множників розкладу, якого на прості множники належать J , задача класифікації матриць над K за модулем vK є дика за модулем J .*

Показано, що для локального факторіального кільця K , що не є областю головних ідеалів це означає, що для будь-якого елемента v довжи-

ни $l(v) > 2$ задача класифікації матриць над K за модулем vK є дика за модулем радикала Джекобсона кільця K .

У сьомому розділі «Застосування в теорії групових кілець і теорії кодів» засобами теорії зображень над комутативними кільцями розв'язуються низка задач, які формулюються не в термінах теорії зображень а частина має, навіть, прикладне спрямування.

У підрозділі 7.1 «Одиниці скінченного порядку цілочислового групового кільця групи $PSL(3, 4)$ » методом Лутара — Пасі досліджується гіпотеза Цассенхауза про раціональну спряженість одиниць скінченного порядку цілочислового групового кільця скінченної простої групи $PSL(3, 4)$ та з'ясовуються можливі порядки елементів. Основним результатом підрозділу, що також спираються на результати отримані програмним шляхом у системі GAP, є теорема.

Теорема 7.1. *Нехай $G = PSL(3, 4)$ і $u = \sum_{g \in G} \alpha_g g$ — одиниця скінченного порядку групи $V(\mathbb{Z}G)$, $\nu_C = \varepsilon_C(u) = \sum_{g \in C} \alpha_g$ — значення часткового поповнюючого відображення, що відповідає класу спряжених елементів C групи G на одиниці u .*

- 1) Якщо $|u| \in \{2, 3\}$, то u раціонально спряжена з деяким $g \in G$.
- 2) У $V(\mathbb{Z}G)$ немає елементів порядку 10, 12, 14, 15, 21 або 35.
- 3) Якщо $|u| = 4$, тоді $\nu_{rx} = 0$ для будь-якого $rx \notin \{2a, 4a, 4b, 4c\}$ і $(\nu_{2a}, \nu_{4a}, \nu_{4b}, \nu_{4c}) \in \{(2, -1, -1, 1), (2, -1, 0, 0), (0, -1, 0, 2), (2, -1, 1, -1), (0, -1, 1, 1), (0, -1, 2, 0), (-2, -1, 2, 2), (2, 0, -1, 0), (0, 0, -1, 2), (2, 0, 0, -1), (0, 0, 0, 1), (0, 0, 1, 0), (-2, 0, 1, 2), (0, 0, 2, -1), (-2, 0, 2, 1), (2, 1, -1, -1), (0, 1, -1, 1), (0, 1, 0, 0), (-2, 1, 0, 2), (0, 1, 1, -1)\}$.

$$\begin{aligned} &(-2, 1, 1, 1), (-2, 1, 2, 0), (0, 2, -1, 0), (-2, 2, -1, 2), \\ &(0, 2, 0, -1), (-2, 2, 0, 1), \\ &(-2, 2, 1, 0), (-2, 2, 2, -1)\}. \end{aligned}$$

4) Якщо $|u| = 5$, то $\nu_{rx} = 0$ $rx \notin \{5a, 5b\}$ і

$$(\nu_{5a}, \nu_{5b}) \in \{(2, -1), (1, 0), (0, 1), (-1, 2)\}.$$

5) Якщо $|u| = 7$, то $\nu_{rx} = 0$ $rx \notin \{7a, 7b\}$ і

$$(\nu_{7a}, \nu_{7b}) \in \{(2, -1), (1, 0), (0, 1), (-1, 2)\}.$$

6) Якщо $|u| = 6$, тоді $\nu_{rx} = 0$ $rx \notin \{2a, 3a\}$ і

$$(\nu_{2a}, \nu_{3a}) \in \{(4, -3), (-2, 3)\}.$$

У підрозділі 7.2 «Побудова розширених бінарних кодів Голя за груповим кільцем скінченних груп порядку 24» розглядається групове кільце $\mathbb{F}_2G$ групи G порядку 24 над полем $\mathbb{F}_2$ з двох елементів. З'ясовується, коли за деякими дільниками нуля $v \in \mathbb{F}_2G$ можна побудувати розширений бінарний код Голя (тобто бінарним $[24, 12, 8]$ -код) методом вперше застосованим у [102, 185] для симетричної групи S_4 порядку 24 та для групи D_{24} дієдра того ж порядку.

За цим методом код будується, як лінійний код породжений матрицею

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

якщо

$$\left. \begin{aligned} 1) \quad &\sigma(v) = \sigma(v)^T, \\ 2) \quad &\sigma(v)^2 = 0_{24 \times 24}, \\ 3) \quad &\text{rank}(\sigma(v)) = 12, \end{aligned} \right\}$$

якщо 8 є його мінімальна відстань.

Відомо, що є 15 груп з точністю до ізоморфізму порядку 24. В результаті досліджень, що також спираються на результати отримані програмним шляхом у системі GAP, виявилось, що такі коди можна побудувати ще для 3 груп: $G = (C_6 \times C_2) \rtimes C_2$, $G = C_3 \times D_8$ та $G = C_2 \times A_4$ і не можна для інших. В їх групових кільцях є 576, 128 та 384 елементів v відповідно, з яких утворюються коди.

У підрозділі 7.3 «Одна конструкція самодуальних кодів» з'ясовано, коли даний самоортогональний код є самодуальним. Основним результатом є теорема.

Теорема 7.8. *Нехай R скінченне комутативне фробеніусове кільце характеристики 2 і $G = \{g_1, g_2, \dots, g_n\}$ скінченна група порядку n , $(\gamma_1 + \gamma_2)^2 + n(\alpha_1 + \alpha_2)^2 = 0$, $vv^* = 1 + (\alpha_1 + \alpha_2)^2 \hat{g}$ і $(\gamma_1 + 1)\alpha_1 + (\gamma_2 + \mu)\alpha_2 = 0$, де $\hat{g} = \sum_{i=1}^n g_i$ і $\mu = \sum_{i=1}^n \alpha_{g_i}$, то Код $C(v)$ породжений рядками матриці $M(v)$ є самодуальним кодом довжини $2n + 2$ тоді і тільки тоді, коли $(\gamma_1 + n\alpha_1^2, \gamma_2 + n\alpha_2^2, \mu\alpha_1 + \alpha_2)$ має вільний ранг 1.*

Тут

$$M(v) = \left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 & \alpha_2 & \cdots & \alpha_2 \\ \hline \alpha_1 & & & & \alpha_2 & & & \\ \vdots & & & & \vdots & & & \\ \alpha_1 & & & & \alpha_2 & & & \end{array} \right),$$

де $\sigma(v)$ матриця, що відповідає елементу v групового кільця групи G над кільцем R .

РОЗДІЛ 1.

ПОПЕРЕДНІ ВІДОМОСТІ

У цьому розділі дисертації введено основні поняття та позначення і наведено відомі результати про зображення скінченних груп над комутативними кільцями, матриці над комутативними кільцями, одиницями цілочислового групового кільця, лінійні групи над комутативними кільцями, самодуальні коди над фробеніусовими кільцями, які використовуються далі в роботі.

1.1. Зображення скінченних груп над комутативними кільцями

Розвинута Ф. Г. Фробеніусом та У. Бернсайда класична теорія зображень скінченної групи над полем характеристики 0 містить витончені результати на мові характерів, якою, зокрема, розв'язується задача про еквівалентність незвідних, а зрештою і довільних, зображень скінченної групи над алгебраїчно замкнутим полем характеристики 0 [61, 135].

Характером зображення $\pi : G \rightarrow GL(n, F)$ називається функція $\chi_\pi : G \rightarrow F$, визначена так:

$$\chi_\pi(g) = \text{tr } \Gamma(g),$$

де tr — слід матриці.

Характер χ_π називається *незвідним*, якщо π є незвідне зображення. n також називають *степенем* характеру χ_π . Зрозуміло, що над полем характеристики 0 значення χ_π на одиничному елементі групи є розмірністю зображення π . Значення характеру є незмінними на усіх елементах

довільного класу спряжених елементів групи. Над полем характеристики 0, зображення є еквівалентні, тоді і тільки якщо вони мають однакові характери. Кожне значення характеру $\chi_\pi(g)$ є сумою n коренів з одиниці степеня m , де n степінь зображення π і m — порядок елемента g (або показник групи G , щоб не залежав від вибору g). Зокрема, коли F є полем комплексних чисел, кожне таке значення характеру є цілим алгебраїчним числом. Якщо поле F є алгебраїчно замкнутим полем, характеристика якого не ділить $|G|$, то кількість незвідних характерів групи G рівна кількості класів спряжених елементів групи G . Крім того, у цьому випадку степені незвідних характерів є дільниками порядку групи G .

Усі незвідні характери над полем комплексних чисел, які ще називають *характерами Фробеніуса* можна подати за допомогою таблиці характерів, що містить багато корисної інформації про групу G в компактній формі.

	e	x_2	$\dots$	x_l
χ_1	1	1	$\dots$	1
χ_2	n_2	$\chi_2(x_2)$	$\dots$	$\chi_2(x_l)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_l	n_l	$\chi_l(x_2)$	$\dots$	$\chi_l(x_l)$

Кожен рядок, помічається деяким незвідним характером χ_i і в рядку записуються значення цього характеру на елементах класу спряжених елементів групи G . Стовпці таблиці помічаються класами спряжених елементів групи G або їх представниками x_i . Перший рядок зазвичай відповідає характеру тривіального зображення першого степеня, а перший стовпець є класом спряжених елементів одиниці e групи G . Елементами першого стовпця є значення незвідних характерів на одиниці, тобто

розмірності характерів. Характери зображень степеня 1 відомі як лінійні характери. Таблиці характерів завжди є квадратними, тому, що число незвідних неізоморфних зображень дорівнює кількості класів спряжених елементів.

Теорема 1.1 ([61]). *Нехай F — алгебраїчно замкнуте поле, характеристика якого не ділить порядок групи. Тоді число нееквівалентних незвідних зображень групи G над полем F рівне числу класів спряжених елементів групи G .*

Р. Брауером, роботи якого стоять у витоках теорії модулярних зображень скінченних груп, було одержано такий результат.

Теорема 1.2 ([125]). *Нехай F — поле розкладу скінченної групи G , p — характеристика поля F . Тоді число нееквівалентних незвідних зображень групи G над полем F рівне числу класів спряжених p -регулярних елементів групи G .*

Тут p -регулярним елементом групи G називається такий її елемент, порядок якого не ділиться на p .

Нехай R — кільце цілих величин поля комплексних чисел і M деякий максимальний ідеал кільця R , що містить ідеал pR . Покладемо $F = R/M$, яке буде очевидно полем характеристики p . Воно також є алгебраїчно замкнутим полем.

Нехай $\pi : G \rightarrow GL(n, F)$ — зображення групи G над полем F . Нехай U множина p -регулярних елементів групи G . Можна показати, що для довільного $g \in U$ всі характеристичні корені матриці $\pi(g)$ мають вигляд $\varepsilon_1 + M, \dots, \varepsilon_n + M$ для однозначно визначених комплексних коренів $\varepsilon_1, \dots, \varepsilon_n$ з 1 степенів взаємно простих з p . *Характером Брауера зоб-*

раження π називається функція $\chi_\pi : U \rightarrow F$, визначена так:

$$\chi_\pi(g) = \varepsilon_1 + \dots + \varepsilon_n.$$

Характер χ_π ще називають Характером Брауера, що відповідає характеристиці p .

Характер Брауера χ_π називається *незвідним*, якщо π є незвідне зображення. Значення характеру є незмінними на усіх елементах довільного класу спряжених елементів множини U (зрозуміло остання складається з деяких повних класів спряжених елементів групи G). Еквівалентні зображення над полем F мають однакові характери Брауера. Обернене твердження, взагалі кажучи, не вірне, однак для незвідних зображень воно справедливе. Зразу з означення одержуємо, що кожне значення характеру $\chi_\pi(g)$ є цілим алгебраїчним числом. З теореми 1.2 одержуємо, що кількість незвідних характерів групи G рівна кількості класів спряжених p -регулярних елементів групи G . Крім того, у цьому випадку степені незвідних характерів є дільниками порядку групи G .

Як і усі незвідні характери Фробеніуса, усі незвідні характери Брауера, що відповідають фіксованій характеристиці p можна також подати за допомогою аналогічної таблиці характерів, яка при $p \nmid |G|$ буде відмінна від таблиці характерів Фробеніуса, і буде квадратною меншого розміру.

Нехай тепер F — довільне поле характеристики p , $n = p^\alpha m$ — *показник* групи G , тобто найменше спільне кратне порядків елементів групи G ($\alpha \in \mathbb{N} \cup \{0\}$, m — натуральне число, взаємно просте з p). Нехай далі ε — первісний корінь m -го степеня з одиниці, I — мультиплікативна група кільця класів лишків, ізоморфна групі Галуа поля $F(\varepsilon)$ над F .

Два елементи a, b групи G називають *F -спряженими*, якщо $x^{-1}bx = a^r$ для деякого $x \in G$ і деякого $r \in I$. Е. Віттом і С. Д. Берманом було узагальнено теорему 1.2 на випадок довільного поля характеристики p .

Теорема 1.3 ([10, 223]). *Число нееквівалентних незвідних зображень скінченної групи G над полем F характеристики p рівне числу класів F -спряжених p -регулярних елементів групи G .*

Добре відомо [61], що степені незвідних зображень скінченної групи над довільним полем характеристики p не перевищують порядку цієї групи. В 1954 році Д. Хігман з'ясував, коли число нерозкладних нееквівалентних зображень скінченної групи над довільним полем ненульової характеристики скінченне.

Теорема 1.4 ([164]). *Нехай G — скінченна група з силовською p -підгрупою H і F — поле характеристики p . Число нееквівалентних нерозкладних зображень групи G над полем F скінченне тоді і тільки тоді, коли група H циклічна.*

Зауважимо, що і множина степенів нерозкладних зображень скінченної групи з нециклічною силовською p -групою над полем F нескінченна. Степені ж нерозкладних зображень скінченної групи з циклічною силовською p -підгрупою над полем F не перевищують порядок цієї групи. Крім того, С. Д. Берманом були описані [8] всі, з точністю до еквівалентності, нерозкладні зображення скінченної групи з нормальною циклічною силовською p -підгрупою над полем F .

Поряд з теорією модулярних зображень скінченних груп над полями починаючи з 60-х років XX ст. активно досліджуються модулярні зображення скінченних груп над довільними комутативними кільцями характеристики p^s ($s \in \mathbb{N}$).

В. С. Дроботенко, Е. С. Дроботенко, З. П. Жилінська та Є. Я. Погоріляк описали з точністю до еквівалентності нерозкладні зображення циклічної групи порядку p над кільцем $\mathbb{Z}_{p^s}$ класів лишків за модулем p^s

($s \in \mathbb{N}$, $s > 1$). Ними доведено теореми 1.5 і 1.6.

Теорема 1.5 ([51]). *Кожне нерозкладне матричне $\mathbb{Z}_{p^s}$ -зображення групи $G = \langle a \rangle$ порядку $p \neq 2$ ($s \in \mathbb{N}$, $s > 1$) еквівалентне одному з таких зображень:*

$$\begin{aligned} T_1 : a &\longrightarrow E_n + p^{s-1}F_n. \\ T_2 : a &\longrightarrow \Delta \otimes E_n + \Theta(p^{s-1}) \otimes F_n, \\ T_3 : a &\longrightarrow \Omega. \end{aligned}$$

де Δ і Ω — такі $(p-1) \times (p-1)$ -матриця та $p \times p$ -матриця відповідно:

$$\Delta = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ -C_p^1 & -C_p^2 & -C_p^3 & \dots & -C_p^{p-2} & 1 - C_p^{p-1} \end{pmatrix},$$

$$\Omega = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & -C_p^1 & -C_p^2 & \dots & -C_p^{p-2} & 1 - C_p^{p-1} \end{pmatrix}$$

(тут C_p^i — число сполучень з p елементів по i , де $i = 1, \dots, p-1$), $\Theta(\alpha)$ — $(p-1) \times (p-1)$ -матриця, у якій в правому нижньому кутку розташований елемент α , а всі інші рівні нулю; F_n — нормальна форма Фробеніуса $n \times n$ -матриці над простим полем $\mathbb{Z}_{p^s}/p\mathbb{Z}_{p^s}$ характеристики p , $\otimes$ — символ кронекерівського добутку матриць (тут і далі E_n — одинична $n \times n$ -матриця).

Теорема 1.6 ([51]). *Всі нерозкладні нееквівалентні матричні зображення групи $G = \langle a \rangle$ порядку 2 над кільцем класів лишків за модулем 2^s ($s \in \mathbb{N}$, $s > 1$) вичерпуються такими серіями:*

$$T_1 : a \longrightarrow E_n + 2^{s-1}F_n,$$

$$T_2 : a \longrightarrow -E_n + 2^{s-1}F_n,$$

$$T_3 : a \longrightarrow \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Легко бачити, що в теоремах 1.5, 1.6 тільки T_1 і T_2 — незвідні зображення і тільки при умові, що характеристичний поліном матриці F_n незвідний над полем $\mathbb{Z}_{p^s}/p\mathbb{Z}_{p^s}$. Описаний результат узагальнив Т. Ханнула [155] на випадок фактор-кільця R/P^s дискретно нормованого кільця R , в якому p — простий елемент, де P — радикал Джекобсона кільця R і $s > 1$. Інший підхід, що веде до вказаної класифікації, отримав Дж. Тевеназ [212]. Теореми 1.5 і 1.6 також легко узагальнюються на випадок комутативного локального кільця характеристики p^s , власний максимальний ідеал якого породжений елементом p .

Теорема 1.7 ([32, 35]). *Нехай G — скінченна p -група порядку $|G| > 1$, K — комутативне локальне кільце характеристики p^s ($s > 1$), V — максимальний ідеал кільця K . Група G не є дикою над кільцем K тоді і тільки тоді, коли $|G| = p$ и $V = Kp$.*

Для кільця класів лишків $\mathbb{Z}_{p^s}$ аналогічний результат вперше отримав В. М. Бондаренко [13].

Системний виклад досліджень зображень скінченних груп над комутативними локальними кільцями можна знайти в монографії П. М. Гудивка [37].

1.2. Мономіальні матриці

При побудові серії незвідних не нерозкладних модулярних зображень скінченних груп над комутативними локальними кільцями часом використовуються окремі види квадратних матриць, властивості яких досліджуються окремо, один з яких розглянемо зараз.

Нагадаємо, що над довільним комутативним кільцем з одиницею дві квадратні матриці M і M' називаються *подібними*, якщо існує оборотна матриця X така, що $M' = X^{-1}MX$. Сподіватися, взагалі кажучи, на повне описання квадратних матриць з точністю до подібності над багатьма кільцями не приходить. Задача про описання, з точністю до подібності, матриць над комутативним кільцем, що не є полем, містить у собі задачу про пару матриць вже для локальних кілець головних ідеалів; це вперше для областей цілісності доведено в 1974 р. П. М. Гудивком [27], а для кілець з нільпотентним радикалом — у 1976 р. В. М. Бондаренком [13]. Тому дослідження, навіть деяких спеціальних класів матриць, на предмет еквівалентності, розкладності, звідності, тощо є актуальним.

Р. М. Гуральнік [154] звів задачу про подібність матриць над комутативним кільцем до аналогічної задачі для комутативних локальних кілець.

У роботах [72, 94, 99, 193, 193, 195, 196] розглядалась задача про описання з точністю до подібності квадратних матриць малих розмірів над деякими комутативними кільцями. Окрім вказаних робіт, в окресленому напрямку цікавими є, наприклад, роботи [20, 65, 97, 126, 131, 132, 137, 138, 146, 183, 191, 199, 209, 213, 214], а також монографії Б. Р. Макдоналда [184] і В. К. Брауна [128].

Нерозкладність і незвідність матриць, як правило, вивчалася для мат-

риць пов'язаних з матричними зображеннями циклічних груп (див. у зв'язку з цим (окрім [27] і [13]) роботи [9, 23, 24, 41, 51, 52, 71, 139, 156, 157, 168, 172, 189, 190, 201]).

Всюди далі через K будемо позначати комутативне локальне кільце головних ідеалів, що не є полем; через K^* групу його оборотних елементів відносно множення. Тоді єдиний максимальний ідеал (радикал Джекобсона) $\text{Rad } K$ кільця K дорівнює $tK \neq 0$, де t визначається однозначно з точністю до оборотного множника, і будь-який ненульовий елемент $x \in K$ має вигляд εt^s , де $\varepsilon \in K^*$ і $s \geq 0$ (див. [56, ст. 282]). Число s не залежить від вибору t і називається *вагою елемента x* та позначається через $w(x)$. Елемент ε вже залежить від t ; крім того, навіть при фіксованому t , якщо K не є областю цілісності, він визначається елементом x неоднозначно, а саме $\varepsilon t^s = \varepsilon' t^s$ тоді і лише тоді, коли ε і ε' конгруентні за модулем $\text{Ann}(t^s) = \{y \in K \mid yt^s = 0\}$, тобто $\varepsilon - \varepsilon' \in \text{Ann}(t^s)$. Степінь нільпотентності елемента t позначаємо через $l(\text{Rad } K)$. Якщо K — область цілісності, то $l(\text{Rad } K) = \infty$ і навпаки. Якщо K не є областю цілісності, то K називають локальним кільцем довжини $l(\text{Rad } K)$.

$n \times n$ -матриця M над кільцем K називається *мономіальною*, якщо кожний її рядок і стовпець містить рівно один ненульовий елемент. Якщо в описаному вигляді всі ненульові елементи дорівнюють 1, то матриця M називається *переставною*.

Дві довільні $n \times n$ -матриці A і B називаються *переставно подібними*, якщо $X^{-1}AX = B$ для деякої переставної $n \times n$ -матриці X . Легко бачити, що кожна нерозкладна мономіальна матриця M переставно подібна

матриці вигляду

$$M(a_1, \dots, a_n) = \begin{pmatrix} 0 & \dots & 0 & a_n \\ a_1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & a_{n-1} & 0 \end{pmatrix},$$

де $a_i \neq 0$ ($i = 1, \dots, n$), яку слідуючи за [11] назвемо *канонічно циклічною*. Питання подібності мономіальних матриць легко зводиться до питання подібності канонічно циклічних матриць над довільним комутативним кільцем з одиницею. Зрозуміло, що $a_i = \varepsilon_i t^{s_i}$, де $s_i = w(a_i)$ і $\varepsilon_i \in K^*$ (які, згідно з викладеним вище, визначаються a_i неоднозначно). В цьому випадку матрицю $M(a_1, \dots, a_n)$ позначаємо також через $M(\bar{w}, \bar{\varepsilon})$, де $\bar{w} = (s_1, \dots, s_n)$ і $\bar{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$. Очевидно,

$$M(a_1, \dots, a_n) = M(t^{s_1}, \dots, t^{s_n}) \cdot \text{diag}[\varepsilon_1, \dots, \varepsilon_n].$$

Дві послідовності $\bar{x} = (x_1, \dots, x_n)$ і $\bar{y} = (y_1, \dots, y_n)$ з елементами елементами довільної природи назвемо *циклічно еквівалентними*, якщо $\bar{y}$ отримується із $\bar{x}$ циклічною перестановкою її членів: $\bar{y} = (x_k, \dots, x_n, x_1, \dots, x_{k-1})$.

Твердження 1.8 ([11]). *Матриця $M(\bar{b})$ переставно подібна матриці $M(\bar{a})$ тоді і лише тоді, коли їх визначальні послідовності циклічно еквівалентні.*

Теорема 1.9 ([11]). *Матриці $M = M(\bar{w}, \bar{\varepsilon})$ і $M' = M(\bar{w}', \bar{\varepsilon}')$, де $\bar{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$, $\bar{\varepsilon}' = (\varepsilon'_1, \dots, \varepsilon'_n)$, подібні тоді і лише тоді, коли $\bar{w}$ та $\bar{w}'$ циклічно еквівалентні а елементи $\varepsilon = \prod_{i=1}^n \varepsilon_i$ і $\varepsilon' = \prod_{i=1}^n \varepsilon'_i$ кільця K конгруентні за модулем $\text{Ann}(t^s)$, де s — найбільший член вагової послідовності $\bar{w}$.*

Назвемо послідовність $\bar{x} = (x_1, x_2, \dots, x_n)$ з елементами з довільної множини *періодичною*, якщо для деякого натурального $k < n$ $\bar{x} = (x_{k+1}, \dots, x_n, x_1, \dots, x_k)$. У цьому випадку k назвемо періодом послідовності $\bar{x}$. В іншому випадку послідовність $\bar{x} = (x_1, x_2, \dots, x_n)$ називатимемо *неперіодичною*.

Теорема 1.10 ([11]). *Якщо послідовність $\bar{w}$ неперіодична, то матриця $M = M(\bar{w}, \bar{\varepsilon})$ нерозкладна.*

Нагадаємо, що над довільним комутативним кільцем з одиницею квадратна матриця M називається *розкладною*, якщо існує оборотна матриця X така, що

$$X^{-1}MX = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

для деяких квадратних матриць A, B ненульових розмірів і *нерозкладною* в протилежному випадку.

Квадратна матриця M називається *звідною*, якщо існує оборотна матриця X така, що

$$X^{-1}MX = \begin{pmatrix} A & * \\ 0 & B \end{pmatrix}$$

для деяких квадратних матриць A, B ненульових розмірів і *незвідною* в протилежному випадку.

Питання про звідність мономіальних матриць більш складне. Розгля-

немо спочатку мономіальну $n \times n$ -матрицю над кільцем K вигляду:

$$M(t, k, n) = \begin{pmatrix} \overbrace{0 \dots 0}^k & 0 & \dots & 0 & t \\ 1 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & t & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & t & 0 \end{pmatrix}, \quad (1.1)$$

де $0 < k < n$. З результатів досліджень П. М. Гудивка та здобувача [44] випливає наступне твердження.

Теорема 1.11. *Нехай K — комутативне локальне кільце, радикал Джекобсона якого $tK \neq 0$ ($t \in K$). Матриці $M(t, 1, n)$, $M(t, n - 1, n)$, $n > 1$, незвідні над кільцем K .*

За результатами досліджень Р. Ф. Цімболинець (Динис) та здобувача [44] впливають наступні дві теореми.

Теорема 1.12. *Нехай K — комутативне кільце з одиницею 1, $t \in K$, k, n — натуральні числа, $k < n$. Якщо k, n не взаємно прості, то матриця $M(t, k, n)$ звідна над кільцем K .*

Теорема 1.13. *Нехай K — комутативне локальне кільце, радикал Джекобсона якого $tK \neq 0$ ($t \in K$). k, n — натуральні числа, $k < n < 7$. Матриця $M(t, k, n)$ звідна над кільцем K тоді і тільки тоді, коли k, n не взаємно прості.*

Аналогічне твердження при $n = 7$ виявилось невірним. Пізніше теорему 1.12 було узагальнено В. М. Бондаренком, Р. Ф. Цімболинець (Динис), М. Ю. Бортош та здобувачем [17, 106].

Теорема 1.14 ([17,106]). Нехай K — комутативне локальне кільце, n — натуральне число і $s_1, \dots, s_n \geq 0$ цілі числа, такі, що n і $s = \sum_{i=1}^n s_i$ не є взаємно прості. Тоді для довільного спільного дільника $d > 1$ чисел n, s та довільного $t \in R$ канонічна циклічна матриця

$$M(t, s_1, \dots, s_n) = \begin{pmatrix} 0 & \dots & 0 & t^{s_n} \\ t^{s_1} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & t^{s_{n-1}} & 0 \end{pmatrix}$$

звідна над кільцем K .

1.3. Застосування теорії зображень при вивченні лінійних груп

Нагадаємо повною лінійною групою степеня n над кільцем K з одиницею ми називаємо групу оборотних $n \times n$ -матриць над кільцем K , яка позначається $GL(n, K)$. Довільну підгрупу групи $GL(n, K)$ називають лінійною групою степеня n над кільцем K . В силу простоти матричних обчислень обчислення в абстрактних групах, які допускають зображення лінійними, у тій чи іншій мірі замінюють на обчислення в лінійних групах. Такими питаннями, власне, займається теорія зображень груп. Однак природнім є вивчення підгруп повної лінійної групи чи довільної лінійної групи з точністю до спряження безвідносно до можливості зображати ту чи іншу групу.

Такими підгрупами, наприклад, розглядають p -підгрупи (підгрупи порядку кожного елемента якої є степенем простого числа p). p -підгрупу довільної групи, яка не міститься в жодній іншій p -підгрупі цієї ж групи називають силовською p -підгрупою даної групи. Виявляється, якщо ха-

рактеристика кільця над яким розглядаються лінійні групи є степенем числа p , то поняття p -підгрупи лінійної групи тісно пов'язане з поняттям уніпотентної підгрупи. *Уніпотентною підгрупою* лінійної групи називають підгрупу, всі елементи якої уніпотентні матриці. Під *уніпотентною матрицею* розуміємо $n \times n$ -матрицю A , для якої $A - E_n$ — нільпотентна матриця, де E_n — одинична $n \times n$ -матриця. Відповідно *максимальною уніпотентною підгрупою* лінійної групи називають уніпотентну підгрупу, яка не міститься в жодній іншій уніпотентній підгрупі цієї ж групи.

Д. О. Супруненко [75], Р. Т. Вольвачев [18], В. С. Конюх [59], К. Лідгам-Грін та В. Плескен [176] методами теорії зображень повністю описали всі, з точністю до спряження, силовські p -підгрупи повної лінійної групи $GL(n, F)$ над довільним полем F . Виявилось, що при $p > 2$ силовські p -підгрупи групи $GL(n, F)$ попарно спряжені, а при $p = 2$ можуть існувати, навіть, неізоморфні силовські 2-підгрупи групи $GL(n, F)$.

О. Ю. Залесский досліджував [54] силовські p -підгрупи групи $GL(n, T)$, де T — тіло скінченного рангу над своїм центром. В [19, 29, 30, 33, 39, 40, 43, 153] вивчалися силовські p -підгрупи повної лінійної групи над деякими цілісними кільцями.

Легко бачити, що для комутативного кільця K характеристики p (p — просте число) поняття p -підгрупи групи $GL(n, K)$ суміщається з поняттям уніпотентної підгрупи групи $GL(n, K)$. Зрозуміло, що вивчення силовських p -підгруп з точністю до спряження групи $GL(n, K)$ в цьому випадку зводиться до вивчення максимальних уніпотентних підгруп з точністю до спряження тієї ж групи.

Максимальні уніпотентні підгрупи повної лінійної групи $GL(n, F)$ довільного натурального степеня n над полем F довільної характеристики

були описали з точністю до спряження Мальцев А. І. та Колчин Е. Р. Ними показано (див. [74, ст. 262, наслідок 1] або [63, 174]) така теорема.

Теорема 1.15 ([74]). *Нехай F — поле, $n \in \mathbb{N}$. Довільна максимальна уніпотентна підгрупа групи $GL(n, F)$ спряжена з групою $UT(n, F)$.*

Тут і далі $UT(n, K)$ позначає *унітрикутну групу* степеня n над кільцем K тобто групу верхніх трикутних $n \times n$ -матриць над кільцем K з одиницями на головній діагоналі. Хоча проблема описання, з точністю до спряження, максимальних уніпотентних матричних груп над полями була розв'язана окремі властивості цих груп, як, наприклад, проблема Платонова і Потапчика, досліджувалися в [76, 194]. Узагальнення деяких результатів про уніпотентні матричні групи на некомутативний випадок (над тілами) та новий підхід до описання p -підгруп групи $GL(n, F)$ над полем F запропонував В. М. Петечук [67].

Узагальнення результатів про силовські p -підгруп повної лінійної групи над полями характеристики p на деякі області цілісності отримали П. М. Гудивок та Є. Я. Погоріляк. Ними доведені теореми:

Теорема 1.16 ([33]). *Нехай L — область головних ідеалів характеристики p , $n \in \mathbb{N}$. Довільна силовська p -підгрупа групи $GL(n, L)$ спряжена з групою $UT(n, L)$.*

Теорема 1.17 ([33]). *Нехай L — область цілісності з одиницею характеристики p , $n \in \mathbb{N}$. Група $UT(n, L)$ є силовською p -підгрупою групи $GL(n, L)$.*

Для скінченної групи $GL(n, \mathbb{Z}_{p^s})$ ($s \in \mathbb{N}$) описання з точністю до спряженості силовських p -підгруп теж зводиться до описання однієї такої підгрупи. Добре відомо (див., наприклад, [58, ст. 95, вправа 11.3.3]),

що єдиною, з точністю до спряженості, силовською p -підгрупою групи $GL(n, \mathbb{Z}_{p^s})$ є група матриць вигляду:

$$A = \begin{pmatrix} 1 + pa_{11} & a_{12} & \dots & a_{1n} \\ pa_{21} & 1 + pa_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ pa_{n1} & pa_{n2} & \dots & 1 + pa_{nn} \end{pmatrix},$$

де $a_{ij} \in \mathbb{Z}_{p^s}$ ($i = 1, \dots, n; j = 1, \dots, n$).

В [85] здобувачем показано, що для комутативного локального кільця K характеристики p^s такого, що $K/\text{rad } K$ — область Безу, довільна силовська p -підгрупа групи $GL(n, K)$ спряжена з групою всіх $n \times n$ -матриць, які після редукції за модулем первісного радикала $\text{rad } K$ кільця K належить $UT(n, K/\text{rad } K)$. (Первісним радикалом $\text{rad } K$ комутативного кільця K називають ідеал утворений з усіх його нільпотентних елементів.) Крім того, було доведено, що для довільного комутативного кільця K характеристики p^s група всіх $n \times n$ -матриць, які після редукції за модулем первісного радикала $\text{rad } K$ кільця K належить $UT(n, K/\text{rad } K)$, буде силовською p -підгрупою групи $GL(n, K)$. Для доведення було показано, що група $UT(n, K)$ є силовською p -підгрупою повної лінійної групи $GL(n, K)$ над комутативним кільцем K характеристики p , $\text{rad } K = 0$. Ідея доведення останнього була поширена на дослідження уніпотентних підгруп над комутативними кільцями довільної характеристики і, з огляду на це, заслуговує окремого висвітлення.

Нехай K — комутативне кільце (яке завжди вважається кільцем з одиницею), $T(n, K)$ — множина верхніх трикутних $n \times n$ -матриць ($n > 1$) над кільцем K з нулями на головній діагоналі. Для довільних квадратних матриць A і B одного розміру над кільцем K через $A \circ B$ будемо

позначати матрицю $A+B+AB$, $\det M$ — детермінант квадратної матриці M над кільцем K .

Лема 1.18 ([85]). Нехай A — деяка $n \times n$ -матриця ($n > 1$) над кільцем K . Якщо $\det(A \circ B) = 0$ для будь-якої матриці B із $T(n, K)$, то $\det(A + B) = 0$ для довільної матриці B із $T(n, K)$.

Доведення. Нехай B — довільна матриця із $T(n, K)$, E_n — одинична $n \times n$ -матриця над кільцем K . Тоді $E_n - B \in UT(n, K)$. Отже, матриця $E_n - B$ оборотна і $(E_n - B)^{-1} \in UT(n, K)$. Звідси одержимо, що $B' = (E_n - B)^{-1} - E_n \in T(n, K)$. Оскільки $\det(A \circ B') = 0$, то $\det(A + B) = \det(A + E_n - (E_n - B)) = \det((A(E_n - B)^{-1} + (E_n - B)^{-1} - E_n)(E_n - B)) = \det((A(E_n + B') + B')(E_n - B)) = \det((A + B' + AB')(E_n - B)) = \det((A \circ B')(E_n - B)) = 0$. $\square$

Лема 1.19 ([85]). Нехай $A = \|a_{ij}\|$ — деяка $n \times n$ -матриця ($n > 1$) над кільцем K . Якщо $\det(A \circ B) = 0$ для довільної матриці B із $T(n, K)$, то $a_{n1} = 0$.

Доведення. За лемою 1.18 $\det(A + B) = 0$ для будь-якої матриці B із $T(n, K)$. Нехай $B = \|b_{ij}\|$ — довільна матриця із $T(n, K)$, A' і B' відповідно одержані з матриць A і B заміною q -го стовпця на нульовий ($1 \leq q \leq n$). Тоді $B' \in T(n, K)$ і $\det(A + B') = 0$. З адитивної властивості детермінанта відносно елементів q -го стовпця одержимо: $\det(A + B) = \det(A + B') + \det(A' + B)$. Звідси $\det(A' + B) = \det(A + B) - \det(A + B') = 0$.

Нехай матриця A^* одержана з матриці A заміною останніх $n - 1$ стовпців на нульові. Очевидно, $\det(A^* + B) = 0$ для довільної матри-

ці B із $T(n, K)$. Розглянемо

$$B_1 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \in T(n, K).$$

Тоді

$$\det(A^* + B_1) = \det \begin{pmatrix} a_{11} & 1 & 0 & \dots & 0 \\ a_{21} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-11} & 0 & 0 & \dots & 1 \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix} = (-1)^{n+1} a_{n1}$$

і $a_{n1} = 0$. □

Лема 1.20 ([85]). *Нехай P — деяка підгрупа групи $GL(n, K)$ ($n > 1$), E_n — одинична $n \times n$ -матриця над кільцем K . Якщо у всіх матрицях з групи P елемент у деякій фіксованій позиції (i, j) ($i \neq j$) рівний нулю, то рівний нулю і елемент матриці A^r у позиції (i, j) для будь-якого натурального числа r і кожної $n \times n$ -матриці A над кільцем K такої, що $E_n + A \in P$.*

Доведення. Доведемо лему індукцією за числом r . Для $r = 1$ лема, очевидно, виконується. Нехай $r > 1$ і лема виконується для всіх натуральних чисел m менших за r . Нехай далі A — $n \times n$ -матриця над кільцем K , $E_n + A \in P$. Оскільки $(E_n + A)^r \in P$, то елемент матриці $E_n + \sum_{m=1}^{r-1} C_r^m A^m + A^r = (E_n + A)^r$ у позиції (i, j) рівний нулю (тут C_r^m — число сполучень з r елементів по m). За припущенням індукції елемент

матриці A^m у позиції (i, j) рівний нулю ($m = 1, \dots, r - 1$), тому рівний нулю і елемент матриці A^r у цій же позиції. $\square$

Теорема 1.21 ([85]). *Нехай p — просте число, K — комутативне кільце характеристики p , $\text{rad } K = 0$. Група $UT(n, K)$ є силовською p -підгрупою групи $GL(n, K)$.*

Доведення. Легко бачити, що $UT(n, K)$ є p -підгрупою групи $GL(n, K)$. Очевидно, при $n = 1$ $UT(n, K) = \{1\}$ — єдина p -підгрупа групи $GL(n, K)$. Нехай $n > 1$ і P — деяка p -підгрупа групи $GL(n, K)$, що містить групу $UT(n, K)$. Покажемо спочатку, що у всіх матриць з групи P елемент у позиції $(n, 1)$ рівний нулю. Дійсно, нехай A' — довільна матриця з групи P , E_n — одинична $n \times n$ -матриця над кільцем K , $A = A' - E_n$, B — довільна матриця з $T(n, K)$. Тоді $E_n + A \in P$, $E_n + B \in UT(n, K)$. Звідси матриця $E_n + (A \circ B) = E_n + A + B + AB = (E_n + A)(E_n + B) \in P$ є p -елементом групи $GL(n, K)$. Тоді матриця $A \circ B$ нільпотентна і $\det(A \circ B) \in \text{rad } K$. Тому $\det(A \circ B) = 0$. За лемою 1.19 елемент матриці A , а отже, і $A' = E_n + A$ у позиції $(n, 1)$ рівний нулю.

Нехай k — натуральне число ($1 < k < n$) і у всіх матриць групи P елемент у позиції $(i, 1)$ рівний нулю ($i = k+1, \dots, n$). Покажемо, що у всіх матриць з групи P елемент у позиції $(k, 1)$ також рівний нулю. Дійсно, нехай знову A' — довільна матриця з групи P , $A = A' - E_n$, B — довільна матриця з $T(n, K)$. Тоді $E_n + A \in P$, $E_n + B \in UT(n, K)$. Звідси, як і раніше, одержимо $E_n + A \circ B \in P$, матриця $A \circ B$ нільпотентна. За лемою 3 елемент матриці $(E_n \circ A)^r$ у позиції $(i, 1)$ рівний нулю ($i = k+1, \dots, n$; r — натуральне число).

Позначимо через $M(C)$ матрицю, утворену з $n \times n$ -матриці C над кільцем K відкиданням останніх $n - k$ рядків і останніх $n - k$ стовпців. Покажемо, що в матриць $M((A \circ B)^m)$ і $(M(A \circ B))^m$ однакові перші

стовпці при будь-якому натуральному числу m . Застосуємо індукцію за числом m . Для $m = 1$ твердження очевидне. Нехай $m > 1$ і в матриці $M((A \circ B)^{m-1})$ та $(M(A \circ B))^{m-1}$ перший стовпець рівний

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix},$$

де $x_j \in K$ ($j = 1, \dots, k$). Тоді перший стовпець матриці $(M(A \circ B))^m = M(A \circ B) \times (M(A \circ B))^{m-1}$ рівний $M(A \circ B)X$. З іншого боку, у матриці $(A \circ B)^{m-1}$ елемент у позиції $(j, 1)$ рівний x_j ($j = 1, \dots, k$), бо X є першим стовпцем матриці $M((A \circ B)^{m-1})$, а в позиції $(i, 1)$ рівний нулю ($i = k + 1, \dots, n$). Тому стовпець

$$X' = \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

буде першим стовпцем матриці $(A \circ B)^{m-1}$. Звідси одержимо, що перший стовпець матриці $(A \circ B)^m = (A \circ B)(A \circ B)^{m-1}$ рівний

$$(A \circ B)X' = \begin{pmatrix} M(A \circ B)X \\ D \end{pmatrix},$$

де D — деяка $(n - k) \times 1$ -матриця над кільцем K . Тому $M(A \circ B)X$ є першим стовпцем матриці $M((A \circ B)^m)$. Отже, у матриць $M((A \circ B)^m)$ і $(M(A \circ B))^m$ однакові перші стовпці для будь-якого натурального числа m .

Оскільки матриця $A \circ B$ нільпотентна, то для досить великого m перший стовпець матриці $M((A \circ B)^m)$, як і $(M(A \circ B))^m$, рівний нулю. Звідси $(\det M(A \circ B))^m = \det (M(A \circ B)^m) = 0$. Оскільки $\text{rad } K = 0$, то $\det M(A \circ B) = 0$. Легко бачити, що $M(A + B + AB) = M(A) + M(B) + M(AB)$. Так як $B \in T(n, K)$, то $M(AB) = M(A)M(B)$. Отже, $\det (M(A) \circ M(B)) = \det (M(A) + M(B) + M(A)M(B)) = \det M(A + B + AB) = \det M(A \circ B) = 0$.

Нехай B' — довільна матриця з $T(k, K)$. Очевидно, знайдеться така матриця $B_1 \in T(n, K)$, що $B' = M(B_1)$. Тоді $\det (M(A) \circ B') = \det (M(A) \circ M(B_1)) = 0$. За лемою 2 елемент матриці $M(A)$ в позиції $(k, 1)$ рівний нулю, тому рівний нулю і елемент матриці A і $A' = E_n + A$ в позиції $(k, 1)$. Отже, ми показали, що в будь-якій матриці з групи P елемент у позиції $(k, 1)$ рівний нулю для всіх натуральних чисел k ($1 < k \leq n$). Елемент у позиції $(1, 1)$ будь-якої матриці з групи P буде, у такому разі, p -елементом мультиплікативної групи кільця K (для якого $\text{rad } K = 0$) і через це він рівний 1. Отже, будь-яка матриця з групи P має вигляд

$$\begin{pmatrix} 1 & a'_{12} & \dots & a'_{1n} \\ 0 & a'_{22} & \dots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{n2} & \dots & a'_{nn} \end{pmatrix} \quad (a'_{ij} \in K, \ i = 1, \dots, n, \ j = 2, \dots, n).$$

Нескладною індукцією за числом n можна показати, що всі матриці з P містяться в $UT(n, K)$. Тому $UT(n, K)$ є силовською p -підгрупою групи $GL(n, K)$. $\square$

Крім силовських p -підгруп та уніпотентних підгруп повної лінійної групи над полем проводяться багато досліджень таких підгруп довіль-

них лінійних груп над полем. В [55, 69, 70] досліджувалася силовські p -підгрупи алгебраїчних груп матриць над полями. В [187, 207] також досліджуються уніпотентні підгрупи алгебраїчних груп матриць над полями.

Класичним прикладом лінійної групи над комутативним кільцем K відмінної від повної лінійної групи (якщо група K^* нетривіальна) є *спеціальна лінійна група* $SL(n, K)$, яка складається з всіх $n \times n$ -матриць над кільцем K , детермінант яких рівний 1. Легко бачити, що довільний p -елемент повної лінійної групи над полем F характеристики p є матрицею детермінант якої є p -елементом мультиплікативної групи F^* поля F і рівний 1, тому всі силовські p -підгрупи групи $GL(n, F)$ ($n \in \mathbb{N}$, F — поле характеристики p) містяться в спеціальній лінійній групі $SL(n, F)$ і є спряженими за теоремою 1.15 з унітрикутною групою $UT(n, F)$ у групі $GL(n, F)$. Оскільки група $UT(n, F)$ нормалізується групою всіх діагональних невідроджених $n \times n$ -матриць, то довільна підгрупа групи $SL(n, F)$, яка спряжена з $UT(n, F)$ у групі $GL(n, F)$, буде також спряженою з $UT(n, F)$ у групі $SL(n, F)$, а всі силовські p -підгрупи групи $SL(n, F)$ попарно спряжені. В [86] аналогічне питання про попарну спряженість силовських p -підгруп спеціальної лінійної групи $SL(n, K)$ над комутативним кільцем K характеристики p^s зводиться до питання про спряженість силовських p -підгруп групи $GL(n, K)$.

1.4. Групові кільця

Поняття групового кільця вперше використали Ф. Г. Фробеніус та І. Шур на початку минулого століття, як корисний допоміжний засіб при вивченні зображень скінченних груп. Згодом групове кільце стало виступати, як окремий об'єкт досліджень, що знайшов численні застосування,

наприклад, у прикладній теорії кодування.

1.4.1. Одиниці скінченного порядку цілочислових групових кілець. Нехай $\mathbb{Z}G$ — цілочислове групове кільце скінченної групи G , тобто кільце формальних сум вигляду

$$\sum_{g \in G} \alpha_g g,$$

де $\alpha_g \in \mathbb{Z}$ ($g \in G$). Одиниця групи G буде, очевидно, одиницею групового кільця $\mathbb{Z}G$, яку далі позначатимемо 1. Крім того, всі оборотні елементи кільця $\mathbb{Z}G$ прийнято в теорії групових кілець називати *одиницями* кільця $\mathbb{Z}G$. Будемо позначати через $U(\mathbb{Z}G) = (\mathbb{Z}G)^*$ — мультиплікативну групу кільця $\mathbb{Z}G$, яку називають *групою одиниць* кільця $\mathbb{Z}G$. Відображення $\varepsilon : \mathbb{Z}G \rightarrow \mathbb{Z}$, задане за правилом

$$\varepsilon \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} \alpha_g \quad (\alpha_g \in \mathbb{Z}, g \in G)$$

називається *поповнюючим відображенням* кільця $\mathbb{Z}G$. Очевидно, воно є гомоморфізмом аддитивних груп. Крім того, для будь-яких $\sum_{g \in G} \alpha_g g$, $\sum_{h \in G} \beta_h h \in \mathbb{Z}G$ маємо

$$\begin{aligned} \varepsilon \left(\sum_{g \in G} \alpha_g g \sum_{h \in G} \beta_h h \right) &= \varepsilon \left(\sum_{g \in G} \sum_{h \in G} \alpha_g \beta_h gh \right) = \\ \sum_{g \in G} \sum_{h \in G} \alpha_g \beta_h &= \sum_{h \in G} \left(\sum_{g \in G} \alpha_g \right) \beta_h = \left(\sum_{g \in G} \alpha_g \right) \left(\sum_{h \in G} \beta_h \right) = \\ &= \varepsilon \left(\sum_{g \in G} \alpha_g g \right) \varepsilon \left(\sum_{h \in G} \beta_h h \right). \end{aligned}$$

Тобто ε — гомоморфізм кілець.

Нехай $u = \sum_{g \in G} \alpha_g g \in U(\mathbb{Z}G)$. Легко бачити, що $U(\mathbb{Z}G) = \mathbb{Z}^* \times V(\mathbb{Z}G) = \{\pm 1\} \times V(\mathbb{Z}G)$, де

$$V(\mathbb{Z}G) = \{u \in U(\mathbb{Z}G) | \varepsilon(u) = 1\}.$$

$V(\mathbb{Z}G)$ називають нормалізованою мультиплікативною групою групового кільця $\mathbb{Z}G$. Будь-який елемент групи G є, очевидно, одиницею з групи $U(\mathbb{Z}G)$ та, навіть, з $V(\mathbb{Z}G)$. Такі одиниці називають *тривіальними*. Нехай G — скінченна група, під одиницями скінченного порядку завжди розуміємо нетривіальні одиниці скінченного порядку групи $V(\mathbb{Z}G)$. Наступна гіпотеза є одна із важливіших у теорії цілочислових групових кілець.

Гіпотеза 1.22. *Якщо G — скінченна група, то для кожної одиниці скінченного порядку $u \in V(\mathbb{Z}G)$ існує елемент $g \in G$, такий, що $|u| = |g|$.*

Х. Цассенхауз сформулював більш сильну версію цієї гіпотези в [224], в якій говориться наступне.

Гіпотеза 1.23 (Цассенхауза). *Нехай G — скінченна група. Будь-яка одиниця скінченного порядку у $V(\mathbb{Z}G)$ раціонально спряжена з елементом групи G .*

Тут і далі елементи a, b групового кільця $\mathbb{Z}G$ називають *раціонально спряженими*, якщо вони спряжені за допомогою одиниці раціонального групового кільця $\mathbb{Q}G$, тобто

$$a = u^{-1}bu$$

для деякого $u \in U(\mathbb{Q}G)$.

Гіпотеза 1.23 (Цассенхауза) була підтверджена для деяких класів розв'язних груп у [159] та нільпотентних групи в [204, 222]. Актуальним інструмент досліджень цілочислового групового кільця простої групи щодо гіпотези Цассенхауз — метод Лутара — Пассі, який був введений в [177]. Гіпотеза Цассенхауза виявилась також правдивою для всіх груп

до порядку 71, A_5 , S_5 та A_6 , центральних розширення S_5 та інших простих скінченних груп у [98,111,112,162,177,178,206]. Справедливість гіпотези було доведено також для $PSL(2, p)$, коли $p \in \{7, 11, 13\}$ в [161], а для $p \in \{8, 17\}$ у [147]. З подальшими результатами досліджень $PSL(2, p)$ можна ознайомитися в [163].

Нехай $x \in G$ позначимо $x^g = g^{-1}xg$ ($g \in G$) *спряжений елемент* до елемента x за допомогою елемента g в групі G , $x^G = \{x^g | g \in G\}$ *клас спряжених елементів* до елемента x у групі G . *Часткове поповнююче відображення* $\varepsilon_x : \mathbb{Z}G \rightarrow \mathbb{Z}$, що відповідає елементу x чи класу x^G визначається за правилом

$$\varepsilon_x \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in x^G} \alpha_g \quad (\alpha_g \in \mathbb{Z}, g \in G).$$

Очевидно, воно, як і поповнююче відображення, є гомоморфізмом адитивних груп однак, взагалі кажучи, не є гомоморфізмом кілець. Нехай

$$G = C_1 \cup C_2 \cup \dots \cup C_l$$

— об'єднання неперетинаючихся класів спряжених елементів групи G записаних у деякому порядку, такому, що $C_1 = \{1\}$, l — число класів спряжених елементів групи G , $x_1, \dots, x_l$ є представниками відповідних класів спряжених елементів групи G . Зрозуміло

$$\varepsilon(v) = \sum_{i=1}^l \varepsilon_{x_i}(v),$$

для любого $v \in \mathbb{Z}G$.

Часткове поповнююче відображення зв'язує групове кільце $\mathbb{Z}G$ з $\mathbb{Q}G$:

Твердження 1.24 ([177, теорема 2.5], [182]). *Одиниця $u \in V(\mathbb{Z}G)$ скінченного порядку k раціонально спряжена з елементом скінченної*

групи G тоді і тільки тоді, коли всі частково поповнюючі відображення відображають u^d в нуль, крім рівно одного (яке зрозуміло відображає u^d в 1) для всіх дільників d порядку k .

Оскільки всі частково поповнюючі відображення $\varepsilon_{x_1}, \dots, \varepsilon_{x_l}$, на довільному елементі $u \in V(\mathbb{Z}G)$ приймають значення з $\mathbb{Z}$, то за теоремою 1.24 одиниця $u \in V(\mathbb{Z}G)$ скінченного порядку k раціонально спряжена з елементом групи G тоді і тільки тоді, коли

$$\varepsilon_{x_i}(u^d) \geq 0, \quad (i = 1, \dots, l; \ d \text{ ділить } k). \quad (1.2)$$

Д. Хігман і незалежно С. Д. Берман отримали такий результат.

Лема 1.25 ([1,7]). *Нехай G — скінченна група. Якщо $u = \sum_{g \in G} \alpha_g g$ — нетривіальна одиниця скінченного порядку з $V(\mathbb{Z}G)$, то $\alpha_h = 0$ для будь-якого елемента h центру групи G .*

Доведення. Нехай лема невірна. Тоді для деякого $u = \sum_{g \in G} \alpha_g g \in V(\mathbb{Z}G)$ $u \notin G$ і для деякого елемента h центру групи G $\alpha_h \neq 0$. Оскільки $h^{-1} \in V(\mathbb{Z}G)$, то $uh^{-1} \in V(\mathbb{Z}G)$. Оскільки $uh^{-1} = h^{-1}u$, u , h^{-1} — одиниці скінченного порядку, то uh^{-1} — одиниця скінченного порядку. Якщо $uh^{-1} \in G$, то $u = uh^{-1}h \in G$, що неможливо. Тому $u = uh^{-1} = \sum_{g \in G} \beta_g g$ — нетривіальна одиниця скінченного порядку з $V(\mathbb{Z}G)$, $\beta_e = \alpha_h \neq 0$ (e — одиниця групи G).

Нехай n — порядок групи G ,

$$v = \sum_{i=1}^n \alpha_{g_i} g_i \rightarrow R(v) = \begin{pmatrix} \alpha_{g_1 g_1^{-1}} & \alpha_{g_1 g_2^{-1}} & \dots & \alpha_{g_1 g_n^{-1}} \\ \alpha_{g_2 g_1^{-1}} & \alpha_{g_2 g_2^{-1}} & \dots & \alpha_{g_2 g_n^{-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n g_1^{-1}} & \alpha_{g_n g_2^{-1}} & \dots & \alpha_{g_n g_n^{-1}} \end{pmatrix}$$

— *регулярне зображення* кільця $\mathbb{Z}G$, що відповідає деякому порядку $g_1, g_2, \dots, g_n$ елементів групи G і $\omega_1, \dots, \omega_n$ — характеристичні корені матриці $R(y)$. Оскільки $R(y)$ елемент $GL(n, \mathbb{Z})$ скінченного порядку, то $\omega_1, \dots, \omega_n$ — комплексні корені з одиниці і $|\omega_1| = \dots = |\omega_n| = 1$. Слід матриці $R(y)$ рівний $n\beta_e$, а з іншого боку, він також рівний $\sum_{i=1}^n \omega_i$. Тоді

$$n \leq |n\beta_e| = \left| \sum_{i=1}^n \omega_i \right| \leq \sum_{i=1}^n |\omega_i| = n.$$

Отже, $|\sum_{i=1}^n \omega_i| = \sum_{i=1}^n |\omega_i|$ і $\omega_1 = \dots = \omega_n$. Тоді $\omega_1^{-1}R(y)$ елемент $GL(n, \mathbb{Z})$ скінченного порядку з одиничними власними значеннями. Матриця $\omega_1^{-1}R(y)$ подібна над $\mathbb{Q}$ своїй жордановій нормальній формі, яка належить $UT(n, \mathbb{Q})$. Оскільки характеристика поля $\mathbb{Q}$ нуль, то $UT(n, \mathbb{Q})$ не містить неединичних елементів скінченного порядку. Отже, $\omega_1^{-1}R(y) = E_n$ — одинична $n \times n$ -матриця, $R(y) = \omega_1 E_n$. Оскільки $y \in V(\mathbb{Z}G)$, то $1 = \varepsilon(y) = \omega_1$ і $R(y) = E_n$, $y = e$, що неможливо. $\square$

Нехай H — група з множиною елементів скінченного порядку $t(H)$ скінченного показника, а $\#H$ — множина простих дільників порядків елементів з $t(H)$. $\#H$ називають *простим спектром* групи H . *Спектр групи H* називається множина $\omega(H)$ порядків елементів з $t(H)$. Спектр $\omega(H)$ визначає *граф простих чисел* (*граф Грюнберга—Кегеля*) групи H (позначається $\pi(H)$) — граф з вершинами, позначеними простими числами з $\#H$, таким, що вершини p і q сполучено, тоді і тільки тоді, коли $pq \in \omega(H)$. Подана гіпотеза, була представлена, як проблема в [188, проблема 37].

Гіпотеза 1.26 (графа простих чисел). *Якщо G — скінченна група, то $\pi(G) = \pi(V(\mathbb{Z}G))$.*

Гіпотеза графа простих чисел знайшла підтвердження для розв’язних

груп та груп Фробуніуса в [173]. Також було підтверджено для деяких спорадичних простих груп (див., наприклад, [110, 113–122, 124]).

Ми використовуємо метод Лутара–Пассі для отримання необхідних умов, яким задовольняють одиниці скінченного порядку цілочислового групового кільця скінченної групи G . Нехай $u = \sum_{g \in G} \alpha_g g$ — нетривіальна одиниця скінченного порядку з $V(\mathbb{Z}G)$. Якщо позначити χ звичайний характер групи G і D зображення групи G , що реалізує характер χ тоді дія D може бути лінійно поширений до групового кільця $V(\mathbb{Z}G)$, що забезпечує кільцевий гомоморфізм з $\mathbb{Z}G$ в матричне кільце над полем $\mathbb{Q}$, і таким чином одиниці $V(\mathbb{Z}G)$ відображаються в оборотні матриці. Отже, $D(u)$ — оборотна матриця над полем $\mathbb{Q}$. Нехай знову

$$G = C_1 \cup C_2 \cup \dots \cup C_l$$

— об'єднання неперетинаючихся класів спряжених елементів групи G записаних у деякому порядку, такому, що $C_1 = \{1\}$, l — число класів спряжених елементів групи G , $x_1, \dots, x_l$ є представниками відповідних класів спряжених елементів групи G . Оскільки характер χ $\mathbb{Z}$ -лінійна функція, то

$$\chi(u) = \chi\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g \chi(g) = \sum_{i=1}^l \varepsilon_{x_i}(u) \chi(x_i).$$

Позначимо $\chi_1, \dots, \chi_l$ — всі різні незвідні комплексні характери групи G . Тоді $X(G) = (\chi_i(x_j))$ так звана таблиця характерів групи G , що задовольняє умовам

$$\begin{pmatrix} \chi_1(u) \\ \chi_2(u) \\ \vdots \\ \chi_l(u) \end{pmatrix} = \begin{pmatrix} \chi_1(x_1) & \chi_1(x_2) & \dots & \chi_1(x_l) \\ \chi_2(x_1) & \chi_2(x_2) & \dots & \chi_2(x_l) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_l(x_1) & \chi_l(x_2) & \dots & \chi_l(x_l) \end{pmatrix} \begin{pmatrix} \varepsilon_{x_1}(u) \\ \varepsilon_{x_2}(u) \\ \vdots \\ \varepsilon_{x_l}(u) \end{pmatrix} = X(G) \begin{pmatrix} \varepsilon_{x_1}(u) \\ \varepsilon_{x_2}(u) \\ \vdots \\ \varepsilon_{x_l}(u) \end{pmatrix}. \quad (1.3)$$

Оскільки u — одиниця скінченного порядку, то $D(u)$ — оборотна матриця, що має скінченний порядок $|D(u)|$, як елемент мультиплікативної групи. Крім того, $|D(u)|$ ділить $|u|$. Оскільки $D(u)$ діагоналізовувана матриця з власними значеннями, що є коренями степеня $|u|$ з одиниці, то лише скінченна можлива кількість для значень $\chi(u)$. Отже, розглядаючи всі можливі значення $\chi_i(u)$ всіх незвідних зображень групи G на елементі u враховуючи оборотність таблиці характерів, отримаємо з рівняння (1.3) скінченну можливу кількість для значень часткових поповнюючих відображень $\varepsilon_{x_i}(u)$. Якщо припустити, що часткові поповнюючі відображення від u відомі, скажімо, за допомогою індукції, то необхідні умови власних значень $D(u)$ можна значно посилити, оскільки вони можуть бути отримані як відповідні добутки власних значень $D(u^t)$ і $D(u^s)$, де t, s позначають цілі числа, які взаємно прості з $|u|$, такі, що $t + s \equiv 1 \pmod{|u|}$.

Зрозуміло, якщо припустити, що K — алгебраїчно замкнене поле характеристики p , що не ділить $|u|$, тоді аргументи останнього абзацу також застосовні. Застосування відповідності між комплексними коренями з одиниці порядку не кратному p та коренями з одиниці в K , як це прийнято в модулярній теорії зображень, можна розглядати характери Брауера над полем характеристики p , що мають комплексні значення. Гертвек [161, розділ 3] розглянув модулярне продовження ідеї Лютара–Пассі. Суть цього методу полягає в розгляді всіх різних незвідних характерів Брауера $\chi_1, \dots, \chi_h$ над полем характеристики p (для фіксованого простого p), що визначені лише на представниках $x_1, \dots, x_h$ p -регулярних класів спряжених елементів групи G . Гертвек показав, що рівняння вигляду (1.3) також застосовне.

Теорема 1.27. *Нехай G — скінченна група. Якщо u — одиниця скін-*

ченного порядку з $V(\mathbb{Z}G)$, то порядок u ділить $|G|$.

Доведення. Нехай u — одиниця скінченного порядку m з $V(\mathbb{Z}G)$. Розглянемо $e = (1 + u + u^2 + \dots + u^{m-1})/m \in \mathbb{Q}G$. Тоді $eu = e$ і $e^2 = e(1 + u + u^2 + \dots + u^{m-1})/m = (e + e + e + \dots + e)/m = e$. Тобто e — ідемпотент.

Нехай $v \rightarrow R(v)$ — регулярне зображення кільця $\mathbb{Z}G$. Оскільки e — ідемпотент, то $0, 1$ — всі можливі характеристичні корені матриці $R(e)$ і слід матриці $R(e)$ є ціле число в межах $0 \leq \text{tr } R(e) \leq |G|$. Нехай $u = \sum_{g \in G} \alpha_g g$. Тоді за лемою 1.25 $\text{tr } R(u) = n\alpha_1 = 0$, де $n = |G|$ — степінь зображення R і $\text{tr } R(u^i) = 0$ ($i = 1, \dots, m-1$). Крім того, $\text{tr } R(1) = n$. Таким чином

$$\begin{aligned} \text{tr } R(e) &= \text{tr } R((1 + u + u^2 + \dots + u^{m-1})/m) = \\ &= \frac{\text{tr } R(1) + \text{tr } R(u) + \text{tr } R(u^2) + \dots + \text{tr } R(u^{m-1})}{m} = \frac{n + 0 + \dots + 0}{m} = \frac{n}{m}. \end{aligned}$$

Отже, m ділить $n = |G|$. $\square$

Теорема 1.27 була узагальнена Д. Коном та Д. Лівінгстоном [133] до висновку, що порядок одиниці скінченного порядку з $V(\mathbb{Z}G)$ ділить показник групи G .

1.4.2. Застосування зображень групових кілець для побудови самодуальних кодів. Теорія кодування знайшла численні застосування для виявлення і корекції помилок при передачі даних. Особливо цікавою є алгебраїчна теорія кодування, яка ефективно використовує результати теорії груп та групових кілець, теорію зображень групових кілець.

Взагалі при передачі системами зв'язку даних останні можуть розглядатися як послідовності довільної довжини символів деякого скінченного алфавіту. Із міркувань простоти і надійності більшість систем зв'язку

конструюють для передачі послідовностей символів двійкового алфавіту $\{0, 1\}$. За означенням, блочний код замінює кожний блок символів деяким більш довгим блоком із n символів, які після передачі підлягають декодуванню. Останній процес і передбачає виявлення чи виправлення помилок. Таким чином суттєвою характеристикою коду є множина всіх довших блоків із одної і тої ж кількості символів n , які називаються *кодovими словами* а n — їх *довжиною* і тільки вони можуть передаватися на канал зв'язку. Зрозуміло не будь-яка послідовність з n символів даного алфавіту є кодовим словом. *Відстанню Хемінга* між двома кодovими словами називають кількість позицій в яких відрізняються ці слова. *Мінімальною відстанню* коду називають найменшу відстань Хемінга між двома різними кодovими словами. Хороший код має малу довжину n кодovих слів для швидкої передачі повідомлень, велику кількість M кодovих слів щоб дозволяв передавати повідомлення більшої різноманітності, і велику мінімальну відстань d для виявлення або виправлення більшої кількості помилок. Основна проблема теорії кодування — оптимізувати один з параметрів при фіксуванні двох інших.

Власне в алгебраїчній теорії кодування скінченний алфавіт R має структуру кільця з одиницею а *кодом* довжиною n над кільцем R називають будь-яку підмножину вільного R -модуля $R^n = \{(x_1, \dots, x_n) | x_i \in R, i = 1, \dots, n\}$. Елемент $x_i \in R$ для кодового слова $(x_1, x_2, \dots, x_n)$ називають його i -ою *координатою*. Для двійкового алфавіту $\{0, 1\}$ який розглядають, як поле $\mathbb{F}_2$ з двох елементів відповідний код називають *бінарним*. Якщо код є підмодулем R^n , тоді код називається *лінійним кодом*. Далі ми будемо розглядати тільки такі коди над спеціальним класом так званих фробеніусових кілець. Для введення поняття фробеніусового кільця нам будуть потрібні допоміжні конструкції.

Нехай R — скінченне кільце з одиницею. Гомоморфізм адитивних груп $\chi : R \rightarrow \mathbb{Q}/\mathbb{Z}$ називається *характером* кільця R . (З таким же успіхом у ролі $\mathbb{Q}/\mathbb{Z}$ можна було розглядати мультиплікативну групу комплексних чисел $\mathbb{C}^*$ чи, навіть, групу комплексних коренів з одиниці.) Характери кільця R утворюють адитивну групу $\hat{R}$ відносно природно введеної операції додавання. Для характерів $\chi, \psi : R \rightarrow \mathbb{Q}/\mathbb{Z}$ характер $\chi + \psi : R \rightarrow \mathbb{Q}/\mathbb{Z}$ визначається за правилом

$$(\chi + \psi)(r) = \chi(r) + \psi(r) \quad (r \in R).$$

За основною теоремою про скінченні абелеві групи маємо ізоморфізм адитивних груп

$$R \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_l}.$$

Довільному $\alpha = (\alpha_1 + m_1\mathbb{Z}, \dots, \alpha_l + m_l\mathbb{Z}) \in \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_l}$ відповідає характер

$$\chi_\alpha : (\beta_1 + m_1\mathbb{Z}, \dots, \beta_l + m_l\mathbb{Z}) \rightarrow (\alpha_1\beta_1 + m_1\mathbb{Z}, \dots, \alpha_l\beta_l + m_l\mathbb{Z}).$$

Побудоване відображення $\alpha \rightarrow \chi_\alpha$ є, очевидно, ізоморфізм у відповідну групу характерів. Крім того, очевидно, $\chi_\alpha(\beta) = \chi_\beta(\alpha)$ для довільних $\alpha, \beta \in \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_l}$. Отже, існує ізоморфізм адитивних груп $R \rightarrow \hat{R}$ при якому $a \rightarrow \chi_a$, що $\chi_a(b) = \chi_b(a)$ для довільних $a, b \in R$. Адитивна група $\hat{R}$ легко перетворюється в лівий R -модуль введенням множення $r\chi$, що для довільних $r \in R$, $\chi \in \hat{R}$ визначає характер

$$(r\chi)(x) = \chi(xr).$$

Зокрема, для довільних $r_1, r_2 \in R$, $\chi \in \hat{R}$ $(r_1(r_2\chi))(x) = (r_2\chi)(xr_1) = \chi(xr_1r_2) = ((r_1r_2)\chi)(x)$. Тобто

$$(r_1r_2)\chi = r_1(r_2\chi).$$

Правий R -модуль визначається аналогічно введенням множення χr , що для довільних $r \in R$, $\chi \in \hat{R}$ визначає характер

$$(\chi r)(x) = \chi(rx).$$

Кільце R називається *фробеніусовим*, якщо існує *утворюючий справа характер* тобто такий елемент $\chi \in \hat{R}$, що $\hat{R} = \{r\chi | r \in R\}$. Кожен утворюючий справа характер буде також *утворюючим зліва характером* тобто таким елемент $\chi \in \hat{R}$, що $\hat{R} = \{\chi r | r \in R\}$. Такий характер називають просто *утворюючий характер* (фробеніусового) кільця.

Теорема 1.28. *Для скінченного кільця R наступні умови еквівалентні.*

- R — фробеніусове кільце.
- Як лівий модуль, $\hat{R} \cong {}_R R$.
- Як правий модуль, $\hat{R} \cong R_R$.

Тут під ${}_R R$ розуміємо так званий *лівий регулярний модуль*, що природно визначається самим кільцем R , як *правий модуль над собою ж*. Аналогічно вводиться *правий регулярний модуль* R_R .

Для комутативних кілець можна сказати, що R -модуль R є ін'єктивним, а якщо R — скінченне локальне кільце з максимальним ідеалом $\text{Rad } R = M$ і полем лишків k , тоді має місце $\dim_k \text{Ann}(M) = 1$. Усі кільця, що використовуються як алфавіти, далі вважатимуться скінченними комутативними фробеніусовими. Прикладами скінченних комутативних фробеніусових кілець (див., наприклад, [141]) є скінченне поле $\mathbb{F}_q$ з q елементів, кільце класів лишків $\mathbb{Z}_m$ за довільним модулем m , комутативне локальне кільце скінченної довжини з скінченним полем лишків.

Ми приєднуємо до модуля R^n скалярний добуток $(v, w) = \sum_{i=1}^n v_i w_i$ та визначаємо *ортогональне доповнення* до будь-якої підмножини $C \subset R^n$ щодо цього скалярного добутку як $C^\perp = \{v \in R^n \mid (v, w) = 0, \text{ для довільного } w \in C\}$. Ми розглядаємо єдине ортогональне доповнення. Однак у некомутативному випадку, є і ліве, і праве ортогональне доповнення, які можуть відрізнятися. Ортогональне доповнення до будь-якої підмножини модуля R^n є, очевидно, підмодулем модуля R^n . Як було відмічено ми обмежуємося розгляданням тільки скінченних фробеніусових кілець R , оскільки це клас кілець для яких виконується фундаментальний результат у теорії кодування — теорема Мак-Вільямс [180]. З згаданої теореми, зокрема, випливає, що для довільного коду C довжини n над скінченним фробеніусовим кільцем R маємо $|C| \cdot |C^\perp| = |R|^n$.

Код C називається *самоортогональним*, якщо $C \subset C^\perp$ і *самодуальним*, якщо $C = C^\perp$. Кажемо, що два коди C і C' однакової довжини еквівалентні, якщо C може бути утворений від C' шляхом перестановки координат C . У деяких роботах про коди над кільцями, допускається також множення координати на оборотні елементи кільця R при визначенні еквівалентності, але зауважмо, що ми дозволяємо лише перестановку координат у нашому визначенні еквівалентності. *Група автоморфізму* коду C це група перестановок координат кодових слів, що не міняє код C (множину кодових слів).

Розглянемо метод побудову кодів у R^n за допомогою групового кільця RG скінченної групи G . Ця конструкція вперше була застосована для кодів над полями Харлі в [166]. Нехай R скінченне комутативне фробеніусове кільце і нехай $G = \{g_1, g_2, \dots, g_n\}$ скінченної групи порядку n . Нехай $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \dots + \alpha_{g_n} g_n \in RG$. Визначимо матрицю

$\sigma(v) \in M(n, R)$ вигляду

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

Відображення $v \rightarrow \sigma(v)$ розглядається в теорії зображень скінченних груп над кільцями, як *регулярне зображення* кільця RG , що відповідає такому порядку $g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}$ елементів групи G . Для заданого елемента $v \in RG$ визначаємо наступний код над кільцем R : $C(v) = \langle \sigma(v) \rangle$. А саме, код $C(v)$ формується як R -підмодуль R^n породжений рядками матриці $\sigma(v)$. Код $C(v)$, очевидно, лінійний код. Зрозуміло, що код $C(v)$ самоортогональний, якщо $\sigma(v)\sigma(v)^T = 0$. Для елемента $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_n}g_n \in RG$ позначимо $v^* = \alpha_{g_1}g_1^{-1} + \alpha_{g_2}g_2^{-1} + \dots + \alpha_{g_n}g_n^{-1} \in RG$. Відображення $v \rightarrow v^*$ ще називається *канонічною інволюцією*. Канонічна інволюція, як елемент групи всіх взаємно однозначних відображень RG в себе, має порядок 2. Легко бачити, що

$$\sigma(v)^T = (\alpha_{g_i^{-1}g_j})^T = (\alpha_{g_j^{-1}g_i}) = (\alpha_{(g_i^{-1}g_j)^{-1}}) = \sigma(v^*).$$

Лема 1.29. *Нехай R скінченне комутативне фробеніусове кільце і G скінченної група порядку n з елементом v групового кільця RG . Якщо*

$$1) \ v = v^*,$$

$$2) \ v^2 = 0,$$

тоді код $C(v)$ самоортогональний.

Доведення. Оскільки $v \rightarrow \sigma(v)$ — зображення кільця RG , то

$$\sigma(v)\sigma(v)^T = \sigma(v)\sigma(v^*) = \sigma(vv^*) = \sigma(v^2) = \sigma(0) = 0,$$

то код $C(v)$ самоортогональний. □

Тепер ми можемо використати цю лему для побудови самодуальних кодів. Для кодів вигляду $C(v)$ над полями ми могли б просто використувати ранг $\sigma(v)$, однак над довільним скінченним комутативним фробеніусовим кільцем ми не можемо визначити розмір згенерованого коду просто з рангу матриці. Тому використовуватимемо таку теорему.

Лема 1.30. *Нехай R скінченне комутативне фробеніусове кільце і G скінченної групи порядку n з елементом v групового кільця RG . Якщо*

- 1) $v = v^*$,
- 2) $v^2 = 0$,
- 3) $|C(v)| = |R|^{\frac{n}{2}}$,

тоді код $C(v)$ самодуальний.

Доведення. За лемою 1.29 код $C(v)$ самодуальний і $C(v) \subset C(v)^\perp$. За теоремою Мак-Вільямс [180] $|R|^n = |C| \cdot |C^\perp| = |R|^{\frac{n}{2}} \cdot |C^\perp|$. Отже, $|C^\perp| = |C| = |R|^{\frac{n}{2}}$, $C(v) = C(v)^\perp$ і код $C(v)$ самодуальний. $\square$

Дія регулярного зображення σ на певних елементах групового кільця, як частини матриці, рядки якої породжують лінійний код, також використовується [148, 166]. Наступну побудову матриць для кодів над полями вперше запропонував Гарлей у [166]. Нехай R — скінченне комутативне фробеніусове кільце, а $G = \{g_1, g_2, \dots, g_n\}$ — група порядку n .

Визначаємо таку матрицю:

$$M(v) = \left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 & \alpha_2 & \cdots & \alpha_2 \\ \hline \alpha_1 & & & & \alpha_2 & & & \\ \vdots & & & & \vdots & & & \\ \alpha_1 & & & & \alpha_2 & & & \end{array} \right).$$

Для довільного елемента $v \in RG$ визначимо $C(v)$, як лінійний код породжений рядками матриці $M(v)$ над кільцем R .

Теорема 1.31 ([140]). *Нехай R скінченне комутативне фробеніусове кільце характеристики 2 і $G = \{g_1, g_2, \dots, g_n\}$ скінченна група порядку n . Якщо $(\gamma_1 + \gamma_2)^2 + n(\alpha_1 + \alpha_2)^2 = 0$, $(\gamma_1 + 1)\alpha_1 + (\gamma_2 + \mu)\alpha_2 = 0$, $vv^* = 1 + (\alpha_1 + \alpha_2)^2\hat{g}$, де $\hat{g} = \sum_{i=1}^n g_i$, то $C(v)$ самоортогональний код довжини $2n + 2$.*

Доведення. Зрозуміло, що $M(\sigma) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2^T & I_n & A_4^T & \sigma(v) \end{pmatrix}$ де $A_1 = (\gamma_1)$, $A_2 = (\alpha_1 \dots \alpha_1)$, $A_3 = (\gamma_2)$ і $A_4 = (\alpha_2 \dots \alpha_2)$. Тоді

$$M(\sigma)M(\sigma)^T = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2^T & I_n & A_4^T & \sigma(v) \end{pmatrix} \begin{pmatrix} A_1^T & A_2 \\ A_2^T & I_n \\ A_3^T & A_4 \\ A_4^T & \sigma(v)^T \end{pmatrix} =$$

$$\begin{pmatrix} A_1A_1^T + A_2A_2^T + A_3A_3^T + A_4A_4^T & A_1A_2 + A_2 + A_3A_4 + A_4\sigma(v)^T \\ A_2^TA_1^T + A_2^T + A_4^TA_3^T + \sigma(v)A_4^T & A_2^TA_2 + I_n + A_4^TA_4 + \sigma(v)\sigma(v)^T \end{pmatrix}.$$

Крім того,

$$\begin{aligned} & A_1A_1^T + A_2A_2^T + A_3A_3^T + A_4A_4^T = \\ & \gamma_1^2 + (\alpha_1 \dots \alpha_1) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_1 \end{pmatrix} + \gamma_2^2 + (\alpha_2 \dots \alpha_2) \begin{pmatrix} \alpha_2 \\ \vdots \\ \alpha_2 \end{pmatrix} = \\ & \gamma_1^2 + n\alpha_1^2 + \gamma_2^2 + n\alpha_2^2 = (\gamma_1 + \gamma_2)^2 + n(\alpha_1 + \alpha_2)^2 = 0 \end{aligned}$$

і

$$A_2^TA_1^T + A_2^T + A_4^TA_3^T + \sigma(v)A_4^T =$$

$$\begin{aligned} \gamma_1 \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_1 \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_1 \end{pmatrix} + \gamma_2 \begin{pmatrix} \alpha_2 \\ \vdots \\ \alpha_2 \end{pmatrix} + \sigma(v) \begin{pmatrix} \alpha_2 \\ \vdots \\ \alpha_2 \end{pmatrix} = \\ \gamma_1 \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_1 \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_1 \end{pmatrix} + \gamma_2 \begin{pmatrix} \alpha_2 \\ \vdots \\ \alpha_2 \end{pmatrix} + \mu \begin{pmatrix} \alpha_2 \\ \vdots \\ \alpha_2 \end{pmatrix} = 0, \end{aligned}$$

бо $\gamma_1\alpha_1 + \alpha_1 + \gamma_2\alpha_2 + \mu\alpha_2 = 0$. Крім того,

$$\begin{aligned} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_1 \end{pmatrix} \begin{pmatrix} \alpha_1 & \dots & \alpha_1 \end{pmatrix} + I_n + \begin{pmatrix} \alpha_2 \\ \vdots \\ \alpha_2 \end{pmatrix} \begin{pmatrix} \alpha_2 & \dots & \alpha_2 \end{pmatrix} + \sigma(v)\sigma(v^*) = \\ \begin{pmatrix} \alpha_1^2 & \dots & \alpha_1^2 \\ \vdots & \ddots & \vdots \\ \alpha_1^2 & \dots & \alpha_1^2 \end{pmatrix} + I_n + \begin{pmatrix} \alpha_2^2 & \dots & \alpha_2^2 \\ \vdots & \ddots & \vdots \\ \alpha_2^2 & \dots & \alpha_2^2 \end{pmatrix} + \sigma(vv^*) = \\ \begin{pmatrix} \alpha_1^2 + \alpha_2^2 & \dots & \alpha_1^2 + \alpha_2^2 \\ \vdots & \ddots & \vdots \\ \alpha_1^2 + \alpha_2^2 & \dots & \alpha_1^2 + \alpha_2^2 \end{pmatrix} + I_n + \sigma(vv^*). \end{aligned}$$

Оскільки

$$\begin{aligned} \sigma(vv^*) = \sigma(1 + (\alpha_1 + \alpha_2)^2 \hat{g}) = I_n + (\alpha_1 + \alpha_2)^2 \sigma(\hat{g}) = \\ I_n + (\alpha_1 + \alpha_2)^2 \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix} = I_n + \begin{pmatrix} \alpha_1^2 + \alpha_2^2 & \dots & \alpha_1^2 + \alpha_2^2 \\ \vdots & \ddots & \vdots \\ \alpha_1^2 + \alpha_2^2 & \dots & \alpha_1^2 + \alpha_2^2 \end{pmatrix}, \end{aligned}$$

то $A_2^T A_2 + I_n + A_4^T A_4 + \sigma(v)\sigma(v)^T = 0$. Зрозуміло $M(\sigma)M(\sigma)^T$ — симетрична матриця. Отже, $M(\sigma)M(\sigma)^T = 0$ і код C_v є самоортогональним. $\square$

Розглядаючи лінійний код над полем з двох елементів, використовуватимемо термін $[n, k, d]$ -код для позначення лінійних бінарних кодів, де n — довжина кодових слів, k — розмірність підпростору кодових слів і d — мінімальна відстань коду. Легко бачити, що відстань Хемінга між довільними кодовими словами бінарного самодуального коду парна. Бінарний самодуальний код, для якого відстань Хемінга між довільними кодовими словами кратна 4 називається бінарним самодуальним кодом *типу II*, а в іншому випадку бінарним самодуальним кодом *типу I*. Верхня межа мінімальної відстані бінарних самодуальних кодів була знайдена в [198]

Теорема 1.32. *Нехай $d_I(n)$ і $d_{II}(n)$ мінімальна відстань бінарного коду довжини n типу I і II, відповідно. Тоді*

$$d_{II}(n) \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$$

і

$$d_I(n) \leq \begin{cases} 4 \left\lfloor \frac{n}{24} \right\rfloor + 4 & \text{if } n \not\equiv 22 \pmod{24}, \\ 4 \left\lfloor \frac{n}{24} \right\rfloor + 6 & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

Тут $[x]$ позначає цілу частину числа x .

Бінарний код типу I і II, мінімальна відстань якого досягає вказаних у теоремі крайніх значень, називаються *екстремальним*.

Прикладами екстремальних бінарних самодуальних кодів є розширені бінарні коди Голя, які вперше було розглянуто Марселем Дж. Е. Голеем у статті [150] у 1949 році. Ця стаття була названа Е. Р. Берлекемпом [101] «найкращою опублікованою роботою» у теорії кодування. З тих пір такі коди вивчали багато разів і були встановлені багато різних конструкцій для побудови цих кодів у [166, 170, 185, 192].

Розширений бінарний код Голя визначається, як будь-який бінарний лінійний $[24, 12, 8]$ -код. Крім того, відомо [165], що група автоморфізмів

розширеного бінарного коду Голя є група Матьє M_{24} , порядку $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ а відстань Хемінга між двома довільними кодовими словами кратна 4. З останнього, зокрема, легко одержати, що розширений бінарний код Голя самодуальний. Розширений бінарний код Голя є також прикладом екстремального коду типу II ([165]). Його мінімальна відстань $d_{II}(24) = 8 = 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$.

У [102] розширений бінарний код Голя було побудовано у вигляді $C(v)$ з групової алгебри $\mathbb{F}_2 S_4$, де S_4 — симетрична група порядку 24. У [185, 186] аналогічний результат одержано для групи D_{24} дієдра того ж порядку. Для побудови коду з групової алгебри $\mathbb{F}_2 D_{24}$ використовувалася таке твердження, яке тепер легко слідує з леми 1.30.

Теорема 1.33 ([185]). *Нехай G скінченної група порядку 24 з елементом v групового кільця $\mathbb{F}_2 G$. Якщо*

- 1) $\sigma(v) = \sigma(v)^T$,
- 2) $\sigma(v)^2 = 0$,
- 3) $\text{rank}(\sigma(v)) = 12$,

тоді код $C(v)$ самодуальний.

1.5. Висновки до розділу

В цьому розділі викладено основні початкові відомості та основні результати теорії матричних зображень груп та їх застосувань, які потрібні в подальшій роботі. У підрозділі 1.1 наводяться основні твердження теорії матричних зображень скінченних груп над полями та комутативними кільцями. Зокрема, висвітлюється питання про число нееквівалентних

незвідних зображень, питання дикості описання всіх зображень з точністю до еквівалентності та описання всіх з точністю до еквівалентності незвідних зображень для окремих класів груп та кілець. У підрозділі 1.2 вводиться поняття мономіальної матриці та описуються результати досліджень їх еквівалентності, розкладності та звідності над комутативними кільцями та комутативними локальними кільцями головних ідеалів, зокрема. У підрозділі 1.3 описуються результати досліджень уніпотентних підгруп повної та спеціальної лінійних груп над деякими комутативними кільцями. У підрозділі 1.4 описано окремий напрямок дослідження групових кілець а саме дослідження одиниць скінченного порядку цілочислового групового кільця а також застосування групових кілець та зображень скінченних груп при побудові самодуальних кодів над скінченим фробеніусовим кільцем.

Вивчення матричних зображень скінченних груп над комутативними кільцями є предметом багатьох досліджень, що були опубліковані протягом близько століття. У структурній теорії матричних зображень важливе значення мають дослідження нерозкладних та незвідних зображень скінченних груп над комутативними локальними кільцями характеристики p^s . Природною задачею є систематизація отриманих результатів.

РОЗДІЛ 2.

НЕЗВІДНІ ТА ЗВІДНІ МОДУЛЯРНІ ЗОБРАЖЕННЯ p -ГРУП НАД КОМУТАТИВНИМИ ЛОКАЛЬНИМИ КІЛЬЦЯМИ

Протягом всього розділу K будемо позначати комутативне локальне кільце з одиницею, G — скінченну групу, $GL(n, K)$ — повну лінійну групу степеня n над кільцем K (мультіплікативну групу оборотних матриць порядку $n > 0$ над кільцем K), $\text{Rad } K$ — радикал Джекобсона кільця K , $\text{rad } K$ — первісний радикал кільця K , тобто ідеал утворений з всіх нільпотентних елементів кільця K , K^* — мультіплікативну групу кільця K . Кільце K для якого $\text{rad } K = 0$ називається *напівпервісним*. Таким чином комутативне локальне кільце буде напівпервісним, якщо воно не містить ненульових нільпотентних елементів.

Також елемент $t + \text{Rad } K$ поля лишків $K/\text{Rad } K$ кільця K позначаємо через $\bar{t}$ і для (довільної) матриці $T = (t_{ij})$ над кільцем K покладемо $\bar{T} = (\bar{t}_{ij})$. Якщо для матриць однакового розміру T та U над кільцем K всі елементи $T - U$ належать деякому ідеалу I кільця K , то це позначатимемо $T \equiv U \pmod{I}$. через $\det M$ — детермінант квадратної матриці M над комутативним кільцем, $\text{diag}[\alpha_1, \alpha_2, \dots, \alpha_n]$ — діагональну $n \times n$ -матрицю з діагональними елементами $\alpha_1, \alpha_2, \dots, \alpha_n$, $\text{Ann } a = \{x \in K | ax = 0\}$ — анулятор елемента $a \in K$ в кільці K .

2.1. Вступ

Нагадаємо деякі загальні означення для матричних зображень скінченних груп над комутативними кільцями. Гомоморфне відображення

$$\Gamma : G \longrightarrow GL(n, K)$$

називається *матричним зображенням* групи G над кільцем K степеня n . Матричні зображення Γ і Δ групи G над кільцем K степеня n називаються *еквівалентними* над кільцем K , якщо існує оборотна матриця C над кільцем K така, що

$$\Gamma(g) = C^{-1}\Delta(g)C \quad (g \in G).$$

Матричне зображення Γ групи G над кільцем K степеня n над кільцем K називаються *звідним* над кільцем K , якщо воно еквівалентне над кільцем K до зображення Δ вигляду

$$\Delta : g \rightarrow \begin{pmatrix} \Delta_1(g) & * \\ 0 & \Delta_2(g) \end{pmatrix} \quad (g \in G),$$

де Δ_1, Δ_2 — матричні зображення групи G над кільцем K степеня n_1 та n_2 , відповідно і *незвідним* над кільцем K в іншому випадку. Матричне зображення Γ групи G над кільцем K степеня n називаються *розкладним* над кільцем K , якщо воно еквівалентне над кільцем K до зображення Δ вигляду

$$\Delta : g \rightarrow \begin{pmatrix} \Delta_1(g) & 0 \\ 0 & \Delta_2(g) \end{pmatrix} \quad (g \in G),$$

де Δ_1, Δ_2 — матричні зображення групи G над кільцем K степеня n_1 та n_2 , відповідно і *нерозкладним* над кільцем K в іншому випадку.

Поняття звідності та розкладності часто застосовується і до довільних множин матриць, які не утворюють групу, як образ зображення. Ми

застосовуватимемо ці поняття для одної матриці. Квадратна матриця M називається *звідною* над кільцем K , якщо існує оборотна матриця C над кільцем K така, що

$$C^{-1}MC = \begin{pmatrix} A & * \\ 0 & B \end{pmatrix},$$

де A і B — квадратні матриці ненульових розмірів, і *незвідною* в протилежному випадку. Квадратна матриця M називається *розкладною* над кільцем K , якщо існує оборотна матриця C над кільцем K така, що

$$C^{-1}MC = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

де A і B — квадратні матриці ненульових розмірів, і *нерозкладною* в протилежному випадку.

Далі в межах розділу досліджуватимемо незвідні зображення скінченних груп над деякими комутативними локальними кільцями в модулярному випадку. Ці кільця заслуговують на увагу як такі, які можна використати при дослідженні зображення скінченних груп над довільними комутативними кільцями. Огляд досліджень зображень над комутативними локальними кільцями можна знайти в [37]. Зауважмо тільки, що В. М. Бондаренко вияснив [13], коли буде дикою задача описання всіх, з точністю до еквівалентності, матричних зображень скінченної p -групи G над кільцем $\mathbb{Z}_{p^s}$ класів лишків за модулем p^s , яке не є полем. У випадку, коли згадана задача не є дикою, незвідні і нерозкладні матричні зображення групи G над кільцем $\mathbb{Z}_{p^s}$, яке не є полем, були описані В. С. Дроботенком, Е. С. Дроботенком, З. П. Жилінською та Є. Я. Погоріляк [51]. Цей результат узагальнив Т. Ханнула [155] на випадок зображень циклічної групи порядку p над фактор-кільцем $K/(\text{Rad } K)^s$ дискретно нормованого кільця K , в якому p — простий елемент, $s > 1$.

2.2. Зображення скінченних p -груп над кільцями характеристики p^s

В цьому підрозділі вивчається, коли є скінченною множина нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи над комутативним нетеровим локальним кільцем характеристики p^s ($s > 0$), яке не є напівпервісним.

Твердження 2.1. *Нехай K — комутативне артінове кільце з одиницею. Кільце K скінченне тоді і тільки тоді, коли кільце $K/\text{Rad } K$ скінченне.*

Доведення. Необхідність очевидна. Нехай кільце $K/\text{Rad } K$ скінченне і $\varepsilon_1, \dots, \varepsilon_s$ — представники всіх різних суміжних класів кільця K за ідеалом $\text{Rad } K$. Тоді $K = \bigcup_{1 \leq j \leq s} (\varepsilon_j + \text{Rad } K)$. Оскільки кільце K артінове, а отже, і нетерове, то ідеал $\text{Rad } K$ скінченно породжений. Нехай $u_1, \dots, u_l$ — система твірних ідеалу $\text{Rad } K$. Тоді $\text{Rad } K = \sum_{i=1}^l u_i K$. Вважатимемо, що $(\text{Rad } K)^0 = K$. Оскільки кільце K артінове, то для деякого $r > 0$ $(\text{Rad } K)^r = 0$. Припустимо тепер, що ідеал $(\text{Rad } K)^{m+1}$ теж скінченний для деякого $0 \leq m < r$. Очевидно, $(\text{Rad } K)^m = \sum_{i_1=1}^l \dots \sum_{i_m=1}^l u_{i_1} \dots u_{i_m} K = \sum_{i_1=1}^l \dots \sum_{i_m=1}^l u_{i_1} \dots u_{i_m} \times \bigcup_{1 \leq j \leq s} (\varepsilon_j + \text{Rad } K) \subset \sum_{i_1=1}^l \dots \sum_{i_m=1}^l \bigcup_{1 \leq j \leq s} (u_{i_1} \dots u_{i_m} \varepsilon_j + (\text{Rad } K)^{m+1})$. Отже, ідеал $(\text{Rad } K)^m$ скінченний. Зокрема, скінченним є і кільце $K = (\text{Rad } K)^0$. $\square$

Теорема 2.2. *Нехай G — скінченна нециклічна p -група і K — комутативне локальне кільце характеристики p^s ($s > 0$), яке не є напівпервісним, з нескінченним полем лишків. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем*

K довільного наперед заданого степеня $n > 1$.

Доведення. Згідно [61, ст. 32, (6.10)] довільна скінченна нециклічна p -група має абелеву фактор-групу типу (p, p) . Оскільки будь-яке незвідне матричне зображення фактор-групи групи G над кільцем K визначає незвідне матричне зображення групи G над кільцем K того ж степеня і ця відповідність зберігає відношення еквівалентності, то досить розглянути випадок, коли $G = \langle a \rangle \times \langle b \rangle$ — група типу (p, p) .

У випадку, коли $s > 1$ покладемо $u = p$. За умовою теореми кільце K містить ненульовий нільпотентний елемент. У випадку, коли $s = 1$ покладемо u рівним довільному ненульовому нільпотентному елементу кільця K . При будь-якому з двох можливих випадків u — ненульовий нільпотентний елемент кільця K . Нехай r — степінь нільпотентності елемента u , тоді $r > 1$. Покладемо $t = u^{r-1}$. Очевидно, $t \neq 0$. Так як $(r-1)2 \geq (r-1) + 1 = r$, то $t^2 = u^{(r-1)2} = 0$. Якщо $s > 1$, то $u = p$. Враховуючи, що p^s — характеристика кільця K , маємо $r = s$, $t = p^{s-1}$ і $pt = p^s = 0$. Якщо $s = 1$, то $p = 0$ і $pt = 0$. Отже, при будь-якому з двох можливих випадків t — нільпотентний елемент другого степеня такий, що $pt = 0$.

Нехай E — одинична матриця порядку n . Розглянемо відображення Γ_λ вигляду:

$$a \longrightarrow E + tM_1, \quad b \longrightarrow E + t\lambda M_2,$$

де λ — оборотний елемент кільця K , M_1, M_2 — $n \times n$ -матриці над кільцем

K вигляду:

$$M_1 = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}. \quad (2.1)$$

Оскільки E_n та tM_1 комутують, то

$$\Gamma(a_1)^p = (E_n + tM_1)^p = E_n + \sum_{i=1}^{p-1} C_p^i t^i M_1^i + t^p M_1^p.$$

Враховуючи, що $C_p^i = c_p^i p$ ($c_p^i \in \mathbb{N}$; $i = 1, \dots, p-1$), $pt = 0$, маємо

$$\Gamma(a_1)^p = E_n + \sum_{i=1}^{p-1} c_p^i p t t^{i-1} M_1^i + t^p M_1^p = E_n + t^p M_1^p.$$

Враховуючи, що $p \geq 2$ і $t^2 = 0$, маємо

$$\Gamma(a_1)^p = E_n + t^2 t^{p-2} M_1^p = E_n.$$

Аналогічно, $\Gamma(a_2)^p = E_n$. Крім того,

$$\Gamma(a_1)\Gamma(a_2) = (E_n + tM_1)(E_n + t\lambda M_2) = (E_n + t\lambda M_2 + tM_1),$$

$$\Gamma(a_2)\Gamma(a_1) = (E_n + t\lambda M_2)(E_n + tM_1) = (E_n + tM_1 + t\lambda M_2).$$

Тому $\Gamma(a_1)\Gamma(a_2) = \Gamma(a_2)\Gamma(a_1)$. Отже, Γ є зображенням групи G над кільцем K .

Припустимо, що зображення Γ звідне над кільцем K . Тоді знайдеться така матриця $C \in GL(n, K)$, що

$$tC^{-1}M_1C = t \begin{pmatrix} A_1 & D_1 \\ 0 & B_1 \end{pmatrix}, \quad t\lambda C^{-1}M_2C = t\lambda \begin{pmatrix} A_2 & D_2 \\ 0 & B_2 \end{pmatrix}, \quad (2.2)$$

де A_j і B_j — $r \times r$ -матриця та $(n-r) \times (n-r)$ -матриця над кільцем K відповідно ($j = 1, 2$; $1 \leq r < n$). Нехай $S = \|\alpha_{ij}\|$ ($\alpha_{ij} \in K$). Позначимо $\bar{S} = \|\alpha_{ij} + \text{Rad } K\|$. Оскільки λ — оборотний елемент кільця K , то елемент $t\lambda$, як і t , відмінний від нуля. З (2.2) одержимо, що над полем $K/\text{Rad } K$

$$\bar{C}^{-1} \bar{M}_j \bar{C} = \begin{pmatrix} \bar{A}_j & \bar{D}_j \\ 0 & \bar{B}_j \end{pmatrix} \quad (j = 1, 2),$$

що суперечить [44, ст. 78, лема 1]. Отже, Γ — незвідне зображення групи H над кільцем K .

Нехай $\lambda', \lambda'' \in K$; $\lambda', \lambda'' \notin \text{Rad } K$ і $\lambda' \not\equiv \lambda'' \pmod{\text{Rad } K}$. Якщо зображення $\Gamma_{\lambda'}$ та $\Gamma_{\lambda''}$ еквівалентні, то матриці $\bar{M}_1 + \lambda' \bar{M}_2$ та $\bar{M}_1 + \lambda'' \bar{M}_2$ подібні над полем $K/\text{Rad } K$, тому їх детермінанти $(-1)^{n-1} \lambda' + \text{Rad } K$ та $(-1)^{n-1} \lambda'' + \text{Rad } K$ рівні, що неможливо. Отже, зображення $\Gamma_{\lambda'}$ та $\Gamma_{\lambda''}$ не еквівалентні над кільцем K . Теорема доведена. $\square$

Лема 2.3. *Нехай $H = \langle a \rangle$ — циклічна група порядку p і K — комутативне локальне кільце, яке містить елементи u і v такі, що $u \neq vv_1, v \neq uv_1$ ($u_1 \in K, v_1 \in K$) і $uv = up = vp = u^2 = 0$, з нескінченним полем лишків. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи H над кільцем K довільного наперед заданого степеня $n > 1$.*

Доведення. Нехай λ — оборотний елемент кільця K , M_1, M_2 — матриці вигляду (2.1).

Розглянемо відображення

$$\Gamma_{\lambda} a \longrightarrow E_n + uM_1 + v\lambda M_2,$$

де E_n — одинична $n \times n$ -матриця. Оскільки E_n та $uM_1 + v\lambda M_2$ комутують,

то

$$\begin{aligned}\Gamma(a)^p &= (E_n + uM_1 + v\lambda M_2)^p = \\ &= E_n + \sum_{i=1}^{p-1} C_p^i (uM_1 + v\lambda M_2)^i + (uM_1 + v\lambda M_2)^p.\end{aligned}$$

Враховуючи, що $C_p^i = c_p^i p$ ($c_p^i \in \mathbb{N}$; $i = 1, \dots, p-1$), $pu = pv = 0$, маємо

$$\Gamma(a)^p = E_n + \sum_{i=1}^{p-1} c_p^i p (uM_1 + v\lambda M_2)^i + (uM_1 + v\lambda M_2)^p = E_n + (uM_1 + v\lambda M_2)^p.$$

Враховуючи, що $uv = u^2 = 0$, $p \geq 2$, $M_2^2 = 0$ і $(uM_1 + v\lambda M_2)^2 = u^2 M_1 + uv\lambda M_1 M_2 + uv\lambda M_2 M_1 + v^2 \lambda^2 M_2^2 = 0$, то

$$\Gamma(a)^p = E_n + (uM_1 + v\lambda M_2)^p = E_n + (uM_1 + v\lambda M_2)^2 (uM_1 + v\lambda M_2)^{p-2} = E_n.$$

Отже, Γ є зображенням групи H над кільцем K .

Припустимо, що зображення Γ_λ звідне над кільцем K . Тоді знайдеться така матриця $C \in GL(n, K)$, що

$$uC^{-1}M_1C + v\lambda C^{-1}M_2C = u \begin{pmatrix} A_1 & D_1 \\ 0 & B_1 \end{pmatrix} + v\lambda \begin{pmatrix} A_2 & D_2 \\ 0 & B_2 \end{pmatrix}, \quad (2.3)$$

де A_i, B_i — $r \times r$ -матриці $(n-r) \times (n-r)$ -матриця над кільцем K відповідно ($i = 1, 2$; $1 \leq r < n$). Враховуючи оборотність елемента λ , одержимо $u \neq v\lambda \cdot v_1$, $v\lambda \neq u \cdot u_1$ ($u_1, v_1 \in K$) Звідси і з (2.3) випливає, що над полем $K/\text{Rad } K$

$$\overline{C}^{-1} \overline{M}_i \overline{C} = \begin{pmatrix} \overline{A}_i & \overline{D}_i \\ 0 & \overline{B}_i \end{pmatrix} \quad (i=1,2),$$

де $\overline{S} = \|\alpha_{ij} + \text{Rad } K\|$, $S = \|\alpha_{ij}\|$ — довільна матриця над кільцем K . А це суперечить [44, ст. 78, лема 1]. Значить, зображення Γ_λ незвідне над кільцем K .

Нехай $\lambda', \lambda'' \in K$; $\lambda', \lambda'' \notin \text{Rad } K$ і $\lambda' \not\equiv \lambda'' \pmod{\text{Rad } K}$. Якщо зображення $\Gamma_{\lambda'}$ та $\Gamma_{\lambda''}$ еквівалентні, то матриці

$$\overline{M_1} + \overline{\lambda' M_2} = \begin{pmatrix} 0 & 0 & \dots & 0 & \overline{\lambda'} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \quad \text{та} \quad \overline{M_1} + \overline{\lambda'' M_2} = \begin{pmatrix} 0 & 0 & \dots & 0 & \overline{\lambda''} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

подібні над полем $K/\text{Rad } K$, що неможливо, бо їх відповідні характеристичні многочлени $(-1)^n(x^n - \overline{\lambda'})$ та $(-1)^n(x^n - \overline{\lambda''})$ різні. Лема доведена. $\square$

Лема 2.4. *Нехай K — комутативне локальне кільце, яке не є полем, $u_1, u_2, \dots, u_l$ — мінімальна система твірних ідеалу $\text{Rad } K$ і λ, λ' — оборотні елементи кільця K , $\lambda \not\equiv \lambda' \pmod{\text{Rad } K}$. Матриця*

$$D(\lambda) = \begin{pmatrix} 0 & 0 & \dots & 0 & \lambda \\ u_1 & 0 & \dots & 0 & 0 \\ 0 & u_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & u_1 & 0 \end{pmatrix} \quad (2.4)$$

порядку $n > 1$ незвідна над кільцем K , а матриці $D(\lambda), D(\lambda')$ не є подібними.

Доведення. Припустимо, що існує така матриця $C \in GL(n, K)$, що

$$C^{-1}D(\lambda)C = \begin{pmatrix} D_1 & D_3 \\ 0 & D_2 \end{pmatrix}, \quad (2.5)$$

де D_1 і D_2 — $n \times n$ -матриця та $(n-r) \times (n-r)$ -матриця над кільцем K ($1 \leq r < n$).

Очевидно, ранг матриці

$$\overline{D(\lambda)} = \begin{pmatrix} 0 & \dots & 0 & \bar{\lambda} \\ 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 \end{pmatrix}$$

в полі $K/\text{Rad } K$ дорівнює 1. Тоді ранг матриці

$$\overline{C}^{-1} \overline{D(\lambda)} \overline{C} = \begin{pmatrix} \overline{D}_1 & \overline{D}_3 \\ 0 & \overline{D}_2 \end{pmatrix}$$

теж рівний 1. Звідси випливає, що хоча б одна із матриць $\overline{D}_1$ або $\overline{D}_2$ рівна нулю.

Зрозуміло, що перестановкою рядків і тою ж перестановкою стовпчиків до їх слідування в зворотному порядку матриця $D(\lambda)$ зводиться до

$$\begin{pmatrix} 0 & u_1 & 0 & \dots & 0 & 0 \\ 0 & 0 & u_1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & u_1 \\ \lambda & 0 & 0 & \dots & 0 & 0 \end{pmatrix} = D(\lambda)^T.$$

Тобто $D(\lambda)^T$ подібна до $D(\lambda)$. Але маємо також подібність

$$\begin{pmatrix} D_1 & D_3 \\ 0 & D_2 \end{pmatrix}^T = \begin{pmatrix} D_1^T & 0 \\ D_3^T & D_2^T \end{pmatrix} \sim \begin{pmatrix} D_2^T & D_3^T \\ 0 & D_1^T \end{pmatrix}.$$

Тобто, можна вважати, що $\overline{D}_1 = 0$, тобто $D_1 = u_1 S_1 + u_2 S_2 + \dots + u_l S_l$, де S_i — $r \times r$ -матриці над кільцем K ($i = 1, \dots, l$). Із (2.5) одержуємо:

$$D(\lambda)C = C \begin{pmatrix} D_1 & D_3 \\ 0 & D_2 \end{pmatrix}. \quad (2.6)$$

Позначимо: $C = \|c_{ij}\|$ ($c_{ij} \in K$), $C_i = (c_{i1}, \dots, c_{in})$ ($i = 1, \dots, n$). З (2.6) дістаємо, що $\lambda C_n = C_1 D_1$, $u_1 C_i = C_{i+1} D_1 = u_1 C_{i+1} S_1 + u_2 C_{i+1} S_2 + \dots + u_l C_{i+1} S_l$ ($i = 1, \dots, n-1$). Оскільки $u_1, u_2, \dots, u_l$ — мінімальна система твірних деякого ідеалу, то рівність

$$u_1 \alpha_1 + u_2 \alpha_2 + \dots + u_l \alpha_l = 0 \quad (\alpha_i \in K, \quad i = 1, \dots, l)$$

можлива хіба, що для деяких $\alpha_i \in \text{Rad } K$ ($i = 1, \dots, l$).

Отже, $C_n \equiv 0 \pmod{\text{Rad } K}$, $C_i \equiv C_{i+1} S_1 \pmod{\text{Rad } K}$ ($i = 1, \dots, n-1$), $C_i \equiv 0 \pmod{\text{Rad } K}$ ($i = 1, \dots, n$). Тому $\det C \equiv 0 \pmod{\text{Rad } K}$. Одержане протиріччя показує, що матриця $D(\lambda)$ незвідна над кільцем K .

Припустимо, що існує така матриця $C \in GL(n, K)$, що $C^{-1} D(\lambda) C = D(\lambda')$, тобто $D(\lambda) C = C D(\lambda')$. Позначимо: $C = \|c_{ij}\|$ ($c_{ij} \in K$). Тоді

$$\begin{pmatrix} \lambda c_{n1} & \lambda c_{n2} & \dots & \lambda c_{nn-1} & \lambda c_{nn} \\ u_1 c_{11} & u_1 c_{12} & \dots & u_1 c_{1n-1} & u_1 c_{1n} \\ u_1 c_{21} & u_1 c_{22} & \dots & u_1 c_{2n-1} & u_1 c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ u_1 c_{n-11} & u_1 c_{n-12} & \dots & u_1 c_{n-1n-1} & u_1 c_{n-1n} \end{pmatrix} = \begin{pmatrix} u_1 c_{12} & u_1 c_{13} & \dots & u_1 c_{1n} & \lambda' c_{11} \\ u_1 c_{22} & u_1 c_{23} & \dots & u_1 c_{2n} & \lambda' c_{21} \\ u_1 c_{32} & u_1 c_{33} & \dots & u_1 c_{3n} & \lambda' c_{31} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ u_1 c_{n2} & u_1 c_{n3} & \dots & u_1 c_{nn} & \lambda' c_{n1} \end{pmatrix}.$$

Звідси $\lambda c_{ni} = u_1 c_{i+1}$ ($i = 1, \dots, n-1$), $\lambda c_{nn} = \lambda' c_{11}$, $u_1 c_{ii} = u_1 c_{i+1}$ ($i = 1, \dots, n-1$). Тому $c_{ni} \equiv 0 \pmod{\text{Rad } K}$ ($i = 1, \dots, n-1$), $c_{ii} \equiv c_{i+1} \pmod{\text{Rad } K}$ ($i = 1, \dots, n-1$). Звідси $c_{11} \equiv c_{nn} \pmod{\text{Rad } K}$, $(\lambda -$

$\lambda')c_{nn} \equiv \lambda c_{nn} - \lambda' c_{nn} \equiv \lambda c_{11} - \lambda' c_{nn} \equiv 0 \pmod{\text{Rad } K}$. Оскільки $\lambda \not\equiv \lambda' \pmod{\text{Rad } K}$, то $c_{nn} \equiv 0 \pmod{\text{Rad } K}$. Тому $\det C \equiv 0 \pmod{\text{Rad } K}$. Одержане протиріччя показує, що матриці $D(\lambda)$, $D(\lambda')$ не є подібними. Лема доведена. $\square$

Лема 2.5. *Нехай $H = \langle a \rangle$ — циклічна група порядку p і K — комутативне нетерове локальне кільце з нескінченним полем лишків, яке містить такий елемент t , що $t^2 \text{Rad } K = 0$, $tp = 0$ і $t \text{Rad } K \neq 0$. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи H над кільцем K довільного наперед заданого степеня $n > 1$.*

Доведення. Позначимо через $\text{Ann } t$ ідеал $\{w \in K \mid tw = 0\}$ кільця K . Очевидно, фактор-кільце $K/\text{Ann } t$ є комутативне нетерове локальне кільце, яке не є полем. Нехай $u_1 + \text{Ann } t, u_2 + \text{Ann } t, \dots, u_m + \text{Ann } t$ — мінімальна система твірних ідеалу $\text{Rad}(K/\text{Ann } t)$, $u_i \in K$ ($i = 1, \dots, m$; $m > 0$). Крім того, поле лишків кільце $K/\text{Ann } t$ теж нескінченне. Для $n \times n$ -матриці $D(\lambda)$ вигляду (2.4) над кільцем K , де λ — оборотний елемент кільця K , розглянемо відображення

$$\Gamma_\lambda : a \longrightarrow E_n + tD(\lambda),$$

де E_n — одинична матриця порядку $n > 1$. Оскільки E_n та $tD(\lambda)$ комутують, то $\Gamma_\lambda(a)^p = (E_n + tD(\lambda))^p = E_n^p + \sum_{i=1}^{p-1} C_p^i t^i D(\lambda)^i + t^p D(\lambda)^p$. Враховуючи, що $C_p^i = c_p^i p$ ($c_p^i \in \mathbb{N}$; $i = 1, \dots, p-1$), $tp = 0$, то $\Gamma_\lambda(a)^p = E_n^p + \sum_{i=1}^{p-1} c_p^i p t^i D(\lambda)^i + t^p D(\lambda)^p = E_n + t^p D(\lambda)^p$. Враховуючи, що $t^2 \text{Rad } K = 0$, $p \geq 2$, $D(\lambda)^2 \equiv 0 \pmod{\text{Rad } K}$, то $\Gamma_\lambda(a)^p = E_n + t^{p-2} t^2 D(\lambda)^2 D(\lambda)^{p-2} = E_n$ і Γ_λ є зображенням групи H над кільцем K . Зображення Γ_λ є звідним тоді і тільки тоді, коли є звідною матриця $D(\lambda)$ після редукції за модулем ідеала $\text{Ann } t$, а два зображення Γ_λ ,

$\Gamma_{\lambda'}$, де λ' — оборотний елемент кільця K , еквівалентні тільки тоді, коли подібними є матриці одержані з матриць $D(\lambda)$, $D(\lambda')$ за допомогою редукції за модулем ідеалу $\text{Ann } t$. Звідси і з леми 2.4 випливає існування нескінченної кількості нееквівалентних незвідних матричних зображень групи H над кільцем K . Лема доведена. $\square$

Лема 2.6. *Нехай H — циклічна p -група порядку p , K — комутативне нетерове локальне кільце з нескінченним полем лишків і K^* — мультиплікативна група кільця K . Якщо кільце K містить нільпотентний елемент t другого степеня, $pt = 0$ і $\text{Rad } K \cap \text{Ann } p \neq W = \{0, t\theta \mid \theta \in K^*\}$, то існує нескінченна кількість нееквівалентних незвідних матричних зображень групи H над кільцем K довільного наперед заданого степеня $n > 1$.*

Доведення. Із леми 2.5 випливає, що якщо кільце K містить такий нільпотентний елемент u другого степеня, що $pu = 0$, то $u^2 \text{Rad } K = 0$ і можна вважати, що $u \text{Rad } K = 0$. Далі, враховуючи лему 2.3, можна обмежитись розгляданням випадку, коли в кільці K немає жодного з ануляторів p , який не ділить і не ділиться на t .

Оскільки $\text{Rad } K \cap \text{Ann } p \neq W$, то існує такий необоротний елемент $v \in K$, що $vp = 0$ і $v \notin W$. Легко перевірити, що v не ділиться на t . Таким чином, залишилось розглянути випадок, коли t ділиться на v . Очевидно, $v^2 \neq 0$ і $v^2 p = 0$. Нехай $v^2 \notin W$. Тоді v^2 ділить t . Отже, $t = v^2 v_1$ ($v_1 \in \text{Rad } K$), $(vv_1)^2 = v^2 v_1^2 = tv_1 = 0$, $(vv_1)p = 0$ і $vv_1 \neq 0$. Звідси випливає, що $(vv_1) \text{Rad } K = 0$. Значить, $t = v^2 v_1 = (vv_1)v = 0$, що неможливо. Одержане протиріччя показує, що $v^2 = \theta t$ ($\theta \in K^*$). Очевидно, $v \text{Rad } K \neq 0$, $v^2(\text{Rad } K) = 0$. Тому, за лемою 2.5, існує нескінченна кількість нееквівалентних незвідних матричних зображень групи H над кільцем K степеня n . $\square$

Лема 2.7. Нехай $H = \langle a \rangle$ — циклічна p -група порядку p^2 , K — комутативне локальне кільце характеристики p^s ($s \geq 1$) з нескінченним полем лишків і $\text{Rad } K = tK$, де t — нільпотентний елемент кільця K степеня r ($r > 1$). Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи H над кільцем K довільного наперед заданого степеня $n > 1$.

Доведення. З леми 2.5 випливає, що зображення $\Gamma_\lambda: a \rightarrow E + t^{r-2}D(\lambda)$ (E — одинична $n \times n$ -матриця, $D(\lambda)$ — $n \times n$ -квадратна матриця над кільцем K вигляду (2.4), де λ — оборотний елемент кільця K , $u_1 = t$) є незвідним зображенням групи H над кільцем K а два зображення Γ_λ , $\Gamma_{\lambda'}$, де λ' — оборотний елемент кільця K , еквівалентні тільки тоді, коли $\lambda \equiv \lambda' \pmod{tK}$. Лема доведена. $\square$

Лема 2.8. Нехай $H = \langle a \rangle$ — циклічна p -група порядку p , K — комутативне локальне кільце характеристики p з нескінченним полем лишків і $\text{Rad } K = tK$, де t — нільпотентний елемент кільця K степеня r ($r > 1$). Якщо $p > 3$, $n > 1$ або $p > 2$, $n > 2$, то існує нескінченна кількість нееквівалентних незвідних матричних зображень групи H над кільцем K степеня n .

Доведення. Нехай E — одинична $n \times n$ -матриця, D_λ — $n \times n$ -матриця над кільцем K вигляду (2.4), де λ — оборотний елемент кільця K , $u_1 = t$. Очевидно, $D_\lambda^p \equiv 0 \pmod{t^2K}$. Тоді $\Gamma_\lambda: a \rightarrow E + t^{r-2}D_\lambda$ є зображенням групи H над кільцем K . З леми 2.5 випливає, що зображення Γ_λ є незвідним а два зображення Γ_λ , $\Gamma_{\lambda'}$, де λ' — оборотний елемент кільця K , еквівалентні тільки тоді, коли $\lambda \equiv \lambda' \pmod{tK}$. Лема доведена. $\square$

Твердження 2.9. Нехай існує незвідний поліном степеня n над полем F . Існує тільки скінченна кількість незвідних нормованих поліно-

мів над полем F степеня n тоді і тільки тоді, коли поле F — скінченне.

Доведення. Достатність очевидна. Нехай F — нескінченне поле. M — множина незвідних поліномів від невідомої x над полем F старший коефіцієнт, яких рівний 1. Очевидно, $M \neq \emptyset$. Нехай $f(x) \in M$. Розглянемо відображення $\Phi : F \rightarrow M$, задане за правилом $\Phi(a) = f(x + a)$. Якщо $b \in F$, $\Phi(b) = \Phi(a)$, то $f(x + b) = f(x + a)$, $f(b) = f(a)$. Отже, b — корінь полінома $f(x) - f(a)$, який має не більше ніж n коренів. Отже, повний прообраз будь-якого многочлена із $\Phi(F)$ скінченний. Оскільки F — нескінченне поле, то множина $\Phi(F)$, а отже, і M нескінченна. Твердження доведене. $\square$

Теорема 2.10. *Нехай G — скінченна p -група порядку $|G| > 1$ і K — комутативне нетерове локальне кільце характеристики p^s ($s > 0$), яке не є напівпервісним, з нескінченним полем лишків. Множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня $n > 1$ скінченна тоді і тільки тоді, коли виконується одна з таких умов:*

- 1) $|G| = 2$, $s = 1$, $(\text{Rad } K)^2 = 0$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;
- 2) $|G| = 3$, $s = 1$, $(\text{Rad } K)^2 = 0$, $n = 2$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня 2 звідні;
- 3) $|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \notin (p - 1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;
- 4) $|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \in (p - 1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n та $\frac{n}{p-1}$ звідні.

Доведення. Із теореми 2.2 випливає, що можна вважати, що G — циклічна p -група. Розглянемо ряд випадків.

Нехай характеристика кільця K дорівнює p . Очевидно, кільце K містить ненульовий нільпотентний елемент t другого степеня. Якщо $\text{Rad } K \neq tK$, то $\text{Rad } K \cap \text{Ann } p = \text{Rad } K \neq \{0, t\theta \mid \theta \in K^*\}$. Звідси і із леми 2.6 одержуємо, що існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K степеня n .

Залишилось розглянути випадок, коли $\text{Rad } K = tK$. Якщо $|G| > p$, то з леми 2.7 дістанемо, що існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K степеня n . Нехай далі $|G| = p$. Якщо $p > 3$ або $p > 2, n > 2$, то з леми 2.8 випливає, що існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K степеня n .

Нехай тепер $p = 2$, група $G = \langle a \rangle$ є циклічна порядку $|G| = p = 2$, кільцем K характеристики $p = 2$, $\text{Rad } K = tK \neq 0, t^2 = 0$ і $\Gamma : a \rightarrow E_n + M$ — незвідне матричне зображення групи G , де E_n — одинична $n \times n$ -матриця, M — деяка $n \times n$ -матриця над кільцем K . Тоді, враховуючи, що E_n та M комутують, $E_n = (E_n + M)^2 = E_n + 2M + M^2$. Оскільки 2 є характеристика кільця K , то $M^2 = 0$. Якщо матриця M містить стовпчик S з оборотним елементом, то $MS = 0$. Очевидно, існує оборотна матриця C порядку n над кільцем K з першим стовпчиком S . Крім того, $C^{-1}MS = C^{-1}0 = 0$ є першим стовпчиком матриці $C^{-1}MC$. Тобто матриця M , а отже, і зображення Γ зводні, що неможливо. Отже, всі елементи матриці M містяться в $\text{Rad } K = tK$ і $M = tD$, де D — деяка $n \times n$ -матриця над кільцем K . Оскільки зображення Γ незвідне, то матриця $M = tD$ незвідна. А отже, матриця $\overline{D}$ незвідна над полем $K/tK = K/\text{Ann } K$, тобто характеристичний многочлен матриці

$\overline{D}$ незвідний над полем K/tK . Два незвідні зображення вигляду

$$\Gamma : a \rightarrow E_n + tD, \quad \Gamma' : a \rightarrow E_n + tD',$$

де D' — деяка $n \times n$ -матриця над кільцем K , еквівалентні, тоді і тільки тоді, коли характеристичні многочлени степеня n матриць $\overline{D}$ та $\overline{D}'$ над полем K/tK однакові. Отже, множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня $n > 1$ скінченна тоді і тільки тоді, коли скінченна множина незвідних многочленів степеня n над полем K/tK , тобто, коли виконується 1).

Нехай тепер $p = 3$, $n = 2$, група $G = \langle a \rangle$ є циклічна порядку $|G| = p = 3$, K — кільце характеристики $p = 3$, $\text{Rad } K = tK \neq 0$, $t^2 = 0$ і $\Gamma : a \rightarrow E_2 + M$ — незвідне матричне зображення групи G , де E_2 — одинична 2×2 -матриця, M — деяка 2×2 -матриця над кільцем K . Тоді, враховуючи, що E_2 та M комутують, $E_2 = (E_2 + M)^3 = E_n + 3M + 3M^2 + M^3$. Оскільки 3 є характеристика кільця K , то $M^3 = 0$. Таким чином матриця $\overline{M}$ над полем K/tK також нільпотентна і, отже, подібна до

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ або } \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

У першому випадку, не зменшуючи загальності, можна вважати, що

$$M = \begin{pmatrix} tm_{11} & 1 + tm_{12} \\ tm_{21} & tm_{22} \end{pmatrix}.$$

Але тоді

$$\begin{aligned} 0 = M^3 = M^2 M &= \begin{pmatrix} tm_{21} & tm_{11} + tm_{22} \\ 0 & tm_{21} \end{pmatrix} \cdot \begin{pmatrix} tm_{11} & 1 + tm_{12} \\ tm_{21} & tm_{22} \end{pmatrix} = \\ &= \begin{pmatrix} 0 & tm_{21} \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Отже, $tm_{21} = 0$, матриця

$$M = \begin{pmatrix} tm_{11} & 1 + tm_{12} \\ 0 & tm_{22} \end{pmatrix},$$

а отже, і зображення Γ звідні, що неможливо.

У випадку $\overline{M} = 0$, аналогічно до випадку $p = 2$, одержимо, що множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня $n = 2$ скінченна тоді і тільки тоді, коли скінченна множина незвідних многочленів степеня 2 над полем K/tK , тобто, коли виконується 2).

Нехай характеристика кільця K дорівнює p^s ($s > 1$). Очевидно, p^{s-1} — нільпотентний елемент другого степеня, що анулює p . Якщо $\text{Rad } K \neq pK$, то, як показано в [44, ст. 82, лема 8], $\text{Ann } p \neq \{0, p^{s-1}\theta \mid \theta \in K^*\}$ і існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K степеня $n > 1$.

Нехай далі $\text{Rad } K = pK$. Якщо $|G| > p$, то з леми 2.7 випливає, що існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K степеня n . У випадку, коли $|G| = p$, із опису [22, 155] з точністю до еквівалентності нерозкладних матричних зображень групи G над кільцем K дістаємо, що при $p > 2$ з точністю до еквівалентності незвідні матричні зображення вичерпуються такими серіями

$$T_1 : a \longrightarrow E_m + p^{s-1}F_m,$$

$$T_2 : a \longrightarrow \Delta \otimes E_m + \Theta(p^{s-1}) \otimes F_m$$

де Δ — така матриця порядку $(p-1)$:

$$\Delta = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ -C_p^1 & -C_p^2 & -C_p^3 & \dots & -C_p^{p-2} & 1 - C_p^{p-1} \end{pmatrix},$$

$\Theta(\alpha)$ — $(p-1) \times (p-1)$ -матриця, у якій в правому нижньому кутку розташований елемент α , а всі інші рівні нулю; F_m — нормальна форма Фробеніуса $m \times m$ -матриці над полем K/pK з незвідним характеристичним многочленом порядку m . Також при $p = 2$ з точністю до еквівалентності нерозкладні матричні зображення групи G над кільцем K вичерпуються такими серіями

$$T_1 : a \longrightarrow E_m + 2^{s-1}F_m,$$

$$T_2 : a \longrightarrow -E_m + 2^{s-1}F_m.$$

При довільному p зображення T_1 є незвідним зображенням порядку m , число яких рівне числу незвідних многочленів над полем K/pK порядку m а зображення T_2 є незвідним зображенням порядку $m(p-1)$, число яких таке ж.

Якщо $n \notin (p-1)\mathbb{Z}$, то незвідних зображень T_2 групи G над кільцем K порядку n не існує. Отже, множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня n (зображень T_1) скінченна тоді і тільки тоді, коли скінченна множина незвідних многочленів степеня n над полем K/pK , тобто, коли виконується 3).

Якщо $n \in (p-1)\mathbb{Z}$, то число нееквівалентних незвідних матричних зображень T_1 групи G над кільцем K степеня n рівне числу незвідним

многочленів над полем K/pK порядку n а число нееквівалентних незвідних матричних зображень T_2 групи G над кільцем K степеня n рівне числу незвідним многочленів над полем K/pK порядку $\frac{n}{p-1}$. Отже, множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня n (зображень T_1 та T_2) скінченна тоді і тільки тоді, коли скінченна множина незвідних многочленів степеня n та $\frac{n}{p-1}$ над полем K/pK , тобто, коли виконується 4). Теорема доведена. $\square$

Зауважимо, що множина нееквівалентних незвідних зображень p -групи над комутативним нетеровим локальним кільцем характеристики p^s ($s > 0$, p), яке не є напівпервісним, з нескінченним полем лишків, степеня n або нескінченна, або порожня.

Теорема 2.11. *Нехай G — скінченна p -група порядку $|G| > 1$ і K — комутативне артінове локальне кільце характеристики p^s ($s > 0$, p), яке не є полем. Множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня $n > 1$ скінченна тоді і тільки тоді, коли виконується одна з таких умов:*

- 1) *поле $K/\text{Rad } K$ скінченне;*
- 2) *$|G| = 2$, $s = 1$, $(\text{Rad } K)^2 = 0$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;*
- 3) *$|G| = 3$, $s = 1$, $(\text{Rad } K)^2 = 0$, $n = 2$, K — кільце головних ідеалів, всі поліноми над полем $K/\text{Rad } K$ степеня 2 звідні;*
- 4) *$|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \notin (p-1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n звідні;*
- 5) *$|G| = p$, $s > 1$, $\text{Rad } K = pK$, $n \in (p-1)\mathbb{Z}$, всі поліноми над полем $K/\text{Rad } K$ степеня n та $\frac{n}{p-1}$ звідні.*

Доведення. Якщо поле лишків кільця K скінченне, то за твердженням 2.1 саме кільце K скінченне, а отже, і множина нееквівалентних незвідних матричних зображень групи G над кільцем K степеня n . Якщо поле лишків кільця K нескінченне, то твердження теореми випливає з теореми 2.10. Теорема доведена. $\square$

Зауважимо, що у випадках 2)–5) множина нееквівалентних незвідних зображень групи G над кільцем K степеня n порожня.

2.3. Зображення скінченних p -груп над напівпервісними кільцями характеристики p

В підрозділі вивчається, коли є скінченною множина всіх нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи G над комутативним нетеровим локальним напівпервісним нецілісним кільцем характеристики p , поле класів лишків якого нескінченне.

Теорема 2.12. *Нехай G — скінченна p -група порядку $|G| > 1$ і K — комутативне нетерове локальне напівпервісне кільце характеристики p , яке не є цілісним, з нескінченним полем лишків. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K довільного наперед заданого парного степеня n .*

Доведення. Очевидно, досить розглянути випадок, коли $G = \langle a \rangle$ — циклічна група порядку p . Нехай u і v — два елементи кільця K такі, що $uv = 0$, $u \neq 0$, $v \neq 0$. З [80, ст. 104, доведення теореми 1] випливає, що відображення Γ_λ вигляду $a \rightarrow \Gamma_\lambda(a) = E_n + S(\lambda)$, де E_n — одинична матриця порядку n , $S(\lambda) = uS_1 + vS_2(\lambda)$ — $n \times n$ -матриця над кільцем

K ,

$$S_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \quad S_2(\lambda) = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & \lambda \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & q_1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & q_1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & q_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix},$$

є незвідним зображенням групи G над кільцем K для будь-якого $\lambda \in K^*$. Тут $v^2 q_1, v^2 q_2, \dots, v^2 q_l$ — мінімальна система твірних ідеалу $v^2 \text{Rad } K$ ($q_i \in K; i = 1, \dots, l; l > 0$).

Припустимо, що зображення Γ_λ еквівалентне зображенню $\Gamma_{\lambda'}$, де $\lambda, \lambda' \in K^*, \lambda \not\equiv \lambda' \pmod{\text{Rad } K}$. Тоді для деякої матриці $C \in GL(n, K)$

$$uC^{-1}S_1C + vC^{-1}S_2(\lambda)C = C^{-1}\Gamma_\lambda(a)C = \Gamma_{\lambda'}(a) = uS_1 + vS_2(\lambda'). \quad (2.7)$$

З (2.7) випливає, що $u^2C^{-1}S_1C = u^2S_1, v^2C^{-1}S_2(\lambda)C = v^2S_2(\lambda')$. Звідси одержимо, що

$$u^2S_1C = u^2CS_1, \quad (2.8)$$

$$v^2S_2(\lambda)C = v^2CS_2(\lambda'). \quad (2.9)$$

Нехай $C = \|c_{ij}\|, (c_{ij} \in K; i, j = 1, \dots, n)$. З (2.8) одержимо $u^2c_{2i-1, 2i-1} = u^2c_{2i, 2i}$ ($i = 1, \dots, \frac{n}{2}$). Оскільки $\text{rad } K = 0, u \neq 0$, а отже, $u^2 \neq 0$, то

$$c_{2i-1, 2i-1} \equiv c_{2i, 2i} \pmod{\text{Rad } K} \quad (i = 1, \dots, \frac{n}{2}). \quad (2.10)$$

З (2.9) одержимо $v^2\lambda c_{nn} = v^2\lambda' c_{11}, v^2c_{i1} \in v^2q_1K$ ($i = 2, \dots, n$), $v^2q_1c_{2i, 2i} = v^2q_1c_{2i+1, 2i+1}$ ($i = 1, \dots, \frac{n}{2} - 1$).

Оскільки $\text{rad } K = 0$, $v, v^2 \neq 0$, то $\lambda c_{nn} \equiv \lambda' c_{11} \pmod{\text{Rad } K}$, Оскільки $v^2 \neq 0$, $q_1 \in \text{Rad } K$, то $c_{i1} \in \text{Rad } K$ ($i = 2, \dots, n$). Враховуючи оборотність $\det C$ одержимо $c_{11} \in K^*$. Оскільки $v^2 q_1, v^2 q_2, \dots, v^2 q_l$ — мінімальна система твірних ідеалу $v^2 \text{Rad } K \neq 0$, то $c_{2i,2i} \equiv c_{2i+1,2i+1} \pmod{\text{Rad } K}$ ($i = 1, \dots, \frac{n}{2} - 1$), що враховуючи (2.10), означає $c_{11} \equiv c_{ii} \pmod{\text{rad } K}$ ($i = 2, \dots, n$) і, зокрема, $\lambda c_{11} \equiv \lambda' c_{11} \pmod{\text{Rad } K}$. Тоді $\lambda \equiv \lambda' \pmod{\text{Rad } K}$, що неможливо. Теорема доведена. $\square$

Теорема 2.13. *Нехай G — скінченна p -група порядку $|G| > 2$ і K — комутативне нетерове локальне напівпервісне кільце характеристики p , яке не є цілісним, з нескінченним полем лишків. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K довільного наперед заданого степеня $n > 1$.*

Доведення. Враховуючи теорему 2.12, досить розглянути випадок, коли $G = \langle a \rangle$ — циклічна група порядку $|G| > 2$, n — непарне число. Нехай u і v — два елементи кільця K такі, що $uv = 0$, $u \neq 0$, $v \neq 0$. Для будь-якого $\lambda \in K$, $q_1 \in K$ розглянемо відображення Γ_λ вигляду:

$$a \rightarrow E_n + S(\lambda),$$

де

$$S(\lambda) = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & v\lambda \\ u & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & vq_1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & u & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & vq_1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & u & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & vq_1 & 0 \end{pmatrix},$$

E_n — одинична матриця порядку n . Оскільки $uv = 0$

$$S(\lambda)^2 = \begin{pmatrix} 0 & \dots & 0 & v^2\lambda q_1 & 0 \\ 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 \end{pmatrix},$$

$S(\lambda)^3 = S(\lambda)^2 S(\lambda) = 0$. Враховуючи, що матриці E_n та M комутують, p — характеристика кільця K , маємо $(E_n + S(\lambda))^p = E_n + S(\lambda)^p$. Враховуючи, що G — p -група порядку $|G| > 2$, $M^3 = 0$, маємо $(E_n + S(\lambda))^{|G|} = E_n + S(\lambda)^{|G|} = E_n + S(\lambda)^3 S(\lambda)^{|G|-3} = E_n$. Отже, Γ_λ є зображенням групи G над кільцем K .

Нехай тепер $q_1 \in K$ такий, що $v^2 q_1, v^2 q_2, \dots, v^2 q_l$ — мінімальна система твірних ідеалу $v^2 \text{Rad } K$ ($q_i \in K$; $i = 2, \dots, n$; $l > 0$). Очевидно, $S(\lambda) = uS_1 + vS_2(\lambda)$, де

$$S_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}, \quad S_2(\lambda) = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & \lambda \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & q_1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & q_1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & q_1 & 0 \end{pmatrix}$$

— $n \times n$ -матриці над кільцем K . Припустимо, що зображення Γ звідне над кільцем K . Тоді для деякої матриці $C \in GL(2n, K)$

$$C^{-1}S(\lambda)C = uC^{-1}S_1C + vC^{-1}S_2C = \begin{pmatrix} A & D \\ 0 & B \end{pmatrix}, \quad (2.11)$$

де A і B — $r \times r$ -матриця та $(n - r) \times (n - r)$ -матриця над кільцем K відповідно ($1 \leq r < n$). Очевидно, $v \neq uu_1$ ($u_1 \in K$), бо інакше $v^2 = 0$. З (2.11) випливає, що

$$v^2 C^{-1} S_2 C = v \begin{pmatrix} A & D \\ 0 & B \end{pmatrix}$$

і над полем $K/\text{Rad } K$

$$\overline{C}^{-1} \overline{S_2(\lambda)} \overline{C} = \begin{pmatrix} A' & D' \\ 0 & B' \end{pmatrix}, \quad (2.12)$$

де A' — $r \times r$ -матриця над полем $K/\text{Rad } K$. Очевидно, 1 — ранг матриці

$$\overline{S_2(\lambda)} = \begin{pmatrix} 0 & \dots & 0 & \bar{\lambda} \\ 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 \end{pmatrix}$$

в полі $K/\text{Rad } K$. Тоді ранг матриці

$$\overline{C}^{-1} \overline{S_2(\lambda)} \overline{C} = \begin{pmatrix} A' & D' \\ 0 & B' \end{pmatrix}$$

теж рівний 1. Звідси випливає, що хоча б одна з матриць A' або B' нульова.

Розглянемо спочатку випадок, коли $A' = 0$. Тоді $A = uA_1 + vA_2$, де A_1, A_2 — $r \times r$ -матриці, $A_2 \equiv 0 \pmod{\text{Rad } K}$. Позначимо: $C = \|c_{ij}\|$ ($c_{ij} \in K$), $C_i = (c_{i1}, \dots, c_{ir})$ ($i = 1, \dots, n$). З (2.12)

$$\overline{S_2(\lambda)} \overline{C} = \overline{C} \begin{pmatrix} 0 & D' \\ 0 & B' \end{pmatrix}.$$

Звідси

$$C_n \equiv 0 \pmod{\text{Rad } K}. \quad (2.13)$$

Домноживши (2.11) зліва на uC , vC , відповідно одержимо

$$u^2 S_1 C = C \begin{pmatrix} u^2 A_1 & uD \\ 0 & uB \end{pmatrix}, \quad (2.14)$$

$$v^2 S_2(\lambda) C = C \begin{pmatrix} v^2 A_2 & vD \\ 0 & vB \end{pmatrix}. \quad (2.15)$$

З (2.14) маємо $u^2 C_{2i-1} = u^2 C_{2i} A_1$ ($i = 1, \dots, \frac{n-1}{2}$). Оскільки $u, u^2 \neq 0$, то

$$C_{2i-1} \equiv C_{2i} A_1 \pmod{\text{Rad } K} \quad \left(i = 1, \dots, \frac{n-1}{2}\right). \quad (2.16)$$

Так-як $v^2 q_1, v^2 q_2, \dots, v^2 q_l$ — мінімальна система твірних ідеалу $v^2 \text{Rad } K$, $A_2 \equiv 0 \pmod{\text{Rad } K}$, то $v^2 A_2 = v^2 q_1 A_{21} + v^2 q_2 A_{22} + \dots + v^2 q_l A_{2l}$, де A_{2i} — $r \times r$ -матриця ($i = 1, \dots, l$). З (2.15) маємо $v^2 q_1 C_{2i} = v^2 q_1 C_{2i+1} A_{21} + v^2 q_2 C_{2i+1} A_{22} + \dots + v^2 q_l C_{2i+1} A_{2l}$ ($i = 1, \dots, \frac{n-1}{2}$). Отже, $C_{2i} \equiv C_{2i+1} A_{21} \pmod{\text{Rad } K}$ ($i = 1, \dots, \frac{n-1}{2}$). Звідси і з (2.13), (2.16) випливає, що $C_i \equiv 0 \pmod{\text{Rad } K}$ ($i = 1, \dots, n$). Значить, $\det C \equiv 0 \pmod{\text{Rad } K}$, що неможливо.

Розглянемо тепер випадок, коли $B' = 0$. Тоді $B = uB_1 + vB_2$, де B_1, B_2 — $(n-r) \times (n-r)$ -матриці порядку $n-r$, $B_2 \equiv 0 \pmod{\text{Rad } K}$. Позначимо тепер: $C^{-1} = \|c_{ij}\|$ ($c_{ij} \in K$), $C_j = (c_{r+1,j}, \dots, c_{nj})$ ($j = 1, \dots, n$). З (2.12) маємо

$$\overline{C^{-1} S_2(\lambda)} = \begin{pmatrix} A' & D' \\ 0 & 0 \end{pmatrix} \overline{C^{-1}}.$$

Звідси

$$C_1 \equiv 0 \pmod{\text{Rad } K}. \quad (2.17)$$

Домноживши (2.11) зправа на uC^{-1} , vC^{-1} , відповідно одержимо

$$u^2 C^{-1} S_1 = \begin{pmatrix} uA & uD \\ 0 & u^2 B_1 \end{pmatrix} C^{-1}, \quad (2.18)$$

$$v^2 C^{-1} S_2(\lambda) = \begin{pmatrix} vA & vD \\ 0 & v^2 B_2 \end{pmatrix} C^{-1}. \quad (2.19)$$

З (2.18) маємо $u^2 C_{2j} = u^2 B_1 C_{2j-1}$ ($j = 1, \dots, \frac{n-1}{2}$). Оскільки $u, u^2 \neq 0$, то

$$C_{2j} \equiv B_1 C_{2j-1} \pmod{\text{Rad } K} \quad \left(j = 1, \dots, \frac{n-1}{2}\right). \quad (2.20)$$

Так-як $v^2 q_1, v^2 q_2, \dots, v^2 q_l$ — мінімальна система твірних ідеалу $v^2 \text{Rad } K$, $B_2 \equiv 0 \pmod{\text{Rad } K}$, то $v^2 B_2 = v^2 q_1 B_{21} + v^2 q_2 B_{22} + \dots + v^2 q_l B_{2l}$, де B_{2i} — $(n-r) \times (n-r)$ -матриця ($i = 1, \dots, l$). З (2.19) маємо $v^2 q_1 C_{2j+1} = v^2 q_1 B_{21} C_{2j} + v^2 q_2 B_{22} C_{2j} + \dots + v^2 q_l B_{2l} C_{2j}$ ($j = 1, \dots, \frac{n-1}{2}$). Отже, $C_{2j+1} \equiv B_{21} C_{2j} \pmod{\text{Rad } K}$ ($j = 1, \dots, \frac{n-1}{2}$). Звідси і з (2.17), (2.20) випливає, що $C_j \equiv 0 \pmod{\text{Rad } K}$ ($j = 1, \dots, n$). Значить, $\det C \equiv 0 \pmod{\text{Rad } K}$, що неможливо. Отже, зображення Γ незвідне.

Аналогічно, як і при доведенні теореми 2.12, можна показати, що для $\lambda, \lambda' \in K^*$, $\lambda \not\equiv \lambda' \pmod{\text{Rad } K}$ зображення Γ_λ і $\Gamma_{\lambda'}$ не є еквівалентними. Теорема доведена. $\square$

Твердження 2.14. *Нехай $G = \langle a \rangle$ — скінченна циклічна група порядку 2 і K — комутативне локальне напівпервісне кільце характеристики 2, $\text{Rad } K = uK + vK$, $u, v \in K$, $u, v \neq 0$, $uv = 0$. Всі матричні зображення групи G над кільцем K довільного непарного степеня $n > 1$ звідні.*

Доведення. Нехай Γ — матричне зображення групи G над кільцем K степеня n , $\Gamma(a) = E_n + M$, де E_n — одинична $n \times n$ -матриця над кільцем K , M — деяка $n \times n$ -матриця над кільцем K . Очевидно, $(E_n + M)^2 = \Gamma(a)^2 = E_n$. Оскільки матриці E_n та M комутують, 2 — характеристика кільця K , то $E_n = E_n + 2M + M^2 = E_n + M^2$ і $M^2 = 0$. Якщо M містить хоча б один оборотний елемент, то деякий стовпчик X матриці M містить оборотний елемент. Тому X є першим стовпчиком деякої

оборотної матриці C порядку n над кільцем K . Отже, перший стовпчик матриці MC , як і $C^{-1}MC$, рівний нулю. Тоді зображення Γ звідне.

Тоді $M \equiv 0 \pmod{\text{Rad } K}$ і, враховуючи, що $\text{Rad } K = uK + vK$, одержимо $M = uA + vB$, де A, B — деякі $n \times n$ -матриці над кільцем K . Тоді $u^3 A^2 = u(u^2 A^2 + v^2 B^2) = u(uA + vB)^2 = uM^2 = 0$. Якщо $u^3 \alpha = 0$ для деякого $\alpha \in K$, то $(u\alpha)^3 = u^3 \alpha^3 = 0$. Враховуючи, що $\text{rad } K = 0$, маємо $u\alpha = 0$. Отже, $uA^2 = 0$. Так само $vB^2 = 0$. Позначимо через $\widetilde{T} = \|t_{ij} + \text{Ann } u\|$ матрицю над кільцем $K/\text{Ann } u$, де $T = \|t_{ij}\|$ — деяка матриця над кільцем K . Очевидно, $K/\text{Ann } u = K/vK$ — локальна область головних ідеалів. Тоді для деяких $n \times n$ -матриць C, D над кільцем K таких, що $\widetilde{C}, \widetilde{D} \in GL(n, K/vK)$, $\widetilde{C}\widetilde{A}\widetilde{D} = \text{diag}[\alpha_1, \alpha_2, \dots, \alpha_r, 0, \dots, 0]$; ($\alpha_i \in K/vK$; $i = 1, \dots, r$; $r \in 0 \cup \mathbb{N}$). Очевидно, $C, D \in GL(n, K)$. Оскільки в полі лишків кільця K/vK $\widetilde{A}^2 = 0$, то $r = \text{rank } \widetilde{A} \leq \frac{n}{2}$. Враховуючи непарність n , отримуємо $r < \frac{n}{2}$. Крім того, у кільці K/vK

$$\widetilde{AD} = \widetilde{A}\widetilde{D} = \widetilde{C}^{-1} \text{diag}[\alpha_1, \alpha_2, \dots, \alpha_r, 0, \dots, 0] =$$

$$\begin{pmatrix} \alpha_{11} & \dots & \alpha_{1r} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \dots & \alpha_{nr} & 0 & \dots & 0 \end{pmatrix},$$

де $\alpha_{ij} \in K/vK$ ($i = 1, \dots, n$; $j = 1, \dots, r$). Тоді в кільці K

$$uAD = \begin{pmatrix} \alpha'_{11} & \dots & \alpha'_{1r} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha'_{n1} & \dots & \alpha'_{nr} & 0 & \dots & 0 \end{pmatrix}.$$

де $\alpha'_{ij} \in uK$ ($i = 1, \dots, n$; $j = 1, \dots, r$). Нехай матриця B_0 одержана з матриці BD відкиданням перших r стовпців. Позначимо тепер через $\widetilde{T} = \|t + \text{Ann } v\|$ матрицю над кільцем $K/\text{Ann } v = K/uK$, де $T = \|t_{ij}\|$ — деяка матриця над кільцем K . Над полем лишків кільця K/uK $\widetilde{B}^2 = 0$,

тому $\text{rank } \widetilde{B} \leq \frac{n}{2}$. Враховуючи непарність n , отримуємо $\text{rank } \widetilde{B} < \frac{n}{2}$. Отже, у полі лишків кільця K/uK $r_0 = \text{rank } \widetilde{B}_0 < \frac{n}{2}$. Аналогічно, як і для матриці A , можна показати, що для деякої матриці $D_0 \in GL(n - r, K)$

$$\widetilde{B_0 D_0} = \widetilde{B_0} \widetilde{D_0} = \begin{pmatrix} \beta_{11} & \dots & \beta_{1r_0} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \dots & \beta_{nr_0} & 0 & \dots & 0 \end{pmatrix},$$

де $\beta_{ij} \in K/uK$ ($i = 1, \dots, n$; $j = 1, \dots, r_0$). Тоді в кільці K

$$vBD \begin{pmatrix} E_r & 0 \\ 0 & D_0 \end{pmatrix} = \begin{pmatrix} \beta'_{11} & \dots & \beta'_{1r} & \beta'_{1r+1} & \dots & \beta'_{1r+r_0} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \beta'_{n1} & \dots & \beta'_{nr} & \beta'_{nr+1} & \dots & \beta'_{nr+r_0} & 0 & \dots & 0 \end{pmatrix},$$

де $\beta'_{ij} \in K/uK$ ($i = 1, \dots, n$; $j = 1, \dots, r + r_0$), E_r — одинична $n \times n$ -матриця над кільцем K . Очевидно,

$$D' = \begin{pmatrix} E_r & 0 \\ 0 & D_0 \end{pmatrix} \in GL(n, K).$$

Останній стовпчик матриці $uADD'$ та $vBDD'$ рівний нулю, бо $r + r_0 < n$. Отже, останній стовпчик матриці MDD' та $(DD')^{-1}\Gamma(a)DD'$ також рівний нулю. Перестановкою першого з останнім стовпцем і такою ж перестановкою рядків матриця $(DD')^{-1}\Gamma(a)DD'$ зводиться до подібної до себе матриці з нульвим першим стовпцем. Тому матриця $(DD')^{-1}\Gamma(a)DD'$, $\Gamma(a)$ та зображення Γ звідне над кільцем K . Лема доведена. $\square$

Теорема 2.15. *Нехай $G = \langle a \rangle$ — скінченна 2-група порядку $|G| > 1$, K — комутативне нетерове локальне кільце характеристики 2 з нескінченним полем лишків, $\text{rad } K = 0$ і для деякого ненульового елемента $u \in K$ $\text{Ann } u$ містить не головний ідеал. Існує нескінченна кількість нееквівалентних незвідних матричних зображень групи G над кільцем K довільного наперед заданого степеня $n > 1$.*

Доведення. Очевидно теорему досить довести для випадку, коли $G = \langle a \rangle$ — циклічна група порядку 2. З теореми 2.12 випливає, що досить розглянути випадок, коли n — непарне число. Оскільки $\text{Ann } u$ містить не головний ідеал, то для деяких $v, w \in \text{Ann } u$, $v \notin wK$, $w \notin vK$.

Припустимо спочатку, що $v^2 \notin vwK + w^2K$, $w^2 \notin v^2K + vwK$. Розглянемо відображення Γ_λ вигляду $a \rightarrow \Gamma_\lambda(a) = E_n + S(\lambda)$, де E_n — одинична $n \times n$ -матриця, $S(\lambda)$ — $n \times n$ -матриця над кільцем K ,

$$S(\lambda) = \begin{pmatrix} vw & w^2 & 0 & 0 & \dots & 0 & 0 & \lambda u \\ v^2 & vw & 0 & 0 & \dots & 0 & 0 & 0 \\ vw & w^2 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & u & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & v^2 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & u & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & v^2 & 0 \end{pmatrix},$$

$\lambda \in K^*$. Враховуючи, що $uv = uw = 0$, одержимо

$$S(\lambda)^2 = \begin{pmatrix} 2v^2w^2 & 2vw^3 & 0 & \dots & 0 & 0 \\ 2v^3w & 2v^2w^2 & 0 & \dots & 0 & 0 \\ 2v^2w^2 & 2vw^3 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Оскільки 2 — характеристика кільця K , то $S(\lambda)^2 = 0$. Враховуючи, що матриці E_n та $S(\lambda)$ комутують, $\Gamma_\lambda : 2 = (E_n + S(\lambda))^2 = E_n + 2S(\lambda) + S(\lambda)^2 = E_n$. Тому Γ_λ є зображенням групи G над кільцем K .

Припустимо, що зображення Γ_λ звідне. Тоді для деякої матриці $C \in$

$GL(n, K)$

$$C^{-1}S(\lambda)C = \begin{pmatrix} A & D \\ 0 & B \end{pmatrix}, \quad (2.21)$$

де A, B — $r \times r$ -матриця та $(n - r) \times (n - r)$ -матриця над кільцем K відповідно ($1 \leq r < n$).

Нехай $\alpha, \beta, \gamma, \delta \in K$, $\alpha u + \beta v^2 + \gamma vw + \delta w^2 = 0$. Тоді $\alpha u^2 = 0$, $(\alpha u)^2 = 0$, $\alpha u = 0$, $\alpha \in \text{Rad } K$. Крім того, $\beta v^2 + \gamma vw + \delta w^2 = 0$ і $\beta, \delta \in \text{Rad } K$. Звідси і з (2.21) одержимо

$$C^{-1}M_iC \equiv \begin{pmatrix} A_i & D_i \\ 0 & B_i \end{pmatrix} \pmod{\text{Rad } K} \quad (i = 1, 2, 3),$$

де

$$M_1 = M_1(\lambda) = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & \lambda \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix},$$

де A_i, B_i — $n \times n$ -матриця та $(n-r) \times (n-r)$ -матриця над кільцем K відповідно ($i = 1, 2, 3$).

Легко бачити

$$M_1(\lambda)M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$(M_1(\lambda)M_2)^{\frac{n-3}{2}} = \begin{pmatrix} 0 & 0 & 0 & \lambda & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

$$M_1(\lambda)M_3 = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Тоді

$$N_1 = N_1(\lambda) = (M_1(\lambda)M_2)^{\frac{n-3}{2}}M_1(\lambda)M_3 = \begin{pmatrix} 0 & \lambda & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

$$N_2 = N_2(\lambda) = M_1(\lambda) + M_2 + M_3 + \lambda^{-1}N_1(\lambda) = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & \lambda \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}.$$

Звідси

$$C^{-1}N_iC \equiv \begin{pmatrix} A'_i & D'_i \\ 0 & B'_i \end{pmatrix} \pmod{\text{Rad } K} \quad (i = 1, 2), \quad (2.22)$$

де A'_i, B'_i — $r \times r$ -матриця та $(n-r) \times (n-r)$ -матриця над кільцем K відповідно ($i = 1, 2$). Очевидно, 1 — ранг матриці $\overline{N_1}$ в полі $K/\text{Rad } K$.

Тоді ранг матриці

$$\overline{C}^{-1}\overline{N_1}\overline{C} = \begin{pmatrix} \overline{A'_1} & \overline{D'_1} \\ 0 & \overline{B'_1} \end{pmatrix}$$

теж рівний 1 і одна із матриць A'_1 або B'_1 складаються з необоротних елементів.

Нехай спочатку матриця $A'_1 \equiv 0 \pmod{\text{Rad } K}$. Із (2.22) одержуємо:

$$N_iC \equiv C \begin{pmatrix} A'_i & D'_i \\ 0 & B'_i \end{pmatrix} \pmod{\text{Rad } K} \quad (i = 1, 2). \quad (2.23)$$

Позначимо: $C = \|c_{ij}\|$ ($c_{ij} \in K$), $C_i = (c_{i1}, \dots, c_{ir})$ ($i = 1, \dots, n$). З (2.23) дістаємо, що $C_2 \equiv 0 \pmod{\text{Rad } K}$,

$$\begin{pmatrix} 0 & \dots & 0 & \lambda \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix} \begin{pmatrix} C_1 \\ \vdots \\ C_n \end{pmatrix} = \begin{pmatrix} C_1 \\ \vdots \\ C_n \end{pmatrix} A'_2.$$

Звідки $C_i = C_{i+1}A'_2$ ($i = 1, \dots, n-1$), $\lambda C_n = C_1A'_2$. Отже, $C_i \equiv 0 \pmod{\text{Rad } K}$ ($i = 1, \dots, n$). Значить, $\det C \equiv 0 \pmod{\text{Rad } K}$, що неможливо.

Нехай тепер матриця $B'_1 \equiv 0 \pmod{\text{Rad } K}$. Із (2.22) одержуємо:

$$C^{-1}N_i \equiv \begin{pmatrix} A'_i & D'_i \\ 0 & B'_i \end{pmatrix} C^{-1} \pmod{\text{Rad } K} \quad (i = 1, 2). \quad (2.24)$$

Позначимо тепер: $C^{-1} = \|c_{ij}\|$ ($c_{ij} \in K$), $C_j = (c_{rj}, \dots, c_{nj})$ ($j = 1, \dots, n$). З (2.24) дістаємо, що $C_1 \equiv 0 \pmod{\text{Rad } K}$,

$$\begin{pmatrix} C_1 & \dots & C_n \end{pmatrix} \begin{pmatrix} 0 & \dots & 0 & \lambda \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix} = B'_2 \begin{pmatrix} C_1 & \dots & C_n \end{pmatrix}.$$

Звідки $C_j = B'_2 C_{j-1}$ ($j = 2, \dots, n$), $\lambda C_1 = B'_2 C_n$. Отже, $C_j \equiv 0 \pmod{\text{Rad } K}$ ($j = 1, \dots, n$). Значить, $\det C \equiv 0 \pmod{\text{Rad } K}$, що неможливо. Одержане протиріччя показує, що зображення Γ_λ незвідне над кільцем K .

Припустимо, що зображення Γ_λ еквівалентне зображенню $\Gamma_{\lambda'}$, де $\lambda, \lambda' \in K^*$, $\lambda \not\equiv \lambda' \pmod{\text{Rad } K}$. Тоді для деякої матриці $C \in GL(n, K)$ $C^{-1}\Gamma_\lambda(a)C = \Gamma_{\lambda'}(a)$. Тому $C^{-1}M_1(\lambda)C \equiv M_1(\lambda') \pmod{\text{Rad } K}$,

$C^{-1}M_iC \equiv M_i \pmod{\text{Rad } K}$ ($i = 2, 3$). Тоді, $C^{-1}(M_1(\lambda) + M_2 + M_3)C \equiv M_1(\lambda') + M_2 + M_3 \pmod{\text{Rad } K}$ і $\lambda \equiv \det(M_1(\lambda) + M_2 + M_3) \equiv \det(M_1(\lambda') + M_2 + M_3) \equiv \lambda' \pmod{\text{Rad } K}$, що неможливо.

Припустимо тепер, що $v^2 \in vwR + w^2R$. Нехай $v^2 = kvw + lw^2$ ($k, l \in K$). Якщо $l \equiv 0 \pmod{\text{Rad } K}$, то покладемо $v_1 = v + mw$, де $m \in K$, $m \not\equiv 0 \pmod{\text{Rad } K}$, $m \not\equiv k \pmod{\text{Rad } K}$. Тоді $v = v_1 + mw$ і $v_1^2 + m^2w^2 = kv_1w + kmw^2 + lw^2$, $v_1^2 = kv_1w + (m^2 + km + l)w^2$, $m^2 + km + l \equiv m(m + k) \not\equiv 0 \pmod{\text{Rad } K}$. Отже, не зменшуючи загальності, будемо вважати, що $l \in K^*$.

Розглянемо відображення Γ_λ вигляду $a \rightarrow \Gamma_\lambda(a) = E_n + S(\lambda)$, де E_n — одинична $n \times n$ -матриця, $S(\lambda)$ — $n \times n$ -матриця над кільцем K ,

$$S(\lambda) = \begin{pmatrix} v & w & 0 & 0 & \dots & 0 & 0 & \lambda u \\ kv + lw & v & 0 & 0 & \dots & 0 & 0 & 0 \\ v & w & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & u & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & w & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & u & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & w & 0 \end{pmatrix},$$

$\lambda \in K^*$. Враховуючи, що $uv = uw = 0$, одержимо

$$S(\lambda)^2 = \begin{pmatrix} v^2 + kvw + lw^2 & 2vw & 0 & \dots & 0 & 0 \\ 2kv^2 + 2lvw & v^2 + kvw + lw^2 & 0 & \dots & 0 & 0 \\ v^2 + kvw + lw^2 & 2vw & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Оскільки 2 — характеристика кільця K , $v^2 = kvw + lw^2$, то $S(\lambda)^2 = 0$ і знову Γ_λ є зображенням групи G над кільцем K .

Припустимо, що зображення Γ_λ звідне. Тоді для деякої матриці $C \in GL(n, K)$

$$C^{-1}S(\lambda)C = \begin{pmatrix} A & D \\ 0 & B \end{pmatrix}, \quad (2.25)$$

де A, B — $r \times r$ -матриця та $(n-r) \times (n-r)$ -матриця над кільцем K відповідно ($1 \leq r < n$).

Нехай $\alpha, \beta, \gamma \in K$, $\alpha u + \beta v + \gamma w = 0$. Тоді $\alpha u^2 = 0$, $(\alpha u)^2 = 0$, $\alpha u = 0$, $\alpha \in \text{Rad } K$. Крім того, $\beta v + \gamma w = 0$ і $\gamma \in \text{Rad } K$. Звідси і з (2.25) одержимо

$$C^{-1}M_iC \equiv \begin{pmatrix} A_i & D_i \\ 0 & B_i \end{pmatrix} \pmod{\text{Rad } K} \quad (i = 1, 2, 3),$$

де

$$M_1 = M_1(\lambda) = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & \lambda \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ l & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix},$$

де A_i, B_i — $r \times r$ -матриця та $(n-r) \times (n-r)$ -матриця над кільцем K відповідно ($i = 1, 2$). Легко бачити

$$M_1(\lambda)M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$N_1 = N_1(\lambda) = (M_1(\lambda)M_2)^{\frac{n-1}{2}} = \begin{pmatrix} 0 & \lambda & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

$$N_2 = N_2(\lambda) = M_1(\lambda) + M_2 + \lambda^{-1}N_1(\lambda) = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & \lambda \\ l & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix},$$

де $N_1 = N_1(\lambda) = (M_1(\lambda)M_2)^{\frac{n-1}{2}}$, $N_2 = N_2(\lambda)$.

Далі аналогічно до випадку $v^2 \notin vwK + w^2K$, $w^2 \notin v^2K + vwK$ зображення Γ_λ незвідне.

Припустимо, що зображення Γ_λ еквівалентне зображенню $\Gamma_{\lambda'}$, де $\lambda, \lambda' \in K^*$, $\lambda \not\equiv \lambda' \pmod{\text{Rad } K}$. Тоді для деякої матриці $C \in GL(n, K)$ $C^{-1}\Gamma_\lambda(a)C = \Gamma_{\lambda'}(a)$. Тому $C^{-1}M_1(\lambda)C \equiv M_1(\lambda') \pmod{\text{Rad } K}$, $C^{-1}M_2C \equiv M_2 \pmod{\text{Rad } K}$. Тоді, $C^{-1}(M_1(\lambda) + M_2)C \equiv (M_1(\lambda') + M_2) \pmod{\text{Rad } K}$ і $\lambda \equiv l^{-1} \det(M_1(\lambda) + M_2) \equiv l^{-1} \det(M_1(\lambda') + M_2) \equiv \lambda' \pmod{\text{Rad } K}$, що неможливо. Теорема доведена. $\square$

2.4. Зображення скінченних 2-груп над областями цілісності характеристики 2

Раніше здобувачем було показано [80, ст. 110, теорема 2] існування незвідних матричних зображень скінченної p -групи G як завгодно високого степеня над цілісним комутативним нетеровим локальним кільцем характеристики p , яке не є областю головних ідеалів, у випадку, коли $|G| > 2$. Для доведення будувались незвідні зображення групи G довільного парного степеня вище 6 або довільного степеня кратного 4. В підрозділі досліджуються матричні зображення непарного степеня групи другого прядку над локальною областю цілісності характеристики 2, будь-який

скінченно породжений ідеал якої володіє мінімальною системою з не більше ніж двох твірних елементів. Одним з прикладів локальної області цілісності довільної простої характеристики p , будь-який скінченно породжений ідеал якої володіє мінімальною системою з не більше ніж двох твірних елементів є кільце формальних степеневих рядів над довільним полем F тої ж характеристики p вигляду

$$a_0 + a_2x^2 + a_3x^3 + \dots,$$

яке відрізняється від кільця всіх формальних степеневих рядів $F[[x]]$ відсутністю доданка a_1x у вигляді.

Нехай K — комутативне кільце з одиницею. Далі через $\text{Rad } R$ будемо позначати радикал Джекобсона кільця K . Нехай $\det M$ — детермінант $n \times n$ -матриці M над комутативним кільцем.

Лема 2.16. *Нехай K — комутативне локальне кільце, I — ідеал кільця K породжений елементами $a_1, a_2, \dots, a_m$. Якщо I володіє системою твірних елементів $b_1, b_2, \dots, b_n$, де $n \leq m$, то I також володіє системою з n твірних елементів, які можна вибрати серед елементів $a_1, a_2, \dots, a_m$.*

Доведення. Очевидно, лему досить довести для випадку, коли $b_1, b_2, \dots, b_n$ — мінімальна система твірних елементів ідеалу I . Тоді з умови $x_1b_1 + x_2b_2 + \dots + x_nb_n = 0$, де $x_1, x_2, \dots, x_n$ — деякі елементи кільця K , випливає, що $x_i \in \text{Rad } R$ ($i = 1, 2, \dots, n$).

Оскільки $b_1, b_2, \dots, b_n$ — система твірних елементів ідеалу I , $a_i \in I$

$(i = 1, \dots, m)$, то для деякої $m \times n$ -матриці A над кільцем K

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} = A \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Оскільки $a_1, a_2, \dots, a_m$ — система твірних елементів ідеалу I , $b_j \in I$ ($j = 1, \dots, n$), то для деякої $n \times m$ -матриці B над кільцем K

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = B \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}.$$

Тоді

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = BA \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

і $BA \equiv E_n \pmod{\text{Rad } K}$, де E_n — одинична матриця порядку n над кільцем K . У полі лишків кільця K ранг матриці $\overline{A}$, одержаної з матриці A редукцією за модулем ідеалу $\text{Rad } R$, рівний n . Не зменшуючи загальності, будемо вважати, що перші n рядків матриці $\overline{A}$ лінійно незалежні над полем лишків кільця K . Тоді

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix},$$

де A_2 — деяка матриця над кільцем K , A_1 — $n \times n$ -матриця над кільцем

K , $\det A_1 \not\equiv 0 \pmod{\text{Rad } R}$. Отже, A_1 — оборотна матриця,

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = A_1 \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}, \quad \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = A_1^{-1} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

Отже, $a_1, a_2, \dots, a_n$ — система твірних елементів ідеалу I . Лема доведена. $\square$

Теорема 2.17. *Нехай K — локальна область цілісності характеристики 2, будь-який скінченно породжений ідеал якої володіє мінімальною системою з не більше ніж двох твірних елементів, $G = \langle a \rangle$ — циклічна група порядку 2. Всі матричні зображення групи G над кільцем K непарного степеня n звідні.*

Доведення. Нехай $\Gamma : a \rightarrow E_n + A$, де E_n — одинична $n \times n$ -матриця, A — деяка матриця того ж розміру над кільцем K , є незвідним матричним K -зображенням групи G . Очевидно, $A^2 = 0$.

Покажемо, що для довільного l ($0 \leq l \leq k$, $k = \frac{n-1}{2}$) знайдуться такі оборотні матриці B і C порядку n над кільцем K , що BAC має вигляд

$$\begin{pmatrix} a_{11} & a_{12} & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & a_{23} & a_{24} & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{l1} & a_{l2} & a_{l3} & a_{l4} & a_{l5} & \dots & a_{l2l} & 0 & \dots & 0 \\ a_{l+11} & a_{l+12} & a_{l+13} & a_{l+14} & a_{l+15} & \dots & a_{l+12l} & a_{l+12l+1} & \dots & a_{l+1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & a_{n5} & \dots & a_{n2l} & a_{n2l+1} & \dots & a_{nn} \end{pmatrix}, \quad (2.26)$$

де $a_{i2i} \neq 0$ ($i = 1, \dots, l$). Застосуємо індукцію по числу l . При $l = 0$ твердження очевидне. Нехай $0 \leq l < k$ і для деяких оборотних матриць B і C порядку n над кільцем K $A' = BAC$ має вигляд (2.26). Якщо в матриці BAC є нульовий стовпчик, то в матриці AC , а отже, і в матриці $C^{-1}AC$ є нульовий стовпчик. Тоді Γ — звідне зображення, що неможливо. Тому $a_{ij} \neq 0$ для деяких i, j ($l+1 \leq i \leq n, 2l+1 \leq j \leq n$).

Оскільки домноження зліва деякої матриці на матрицю підстановки змінює порядок рядків, то, не зменшуючи загальності, будемо вважати, що $I = a_{l+12l+1}R + a_{l+12l+2}R + \dots + a_{l+1n}R \neq 0$. За лемою 2.16 $I = aR + bR$, де a і b вибрано серед елементів $a_{l+12l+1}, a_{l+12l+2}, \dots, a_{l+1n}$. Очевидно, $a \neq 0$ або $b \neq 0$. Оскільки домноження зправа деякої матриці на матрицю підстановки змінює порядок стовпців, то, не зменшуючи загальності, будемо вважати, що $I = a_{l+12l+1}R + a_{l+12l+2}R$ і $a_{l+12l+2} \neq 0$. Тоді $a_{l+1j} = a_{l+12l+1}\gamma_{1j} + a_{l+12l+2}\gamma_{2j}$ для деяких $\gamma_{ij} \in K$ ($i = 1, 2, j = 2l+3, \dots, n$). Нехай

$$C' = \begin{pmatrix} 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & 0 & \gamma_{12l+3} & \dots & \gamma_{1n} \\ 0 & \dots & 0 & 1 & \gamma_{22l+3} & \dots & \gamma_{2n} \\ 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Тоді

$$A'C' =$$

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{l+11} & \alpha_{l+12} & \alpha_{l+13} & \alpha_{l+14} & \alpha_{l+15} & \dots & \alpha_{l+12l+2} & 0 & \dots & 0 \\ \alpha_{l+21} & \alpha_{l+22} & \alpha_{l+23} & \alpha_{l+24} & \alpha_{l+25} & \dots & \alpha_{l+22l+2} & \alpha_{l+22l+3} & \dots & \alpha_{l+2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \alpha_{n4} & \alpha_{n5} & \dots & \alpha_{n2l+2} & \alpha_{n2l+3} & \dots & \alpha_{nn} \end{pmatrix},$$

де $\alpha_{i2i} = a_{i2i} \neq 0$ ($i = 1, \dots, l+1$).

Проведена індукція показує, що для деяких оборотних матриць B і C порядку n над кільцем K

$$\tilde{A} = BAC = \begin{pmatrix} a_{11} & a_{12} & 0 & 0 & 0 & \dots & 0 & 0 \\ a_{21} & a_{22} & a_{23} & a_{24} & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k1} & a_{k2} & a_{k3} & a_{k4} & a_{k5} & \dots & a_{k2k} & 0 \\ a_{k+11} & a_{k+12} & a_{k+13} & a_{k+14} & a_{k+15} & \ddots & a_{k+12k} & a_{k+1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & a_{n5} & \dots & a_{n2k} & a_{nn} \end{pmatrix},$$

де $a_{j2j} \neq 0$ ($j = 1, \dots, k$).

Оскільки $A^2 = 0$, то в полі лишків кільця K $\text{rank } A \leq \frac{n}{2}$. Враховуючи непарність n , одержимо $\text{rank } A \leq \frac{n-1}{2} = k$. Тоді $\text{rank } \tilde{A} \leq k$. Тому мінор $k+1$ -го порядку

$$\begin{vmatrix} a_{12} & 0 & 0 & \dots & 0 & 0 \\ a_{22} & a_{24} & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k2} & a_{k4} & a_{k6} & \dots & a_{k2k} & 0 \\ a_{i2} & a_{i4} & a_{i6} & \dots & a_{i2k} & a_{in} \end{vmatrix}$$

матриці $\bar{A}$ рівний 0 ($i = k + 1, \dots, n$). Оскільки $a_{j2j} \neq 0$ ($j = 1, \dots, k$), то $a_{in} = 0$ ($i = k + 1, \dots, n$). Але тоді останній стовпчик матриці $\tilde{A} = BAC$, а отже, і AC , $C^{-1}AC$ рівний 0. Перестановкою першого з останнім стовпцем і такою ж перестановкою рядків матриця $C^{-1}AC$ зводиться до подібної до себе матриці з нульовим першим стовпцем. Тому матриця $C^{-1}AC$, A та зображення Γ звідне над кільцем K , що неможливо. Теорема доведена. $\square$

2.5. Зображення діедральних груп порядку $2p$ над кільцями характеристики 2

В підрозділі досліджуються, з точністю до еквівалентності, матричні зображення 2-го степеня групи діедра порядку $2p$ (p — непарне просте число) над комутативними локальними кільцями K головних ідеалів характеристики 2, радикали Джекобсона $\text{Rad } K = tK$ яких є нільпотентними ідеалами другого степеня. Такі кільця ще називають *локальними кільцями довжини 2* характеристики 2. Відомо, що комутант групи діедра $G = \langle a, b | a^2 = b^p = (ab)^2 = e \rangle$ при непарному p рівний $G' = \langle b \rangle$ і міститься в ядрі довільного зображення Γ групи G над кільцем K першого степеня (кожне з яких незвідне). Тоді

$$\Gamma(b) = 1.$$

Якщо $\Gamma(a) = 1 + \alpha'$ ($\alpha' \in K$), то $1 = \Gamma(a)^2 = (1 + \alpha')^2 = 1 + 2\alpha' + \alpha'^2 = 1 + \alpha'^2$. Тобто $\alpha' \in \text{Rad } K = tK$, $\alpha' = t\alpha$ ($\alpha \in K$). Отже,

$$\Gamma(a) = 1 + t\alpha \quad (\alpha \in K).$$

Далі через $\bar{z}$ будемо позначати $z + \text{Rad } R$ поля $R/\text{Rad } R$ ($z \in K$), $\bar{T} = \|\bar{t}_{ij}\|$ — матрицю над цим же полем, де $T = \|t_{ij}\|$ — деяка матриця

над кільцем K . Навпаки, відображення

$$\Gamma_{\bar{\alpha}}: b \rightarrow 1, a \rightarrow 1 + t\alpha \ (\alpha \in K)$$

задовольняє умови

$$\Gamma_{\bar{\alpha}}(a)^p = \Gamma_{\bar{\alpha}}(b)^p = \Gamma_{\bar{\alpha}}(ab)^2 = 1,$$

бо

$$\Gamma_{\bar{\alpha}}(a)^2 = (1 + t\alpha)^2 = 1 + 2t\alpha + t^2\alpha^2 = 1,$$

$$\Gamma_{\bar{\alpha}}(b)^2 = 1^p = 1,$$

$$(\Gamma_{\bar{\alpha}}(a)\Gamma_{\bar{\alpha}}(b))^2 = \Gamma_{\bar{\alpha}}(a)^2 = 1.$$

Отже, $\Gamma_{\bar{\alpha}}$ вичерпує всі (незвідні) матричні зображення першого степеня групи G над кільцем K нееквівалентні при різних значеннях $\bar{\alpha}$ поля $K/\text{Rad } K$.

Лема 2.18. *Нехай K — комутативне локальне кільце характеристики 2, $\text{Rad } R = tR$, $t \in K$, $t^2 = 0$, $t \neq 0$, $G = \langle a, b | a^2 = b^p = (ab)^2 = e \rangle$ — група дієдра порядку $2p$ (p — непарне просте число). Відображення*

$$\Gamma_{\bar{F}}: a \rightarrow E_2 + tF, b \rightarrow E_2,$$

де E_2 — одинична 2×2 -матриця порядку 2, F — будь-яка 2×2 -матриця над кільцем K , є матричне зображення групи G над кільцем K . Зображення $\Gamma_{\bar{F}}$ звідне над кільцем K тоді і тільки тоді, коли звідна матриця $\bar{F}$ над полем $K/\text{rad } K$.

Доведення. Нехай F — будь-яка 2×2 -матриця над кільцем K . Легко бачити, що

$$\Gamma_{\bar{F}}(a)^2 = (E_2 + tF)^2 = E_2 + 2F + t^2F^2 = E_2,$$

$$\Gamma_{\overline{F}}(b)^p = E_2^p = E_2,$$

$$(\Gamma_{\overline{F}}(a)\Gamma_{\overline{F}}(b))^2 = (\Gamma_{\overline{F}}(a)E_2)^2 = \Gamma_{\overline{F}}(a)^2 = E_2.$$

Отже, відображення $\Gamma_{\overline{F}}$ є зображення групи G . Оскільки $\Gamma_{\overline{F}}(b) = E_2$, то зображення $\Gamma_{\overline{F}}$ звідне над кільцем K тоді і тільки тоді, коли звідна матриця $\Gamma_{\overline{F}}(b)$ над кільцем K . Тобто, коли звідна матриця tF над кільцем K , або, що одне і те ж, коли звідна матриця $\overline{F}$ над полем $K/\text{rad } K$. $\square$

Лема 2.19. *Нехай K — комутативне локальне кільце характеристики 2, $\text{Rad } R = tR$, $t \in K$, $t^2 = 0$, $t \neq 0$, $G = \langle a, b | a^2 = b^p = (ab)^2 = e \rangle$ — група діебра порядку $2p$ (p — непарне просте число). Відображення*

$$\Delta: a \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow E_2,$$

є звідне матричне зображення групи G над кільцем K .

Доведення. Легко бачити, що

$$\Delta(a)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = E_2,$$

$$\Delta(b)^p = E_2^p = E_2,$$

$$(\Delta(a)\Delta(b))^2 = (\Delta(a)E_2)^2 = \Delta(a)^2 = E_2.$$

Отже, відображення Δ є зображення групи G , звідність якого очевидна. $\square$

Лема 2.20. *Нехай K — комутативне локальне кільце характеристики 2, $\text{Rad } R = tR$, $t \in K$, $t^2 = 0$, $t \neq 0$, $G = \langle a, b | a^2 = b^p = (ab)^2 = e \rangle$ — група діебра порядку $2p$ (p — непарне просте число). Якщо поле лишків кільця K містить тільки один корінь p -го степеня з одиниці,*

то відображення

$$\Lambda_\alpha : a \rightarrow \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix},$$

де α — будь-який елемент кільця K такий, що многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$, є незвідне матричне зображення групи G над кільцем K .

Доведення. Нехай α — будь-який елемент кільця K такий, що многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$. Легко бачити, що

$$\Lambda_\alpha(a)^2 = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix} = E_2.$$

Оскільки многочлен $x^p + 1 = (x^2 + \alpha x + 1)\varphi(x)$ для деякого $\varphi(x) \in K[x]$, то

$$\begin{aligned} \Lambda_\alpha(b)^p + E_n &= (\Lambda_\alpha(b)^2 + \alpha\Lambda_\alpha(b) + 1)\varphi(\Lambda_\alpha(b)) = \\ &= \left(\begin{pmatrix} 1 & \alpha \\ \alpha & 1 + \alpha^2 \end{pmatrix} + \alpha \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \varphi(\Lambda_\alpha(b)) = 0 \cdot \varphi(\Lambda_\alpha(b)) = 0. \end{aligned}$$

Тобто $\Lambda_\alpha(b)^p = E_n$. Крім того,

$$\begin{aligned} (\Lambda_\alpha(a)\Lambda_\alpha(b))^2 &= \left(\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix} \right)^2 = \\ &= \begin{pmatrix} \alpha & 1 + \alpha^2 \\ 1 & \alpha \end{pmatrix}^2 = \begin{pmatrix} 1 + 2\alpha^2 & 2\alpha(1 + \alpha^2) \\ 2\alpha & 1 + 2\alpha^2 \end{pmatrix} = E_2. \end{aligned}$$

Отже, відображення $\Gamma_{\bar{F}}$ є зображенням групи G .

Оскільки многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$, то многочлен $x^2 + \bar{\alpha}x + 1$ ділить $x^p + 1$ у кільці $(K/\text{Rad}K)[x]$. Так-як поле $K/\text{Rad}K$ містить тільки один корінь p -го степеня з одиниці, то многочлен $x^2 + \bar{\alpha}x + 1$ не має коренів у полі $K/\text{Rad}K$. Многочлен $x^2 + \bar{\alpha}x + 1$

незвідний в полі $K/\text{Rad } K$, а многочлен $x^2 + \alpha x + 1$ незвідний у кільці K . Останній, однак, є характеристичним многочленом матриці

$$\Lambda_\alpha(b) = \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}.$$

Отже, зображення Λ_α незвідне над кільцем K . $\square$

Теорема 2.21. *Нехай K — комутативне локальне кільце характеристики 2, $\text{Rad } R = tR$, $t \in K$, $t^2 = 0$, $t \neq 0$, $G = \langle a, b | a^2 = b^p = (ab)^2 = e \rangle$ — група діедра порядку $2p$ (p — непарне просте число). Γ — матричне зображення 2-го степеня групи G над кільцем K . Якщо поле лишків кільця K містить тільки один корінь p -го степеня з одиниці, то виконується одна з умов:*

- 1) зображення Γ еквівалентне зображенню вигляду

$$\Gamma_{\overline{F}}: a \rightarrow E_2 + tF, \quad b \rightarrow E_2,$$

де E_2 — одинична матриця порядку 2, F — будь-яка 2×2 -матриця над кільцем K ;

- 2) зображення Γ еквівалентне зображенню вигляду

$$\Delta: a \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow E_2;$$

- 3) зображення Γ еквівалентне зображенню вигляду

$$\Lambda_\alpha: a \rightarrow \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix},$$

де α — будь-який елемент кільця K такий, що многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$.

Два зображення різних виглядів не еквівалентні над кільцем K . Два зображення $\Gamma_{\overline{F}_1}, \Gamma_{\overline{F}_2}$ (F_1, F_2 — 2×2 -матриці над кільцем K) еквівалентні над кільцем K тоді і тільки тоді, коли матриці $\overline{F}_1, \overline{F}_2$ подібні

над полем лишків кільця K . Два зображення $\Lambda_{\alpha_1}, \Lambda_{\alpha_2}$ ($\alpha_1, \alpha_2 \in K$, многочлени $x^2 + \alpha_1 x + 1$ та $x^2 + \alpha_2 x + 1$ ділять $x^p + 1$ у кільці $K[x]$) еквівалентні над кільцем K тоді і тільки тоді, коли $\alpha_1 = \alpha_2$.

Доведення. Нехай Γ — матричне зображення групи G над кільцем K 2-го степеня, $\Gamma : a \rightarrow A, b \rightarrow B$, де A, B — 2×2 -матриці над кільцем K . Тоді $A^2 = B^p = (AB)^2 = E_2$.

Нормальна форма Фробеніуса матриці $\bar{B}$ над полем лишків кільця K має вигляд

$$\begin{pmatrix} \bar{\varepsilon} & \bar{0} \\ \bar{0} & \bar{\theta} \end{pmatrix} \text{ або } \begin{pmatrix} \bar{0} & \bar{\delta} \\ \bar{1} & \bar{\gamma} \end{pmatrix}$$

для деяких $\varepsilon, \theta, \gamma, \delta \in K$. Оскільки $\bar{B}^p = \bar{E}_2$ і поле лишків кільця K містить тільки один корінь p -го степеня з одиниці, то $\bar{\varepsilon} = \bar{\theta} = \bar{1}$, $\bar{\delta} = \det \bar{B} = \bar{1}$. Не зменшуючи загальності, будемо вважати, що

$$B = E_2 + tL \quad (2.27)$$

або

$$B = \begin{pmatrix} 0 & 1 \\ 1 & \gamma \end{pmatrix} + tL, \quad (2.28)$$

де L — 2×2 -матриця над кільцем K .

Розглянемо спочатку випадок (2.27). Очевидно, $p = 2q + 1$ (q — ціле число). Тоді $E_2 = B^p = ((E_2 + tL)^2)^q (E_2 + tL) = E_2 + tL$. Отже, $tL = 0$, $B = E_2$. Оскільки $A^2 = E_2$, то матриця $\bar{A}$ над полем $R/\text{Rad } R$ характеристики 2 подібна до матриці $\bar{E}_2$ або до матриці

$$\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}.$$

Для будь-якої оборотної матриці C порядку 2 над кільцем K $C^{-1}BC = C^{-1}E_2C = E_2 = B$. Тому, не зменшуючи загальності, будемо вважати,

що

$$A = E_2 + tF \quad (2.29)$$

або

$$A = E_2 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + tF, \quad (2.30)$$

де F — 2×2 -матриця над кільцем K .

У випадку (2.29) зображення Γ має вигляд

$$\Gamma : a \rightarrow E_2 + tF, \quad b \rightarrow E_2. \quad (2.31)$$

За лемою 2.18 при будь-якій 2×2 -матриці F над кільцем K відображення вигляду (2.31) є зображенням групи G . Очевидно, два зображення такого вигляду еквівалентні над кільцем K тоді і тільки тоді, коли відповідні матриці $\bar{F}$ подібні над полем $R/\text{Rad } R$.

Розглянемо тепер випадок (2.30). Нехай

$$F = \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \quad (f_{ij} \in K, \quad i, j = 1, 2).$$

Оскільки $A^2 = E_2$, E_2 комутує з довільною 2×2 -матрицею над кільцем K , характеристика якого 2, то

$$\begin{aligned} E_2 &= \left(E_2 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + t \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \right)^2 = \\ &= E_2 + \left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + t \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \right)^2. \end{aligned}$$

Враховуючи, що $t^2 = 0$, одержимо

$$E_2 = E_2 + t \begin{pmatrix} f_{21} & f_{22} \\ 0 & 0 \end{pmatrix} + t \begin{pmatrix} 0 & f_{11} \\ 0 & f_{21} \end{pmatrix}.$$

Отже, $tf_{21} = 0$, $tf_{11} = tf_{22}$. Тоді матриця A має вигляд

$$A = E_2 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + t \begin{pmatrix} f_{11} & f_{12} \\ 0 & f_{11} \end{pmatrix}.$$

Очевидно,

$$C = E_2 + t \begin{pmatrix} f_{12} & 0 \\ f_{11} & 0 \end{pmatrix} = \begin{pmatrix} 1 + tf_{12} & 0 \\ tf_{11} & 1 \end{pmatrix}$$

— оборотна матриця порядку 2 над кільцем K . Оскільки E_2 комутує з довільною 2×2 -матрицею над кільцем K , характеристика якого 2, то

$$C^2 = \left(E_2 + t \begin{pmatrix} f_{12} & 0 \\ f_{11} & 0 \end{pmatrix} \right)^2 = E_2 + t^2 \begin{pmatrix} f_{12} & 0 \\ f_{11} & 0 \end{pmatrix}^2 = E_2$$

і $C^{-1} = C$. Тоді

$$\begin{aligned} C^{-1}AC &= C^{-1} \left(E_2 + \begin{pmatrix} tf_{11} & 1 + tf_{12} \\ 0 & tf_{11} \end{pmatrix} \right) C = \\ &= E_2 + \begin{pmatrix} 1 + tf_{12} & 0 \\ tf_{11} & 1 \end{pmatrix} \begin{pmatrix} tf_{11} & 1 + tf_{12} \\ 0 & tf_{11} \end{pmatrix} \begin{pmatrix} 1 + tf_{12} & 0 \\ tf_{11} & 1 \end{pmatrix} = \\ &= E_2 + \begin{pmatrix} tf_{11} & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 + tf_{12} & 0 \\ tf_{11} & 1 \end{pmatrix} = E_2 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \\ C^{-1}BC &= C^{-1}E_2C = E_2 = B. \end{aligned}$$

Не зменшуючи загальності, будемо вважати, що

$$A = E_2 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Отже, у випадку (2.30) зображення Γ має вигляд

$$\Gamma : a \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow E_2. \quad (2.32)$$

За лемою 2.19 відображення вигляду (2.32) є зображенням групи G .
Очевидно, воно не еквівалентне жодному зображенню вигляду (2.31).

Розглянемо тепер випадок (2.28). Нехай

$$L = \begin{pmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \end{pmatrix} \quad (l_{ij} \in K, \ i, j = 1, 2).$$

Очевидно,

$$C = E_2 + t \begin{pmatrix} 0 & l_{11} \\ 0 & l_{21} \end{pmatrix} = \begin{pmatrix} 1 & tl_{11} \\ 0 & 1 + tl_{21} \end{pmatrix}$$

— оборотна матриця порядку 2 над кільцем K . Як і раніше, $C^2 = E_2$ і $C^{-1} = C$. Тоді

$$\begin{aligned} C^{-1}BC &= C^{-1} \left(\begin{pmatrix} 0 & 1 \\ 1 & \gamma \end{pmatrix} + \begin{pmatrix} tl_{11} & tl_{21} \\ tl_{12} & tl_{22} \end{pmatrix} \right) C = \\ &= \begin{pmatrix} 1 & tl_{11} \\ 0 & 1 + tl_{21} \end{pmatrix} \begin{pmatrix} tl_{11} & 1 + tl_{21} \\ 1 + tl_{12} & \gamma + tl_{22} \end{pmatrix} \begin{pmatrix} 1 & tl_{11} \\ 0 & 1 + tl_{21} \end{pmatrix} = \\ &= \begin{pmatrix} 2tl_{11} & 1 + t\gamma l_{11} + tl_{21} \\ 1 + 2tl_{21} & \gamma + tl_{22} + t\gamma l_{21} \end{pmatrix} \begin{pmatrix} 1 & tl_{11} \\ 0 & 1 + tl_{21} \end{pmatrix} = \\ &= \begin{pmatrix} 0 & 1 + t\gamma l_{11} + tl_{21} \\ 1 & \gamma + tl_{22} + t\gamma l_{21} \end{pmatrix} \begin{pmatrix} 1 & tl_{11} \\ 0 & 1 + tl_{21} \end{pmatrix} = \begin{pmatrix} 0 & \beta \\ 1 & \alpha \end{pmatrix}, \end{aligned}$$

для деяких елементів $\alpha, \beta \in K$. Оскільки $B^p = E_2$, то $\beta^p = \det B^p = 1$.
Тоді $\beta = 1 + tr$ ($r \in K$). Звідси $1 = (1 + tr)^p = ((1 + tr)^2)^q(1 + tr) = 1 + tr = \beta$. Не зменшуючи загальності, будемо вважати, що

$$B = \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}.$$

Оскільки $\overline{B} \neq E_2$, $(\overline{B}^2)^q \overline{B} = \overline{B}^p = \overline{E}_2$, то

$$\overline{B}^2 = \begin{pmatrix} 1 & \overline{\alpha} \\ \overline{\alpha} & 1 + \overline{\alpha}^2 \end{pmatrix} \neq \overline{E}_2.$$

Отже, елемент $\bar{\alpha} \neq 0$ і α оборотний. Крім того, відображення $\phi : K[x] \rightarrow M(2, K)$ ($M(2, K)$ — повне матричне кільце степаня 2 над кільцем K) задане за правилом $\phi : f(x) \rightarrow f(B)$ є гомоморфізмом кілець.

$$\phi(x^p + 1) = B^p + E_2 = 0,$$

$$\begin{aligned} \phi(x^2 + \alpha x + 1) &= B^2 + \alpha B + E_2 = \\ &= \begin{pmatrix} 1 & \alpha \\ \alpha & 1 + \alpha^2 \end{pmatrix} + \alpha \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0. \end{aligned}$$

Отже, $x^p + 1, x^2 + \alpha x + 1 \in \ker \phi$. Оскільки старший коефіцієнт многочлена $x^2 + \alpha x + 1$ оборотний, то $x^p + 1 = (x^2 + \alpha x + 1)q(x) + \omega x + \nu$ для деяких $q(x) \in K[x]; \omega, \nu \in K$. Звідси

$$0 = \omega B + \nu E_2 = \omega \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix} + \nu \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \nu & \omega \\ \omega & \omega\alpha + \nu \end{pmatrix}.$$

Тоді $\omega = \nu = 0$ і многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$.

Нехай $A = E_2 + A'$, де

$$A' = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

— 2×2 -матриця над кільцем K . Припустимо, що

$$\bar{A}' = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}.$$

Тоді $\bar{A} = \bar{E}_2, \bar{E}_2 = (\bar{A}\bar{B})^2 = (\bar{B})^2$, що неможливо. Отже,

$$\bar{A}' \neq \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}. \quad (2.33)$$

Тоді серед елементів $a_{11}, a_{12}, a_{21}, a_{22}$ є оборотні елементи кільця K . Покладемо

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} \quad \text{або} \quad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix},$$

де $x, y \in K$, так, щоб серед елементів x, y були оборотні елементи кільця K . Визначник $\det C$ матриці

$$C = \begin{pmatrix} x & y \\ y & x + \alpha y \end{pmatrix}$$

має вигляд $x^2 + \alpha xy + y^2$. Припустимо $x^2 + \alpha xy + y^2 \equiv 0 \pmod{\text{Rad } R}$. Нехай y — оборотний елемент кільця K , то $(xy^{-1})^2 + \alpha(xy^{-1}) + 1 \equiv 0 \pmod{\text{Rad } R}$. Оскільки в кільці $K[x]$ $x^2 + \alpha x + 1$ ділить $x^p + 1$, то $(xy^{-1})^p \equiv 1 \pmod{\text{Rad } R}$. Оскільки $R/\text{Rad } R$ не містить неединичних коренів p -го степеня з одиниці, то $x \equiv y \pmod{\text{Rad } R}$. Аналогічний висновок справедливий у випадку, коли y оборотний елемент кільця K . Тоді $x^2 + \alpha xy + y^2 \equiv \alpha x^2 \equiv \alpha y^2 \not\equiv 0 \pmod{\text{Rad } R}$, що неможливо. Отже, матриця C — оборотна і

$$C^{-1} = (\det C)^{-1} \begin{pmatrix} x + \alpha y & y \\ y & x \end{pmatrix}.$$

Оскільки $E_2 + A'^2 = (E_2 + A')^2 = A^2 = E_2$, $A'^2 = 0$, то

$$A' \begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

$$C^{-1}A'C = (\det C)^{-1} \begin{pmatrix} x + \alpha y & y \\ y & x \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x & y \\ y & x + \alpha y \end{pmatrix} = \begin{pmatrix} 0 & \mu \\ 0 & \lambda \end{pmatrix}$$

для деяких $\lambda, \mu \in K$. Легко бачити, що

$$C^{-1}BC = C^{-1}B \begin{pmatrix} x & y \\ y & x + \alpha y \end{pmatrix} = C^{-1}B(xE_2 + yB) =$$

$$C^{-1}(xE_2 + yB)B = C^{-1}CB = B.$$

Не зменшуючи загальності, будемо вважати, що

$$A' = \begin{pmatrix} 0 & \lambda \\ 0 & \mu \end{pmatrix}.$$

Оскільки $A'^2 = E_2$, то $\mu \equiv 0 \pmod{\text{Rad } R}$,

$$\lambda\mu = 0. \quad (2.34)$$

З (2.33) одержимо, що $\lambda \not\equiv 0 \pmod{\text{Rad } R}$, звідси і з (2.34) $\mu = 0$. Тоді

$$A = E_2 + A' = E_2 + \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix},$$

$$E_2 = (AB)^2 = \begin{pmatrix} \lambda & 1 + \lambda\alpha \\ 1 & \alpha \end{pmatrix}^2 = \begin{pmatrix} 1 + \lambda^2 + \lambda\alpha & (1 + \lambda\alpha)(\lambda + \alpha) \\ \lambda + \alpha & 1 + \lambda\alpha + \alpha^2 \end{pmatrix}.$$

Тоді $\lambda = \alpha$.

Отже, у випадку (2.28) зображення Γ має вигляд

$$\Gamma : a \rightarrow \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}.$$

За лемою 2.20 відображення заданого вигляду є зображенням групи G для будь-якого $\alpha \in K$ такого, що многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$. Крім того, воно не еквівалентне жодному зображенню вигляду (2.31) і зображенню вигляду (2.32). Оскільки α — слід матриці $\Gamma(b)$, то він визначається зображенням Γ однозначно.

Теорема доведена. □

Наслідок 2.22. *Нехай K — комутативне локальне кільце характеристики 2, $\text{Rad } R = tR$, $t \in K$, $t^2 = 0$, $t \neq 0$, $G = \langle a, b | a^2 = b^p = (ab)^2 = e \rangle$ — група діедра порядку $2p$ (p — непарне просте число). Якщо поле лишків кільця K містить тільки один корінь p -го степеня з одиниці,*

то довільне незвідне матричне зображення 2-го степеня групи G над кільцем K еквівалентне одному із зображень

$$\Gamma_{f(x)} : a \rightarrow E_2 + tF, \quad b \rightarrow E_2,$$

де E_2 — одинична 2×2 -матриця, F — будь-яка 2×2 -матриця над кільцем K , така, що $\bar{F}$ — супровідна матриця незвідного многочлена $f(x)$ над полем $K/\text{Rad } K$, або

$$\Lambda_\alpha : a \rightarrow \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix},$$

де α — будь-який елемент кільця K такий, що многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$.

Два зображення різних виглядів не еквівалентні над кільцем K . Два зображення $\Gamma_{f_1(x)}, \Gamma_{f_2(x)}$ ($f_1(x), f_2(x)$ — незвідні нормовані многочлени над полем $K/\text{Rad } K$ степеня 2) еквівалентні над кільцем K тоді і тільки тоді, коли $f_1(x) = f_2(x)$. Два зображення $\Lambda_{\alpha_1}, \Lambda_{\alpha_2}$ ($\alpha_1, \alpha_2 \in K$, многочлени $x^2 + \alpha_1 x + 1$ та $x^2 + \alpha_2 x + 1$ ділять $x^p + 1$ у кільці $K[x]$) еквівалентні над кільцем K тоді і тільки тоді, коли $\alpha_1 = \alpha_2$.

Доведення. Нехай Γ — незвідне матричне зображення групи G над кільцем K другого степеня. За теоремою 2.21 зображення Γ еквівалентне і тільки одному з виглядів (2.35)–(2.37) зображень

$$\Gamma_{\bar{F}} : a \rightarrow E_2 + tF, \quad b \rightarrow E_2, \quad (2.35)$$

де F — будь-яка 2×2 -матриця над кільцем K ;

$$\Delta : a \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow E_2; \quad (2.36)$$

$$\Lambda_\alpha : a \rightarrow \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}, \quad (2.37)$$

де α — будь-який елемент кільця K такий, що многочлен $x^2 + \alpha x + 1$ ділить $x^p + 1$ у кільці $K[x]$.

Очевидно, незвідне зображення Γ не еквівалентне зображенню вигляду (2.36), яке є звідним. За лемою 2.18 зображення (2.35) незвідне над кільцем K тоді і тільки тоді, коли незвідна матриця $\overline{F}$ над полем $K/\text{Rad } K$. Тобто, коли незвідний характеристичний многочлен $f(x)$ матриці $\overline{F}$ над полем $K/\text{Rad } K$. Не зменшуючи загальності, можна вважати, що $\overline{F}$ — супровідна матриця незвідного нормованого многочлена $f(x)$ над полем $K/\text{Rad } K$ степеня 2. В цьому випадку зображення $\Gamma_{\overline{F}}$ будемо позначати $\Gamma_{f(x)}$. За теоремою 2.21 два зображення $\Gamma_{f_1(x)}$, $\Gamma_{f_2(x)}$ ($f_1(x)$, $f_2(x)$ — незвідні нормовані многочлени над полем $K/\text{Rad } K$ степеня 2) еквівалентні над кільцем K тоді і тільки тоді, коли супровідні матриці $\overline{F}_1$, $\overline{F}_2$ незвідних многочленів $f_1(x)$, $f_2(x)$ подібні над полем $K/\text{Rad } K$. Тобто, тоді і тільки тоді, коли $f_1(x) = f_2(x)$.

За лемою 2.20 зображення (2.37) незвідне над кільцем K . За теоремою 2.21 два зображення Λ_{α_1} , Λ_{α_2} ($\alpha_1, \alpha_2 \in K$, многочлени $x^2 + \alpha_1 x + 1$ та $x^2 + \alpha_2 x + 1$ ділять $x^p + 1$ у кільці $K[x]$) еквівалентні над кільцем K тоді і тільки тоді, коли $\alpha_1 = \alpha_2$. $\square$

2.6. Висновки до розділу

У цьому розділі досліджуються незвідні зображення над комутативним кільцем та вивчаються їх властивості.

В підрозділі 2.2 встановлено критерій скінченності множини нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи над комутативним нетеровим локальним кільцем характеристики p^s ($s > 0$), яке не є напівпервісним, з нескінченним полем лишків. Показано, що множина нееквівалентних незвідних матричних

зображень наперед заданого степеня скінченної p -групи над цим кільцем або нескінченна, або порожня.

В підрозділі 2.3 показано нескінченність числа всіх нееквівалентних незвідних матричних зображень наперед заданого степеня $n > 1$ скінченної p -групи G порядку $|G| > 2$ над комутативним нетеровим локальним напівпервісним нецілісним кільцем характеристики p , з нескінченним полем лишків. Також показано нескінченність числа всіх нееквівалентних незвідних матричних зображень наперед заданого степеня $n > 1$ скінченної 2-групи G порядку $|G| > 1$ над комутативним локальним напівпервісним нецілісним кільцем, яке містить неголовний анулятор деякого з своїх елементів характеристики p , поле класів лишків якого нескінченне.

В підрозділі 2.4 доводиться, що всі матричні зображення непарного степеня групи другого прядку над локальною областю цілісності характеристики 2, будь-який скінченно породжений ідеал якої володіє мінімальною системою з не більше ніж двох твірних елементів, звідні.

В підрозділі 2.5 описано всі, з точністю до еквівалентності, матричні зображення 2-го степеня групи діедра порядку $2p$ (p — непарне просте число) над комутативними локальними кільцями довжини 2 характеристики 2, та з'ясовано критерій їх незвідності.

Результати цього розділу анонсовано в [218, 221], та опубліковані в роботах [77, 79, 81–83].

РОЗДІЛ 3.

МОНОМІАЛЬНІ МАТРИЦІ НАД КОМУТАТИВНИМИ КІЛЬЦЯМИ

В межах розділу, якщо не сказано іншого, через K будемо позначати комутативне локальне кільце, радикал Джекобсона якого $tK \neq 0$ ($t \in K$), через K^* будемо позначати групу відносно множення оборотних елементів кільця K . Також елемент $t + \text{Rad } K$ поля лишків $K/\text{Rad } K$ кільця K позначаємо через $\bar{t}$ і для (довільної) матриці $T = (t_{ij})$ над кільцем K покладемо $\bar{T} = (\bar{t}_{ij})$.

3.1. Означення і позначення

Як і раніше, називаємо $n \times n$ -матриця M над кільцем K називається *мономіальною*, якщо кожний її рядок і кожний її стовпець містить рівно один ненульовий елемент (див. підрозділ 1.2).

Матрицю над комутативним кільцем K з одиницею

$$M(a_1, \dots, a_n) = \begin{pmatrix} 0 & \dots & 0 & a_n \\ a_1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & a_{n-1} & 0 \end{pmatrix},$$

де $a_i \neq 0$ ($i = 1, \dots, n$) називаємо *канонічно циклічною*. Будь-яку квадратну матрицю над кільцем K переставно подібну канонічно циклічній називають *циклічною*. Очевидно, довільна інша мономіальна матриця подібна прямій сумі канонічно циклічних матриць.

Для комутативного локального кільця K , радикал Джекобсона якого $tK \neq 0$ ($t \in K$), $a_i = \varepsilon_i t^{s_i}$, де $s_i \geq 0$ і $\varepsilon_i \in K^*$. Питання розкладності та

подібності канонічно циклічних матриць над таким кільцем K ґрунтовно досліджено в [11].

З'ясуємо питання звідності матриць $M(a_1, \dots, a_n)$ над довільним комутативним кільцем K з одиницею у випадку, коли $a_i = t^{s_i}$, де $s_i \geq 0$ для деякого елемента $t \in K$. В такому формулюванні задача була покладена В. М. Бондаренком. Квадратну матрицю над кільцем K переставно подібну $M(t^{s_1}, \dots, t^{s_n})$ називаємо *t-циклічною*.

3.2. Спадкова звідність t-циклічних матриць

Кажуть, що *t-циклічна матриця є спадковою звідною*, якщо вона подібна до матриці

$$M' = \begin{pmatrix} M(t^{s'_1}, \dots, t^{s'_{n'}}) & * \\ 0 & N \end{pmatrix}, \quad n' \neq n,$$

для деяких $s_i \in \{0, 1, 2, \dots\}$ ($i = 1, \dots, n'$) і *спадково незвідною* в іншому випадку. Поняття спадкової звідності для *t-циклічних* і аналогічних класів мономіальних матриць було запропоновано В. М. Бондаренком.

Розглянемо спочатку канонічно λ -циклічні матриці над кільцем цілочислових поліномів $\mathbb{Z}[\lambda]$ від невідомої λ . Доведемо кілька тверджень, які використовуватимуться при встановленні спадкової звідності λ -циклічної матриці $M(\lambda, k, n)$ над кільцем $\mathbb{Z}[\lambda]$ в деяких випадках.

Твердження 3.1. Нехай n, n' — натуральні числа, $n' | n$, $l_i \geq 0$ ($i =$

$1, \dots, n)$, $r_i \geq 0$ ($i = 1, \dots, n'$). Існує $n \times n'$ -матриця

$$S = \begin{pmatrix} \lambda^{s_1} & 0 & \dots & 0 \\ 0 & \lambda^{s_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_{n'}} \\ \lambda^{s_{n'+1}} & 0 & \dots & 0 \\ 0 & \lambda^{s_{n'+2}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_{2n'}} \\ \dots & \dots & \dots & \dots \\ \lambda^{s_{n-n'+1}} & 0 & \dots & 0 \\ 0 & \lambda^{s_{n-n'+2}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_n} \end{pmatrix},$$

де $s_i \geq 0$ ($i = 1, \dots, n$), така, що $M(t^{l_1}, \dots, t^{l_n})S = SM(t^{r_1}, \dots, t^{r_{n'}})$ тоді і тільки тоді, коли

$$\frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}.$$

Доведення. Зрозуміло, що

$$M(t^{l_1}, \dots, t^{l_n}) = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{l_n} \\ \lambda^{l_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{l_k} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{l_{k+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{l_{n-1}} & 0 \end{pmatrix},$$

$$M(t^{r_1}, \dots, t^{r_{n'}}) = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{r_{n'}} \\ \lambda^{r_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{r_{k'}} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{r_{k'+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{r_{n'-1}} & 0 \end{pmatrix}.$$

Позначимо через (i, j) скалярну рівність

$$(M(t^{l_1}, \dots, t^{l_n})S)_{ij} = (SM(t^{r_1}, \dots, t^{r_{n'}}))_{ij}.$$

Очевидно, у кожної з матриць $M(t^{l_1}, \dots, t^{l_n})S$ і $SM(t^{r_1}, \dots, t^{r_{n'}})$ є саме n ненульових елементів, які знаходяться в позиції i, j (i -й рядок, j -й стовпець), де $i \equiv j + 1 \pmod{n'}$. Нехай $\delta_{n'}(i) = (i - 1) \bmod n' + 1$ або, що рівнозначно, $\delta_{n'}(i) \equiv i \pmod{n'}$, $1 \leq \delta_{n'}(i) \leq n'$. Таким чином $M(t^{l_1}, \dots, t^{l_n})S = SM(t^{r_1}, \dots, t^{r_{n'}})$ тоді і тільки тоді, коли скалярні рівності

$$\begin{cases} (i + 1, \delta_{n'}(i)) : \lambda^{l_i} \lambda^{s_i} = \lambda^{s_{i+1}} \lambda^{r_{\delta_{n'}(i)}} & (i = 1, \dots, n - 1), \\ (1, n') : \lambda^{l_n} \lambda^{s_n} = \lambda^{s_1} \lambda^{r_{n'}}; \end{cases}$$

виконуються. Очевидно, ці рівності еквівалентні рівностям

$$\begin{cases} (i + 1, \delta_{n'}(i)) : l_i + s_i = s_{i+1} + r_{\delta_{n'}(i)} & (i = 1, \dots, n - 1), \\ (1, n') : l_n + s_n = s_1 + r_{n'}. \end{cases} \quad (3.1)$$

Необхідність. Припустимо, що для деяких $s_i \geq 0$, $i = 1, \dots, n$ $M(t^{l_1}, \dots, t^{l_n})S = SM(t^{r_1}, \dots, t^{r_{n'}})$. Тоді система (3.1) виконується. Додамо всі рівності (3.1).

$$\sum_{i=1}^{n-1} l_i + \sum_{i=1}^{n-1} s_i + l_n + s_n = \sum_{i=1}^{n-1} s_{i+1} + \sum_{i=1}^{n-1} r_{\delta_{n'}(i)} + s_1 + r_{n'}.$$

Але оскільки $\delta_{n'}(n) = n'$ ми маємо

$$\sum_{i=1}^n l_i + \sum_{i=1}^n s_i = \sum_{i=1}^n s_i + \sum_{i=1}^n r_{\delta_{n'}(i)}$$

або $\sum_{i=1}^n l_i = \sum_{i=1}^n r_{\delta_{n'}(i)}$. Ця рівність еквівалентна рівності $\sum_{i=1}^n l_i = \frac{n}{n'} \sum_{i=1}^{n'} r_i$ або $\frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}$.

Достатність. Припустимо тепер, що $\frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}$. Доведемо, що $M(t^{l_1}, \dots, t^{l_n})S = SM(t^{r_1}, \dots, t^{r_{n'}})$ для деяких $s_i \geq 0$ ($i = 1, \dots, n$). Достатньо довести, що деякі $s_i \geq 0$ ($i = 1, \dots, n$) задовольняють систему (3.1). Ця система має розв'язок відносно s_i в невід'ємних цілих числах тоді і тільки тоді, коли ця система має розв'язок у довільних цілих числах, бо додавання до всіх s_i , що утворюють розв'язок, сталого числа залишає їх розв'язком. Нехай $s_1 = 0$, $s_{i+1} = l_i + s_i - r_{\delta_{n'}(i)}$ ($i = 1, \dots, n-1$). Звідси випливає, що всі рівності, за винятком можливо останньої рівності, системи (3.1) виконуються. Крім того, індукцією за j легко показати, що $s_j = \sum_{i=1}^{j-1} l_i - \sum_{i=1}^{j-1} r_{\delta_{n'}(i)}$. Тоді $s_n = \sum_{i=1}^{n-1} l_i - \sum_{i=1}^{n-1} r_{\delta_{n'}(i)}$. Нарешті останнє рівняння системи (3.1) після заміни s_n на $\sum_{i=1}^{n-1} l_i - \sum_{i=1}^{n-1} r_{\delta_{n'}(i)}$ і s_1 на 0 набуває вигляду

$$l_n + \sum_{i=1}^{n-1} l_i - \sum_{i=1}^{n-1} r_{\delta_{n'}(i)} = r_{n'}$$

або

$$l_n + \sum_{i=1}^{n-1} l_i = \sum_{i=1}^{n-1} r_{\delta_{n'}(i)} + r_{n'}.$$

Тобто, $\sum_{i=1}^n l_i = \sum_{i=1}^n r_{\delta_{n'}(i)}$ або $\sum_{i=1}^n l_i = \frac{n}{n'} \sum_{i=1}^{n'} r_i$. Це еквівалентно $\frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}$ і остання рівність справедлива за припущенням достатності, тому остання рівність системи (3.1) також має місце. $\square$

Теорема 3.2. Нехай n — натуральне число, $l_i \geq 0$ ($i = 1, \dots, n$), $(\sum_{i=1}^n l_i, n) > 1$. Тоді для будь-якого дільника $d > 1$ числа $(\sum_{i=1}^n l_i, n)$ мат-

риця $M(t^{l_1}, \dots, t^{l_n}) \in M(n, \mathbb{Z}[\lambda])$ подібна до матриці наступної форми

$$\begin{pmatrix} M(t^{r_1}, \dots, t^{r_{n'}}) & B \\ 0 & A \end{pmatrix} \in M(n, \mathbb{Z}[\lambda]),$$

для деяких $r_i \geq 0$ ($i = 1, \dots, n'$), таких, що

$$d = \frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}.$$

Доведення. Очевидно для $n' = \frac{n}{d}$ та деяких $r_i \geq 0$ ($i = 1, \dots, n'$)

$$d = \frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}.$$

В ролі $r_1, r_2, \dots, r_{n'}$ завжди можна вибрати, наприклад, $0, \dots, 0, \frac{\sum_{i=1}^n l_i}{d}$. За твердженням 3.1 існує $n \times n'$ -матриця

$$S = \begin{pmatrix} \lambda^{s_1} & 0 & \dots & 0 \\ 0 & \lambda^{s_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_{n'}} \\ \lambda^{s_{n'+1}} & 0 & \dots & 0 \\ 0 & \lambda^{s_{n'+2}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_{2n'}} \\ \dots & \dots & \dots & \dots \\ \lambda^{s_{n-n'+1}} & 0 & \dots & 0 \\ 0 & \lambda^{s_{n-n'+2}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_n} \end{pmatrix},$$

де $s_i \geq 0$ ($i = 1, \dots, n$), така, що

$$M(t^{l_1}, \dots, t^{l_n})S = SM(t^{r_1}, \dots, t^{r_{n'}}). \quad (3.2)$$

Зануримо область цілісності $\mathbb{Z}[\lambda]$ у своє поле відношень F . Очевидно для деякої діагональної матриці $D = \text{diag}(t^{-d_1}, \dots, t^{-d_{n'}})$ над полем F , де $d_i \geq 0$ ($i = 1, \dots, n'$), кожен стовпчик матриці $S' = SD$ містить принаймні одну одиницю. Крім того, ненульові елементи матриць $S' = SD$ та S займають одні і ті ж n позиції в обох матрицях. Однак ненульові елементи з різних стовпців матриці S займають різні рядки, тому n' одиниць з n' різних стовпчиків матриці S' займають n' різних рядків тої ж матриці, тому S' займає перші n' стовпчиків деякої оборотної матриці C над кільцем $\mathbb{Z}[\lambda]$. Крім того, з (3.2)

$$M(t^{l_1}, \dots, t^{l_n})SD = SDD^{-1}M(t^{r_1}, \dots, t^{r_{n'}})D$$

або

$$M(t^{l_1}, \dots, t^{l_n})S' = S' \text{diag}(t^{d_1}, \dots, t^{d_{n'}})M(t^{r_1}, \dots, t^{r_{n'}}) \text{diag}(t^{-d_1}, \dots, t^{-d_{n'}}).$$

Домноження зліва чи справа на діагональну матрицю з ненульовими діагональними елементами не змінює кількість і положення ненульових елементів деякої матриці, які (ненульові елементи) у результаті множення одержують, як множники, діагональні елементи діагональної матриці. Тому ненульові елементи S' залишаються степенями t ,

$$M' = \text{diag}(t^{d_1}, \dots, t^{d_{n'}})M(t^{r_1}, \dots, t^{r_{n'}}) \text{diag}(t^{-d_1}, \dots, t^{-d_{n'}}) = M(t^{r'_1}, \dots, t^{r'_{n'}})$$

для деяких цілих r'_i ($i = 1, \dots, n'$). Отже,

$$M(t^{l_1}, \dots, t^{l_n})S' = S'M(t^{r'_1}, \dots, t^{r'_{n'}}). \quad (3.3)$$

Однак S' займає перші n' стовпчиків оборотної матриці C над кільцем $\mathbb{Z}[\lambda]$. Тобто $C = (S' T)$ для деякої $n \times (n - n')$ -матриці T над кільцем $\mathbb{Z}[\lambda]$ і $MC = (MS' MT)$ для довільної квадратної матриці M над кільцем $\mathbb{Z}[\lambda]$. Тоді

$$C^{-1}M(t^{l_1}, \dots, t^{l_n})C = C^{-1}M(t^{l_1}, \dots, t^{l_n})(S' T) =$$

$$\begin{aligned}
& C^{-1}(M(t^{l_1}, \dots, t^{l_n})S' M(t^{l_1}, \dots, t^{l_n})T) = \\
& C^{-1}(S' M(t^{r'_1}, \dots, t^{r'_{n'}}) M(t^{l_1}, \dots, t^{l_n})T) = \\
& C^{-1} \left((S' T) \begin{pmatrix} M(t^{r'_1}, \dots, t^{r'_{n'}}) \\ 0 \end{pmatrix} M(t^{l_1}, \dots, t^{l_n})T \right) = \\
& C^{-1} \left(C \begin{pmatrix} M(t^{r'_1}, \dots, t^{r'_{n'}}) \\ 0 \end{pmatrix} M(t^{l_1}, \dots, t^{l_n})T \right) = \\
& \left(\begin{pmatrix} M(t^{r'_1}, \dots, t^{r'_{n'}}) \\ 0 \end{pmatrix} C M(t^{l_1}, \dots, t^{l_n})T \right).
\end{aligned}$$

Тобто $C^{-1}M(t^{l_1}, \dots, t^{l_n})C$ має вигляд

$$\begin{pmatrix} M(t^{r'_1}, \dots, t^{r'_{n'}}) & B \\ 0 & A \end{pmatrix},$$

для деяких матриць A та B відповідних розмірів над кільцем $\mathbb{Z}[\lambda]$. Оскільки $C^{-1}M(t^{l_1}, \dots, t^{l_n})C \in \mathbb{Z}[\lambda]$, то $r'_i \geq 0$ ($i = 1, \dots, n'$). За твердженням 3.1 та рівністю (3.3)

$$d = \frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}.$$

□

Вперше теорему 3.2 у вужчому формулюванні було доведено М. Ю. Бортош [17, 106]. Доведення було реалізовано в термінах лінійного оператора скінченно вимірного лінійного простору визначеного λ -циклічною матрицею над полем відношень кільця цілочислових многочленів від невідомої λ . В підрозділі було отримане альтернативне доведення теореми 3.2 матричним численням, що не спирається на аналіз лінійного оператора скінченно вимірного лінійного простору над полем,

яке буде також застосоване до питання про спадкову звідність біноміальних матриць у підрозділі 3.3. З теореми 3.2 та існування гомоморфізма кілець $f : \mathbb{Z}[\lambda] \rightarrow K$, який визначається рівностями: $f(1) = 1$ і $f(\lambda) = t$ відразу впливає теорема 3.3.

Теорема 3.3 ([17, 106]). *Нехай K — комутативне кільце, $t \in K$. t -циклічна матриця $M(t^{s_1}, \dots, t^{s_n})$, де $s_i \geq 0$ ($i = 1, \dots, n$), є спадковою звідною, якщо $\sum_{i=1}^n s_i$ і n не є взаємно простими.*

3.3. Спадкова звідність біноміальних матриць

Нехай K — комутативне кільце з одиницею, $t \in K$. Квадратна матриця порядку n над кільцем K називається *біноміальною відносно t* , якщо вона переставно подібна матриці вигляду:

$$M(t, k, n) = \begin{pmatrix} \overbrace{0 \dots 0}^k & 0 & 0 & \dots & 0 & t \\ 1 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & t & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & t & 0 \end{pmatrix}, \quad (3.4)$$

де $0 < k < n$. Кажуть, що така матриця $M = M(t, k, n)$ є *спадковою звідною*, якщо вона подібна до матриці

$$M' = \begin{pmatrix} M(t, k', n') & * \\ 0 & N \end{pmatrix}, \quad n' \neq n,$$

де $0 \leq k' \leq n'$ і *спадково незвідна* в іншому випадку.

$l_n = 1$ і $r_1 = \dots = r_{k'} = 0$, $r_{k'+1} = \dots = r_{n'} = 1$ так, щоб

$$M(\lambda, k, n) = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{l_n} \\ \lambda^{l_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{l_k} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{l_{k+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{l_{n-1}} & 0 \end{pmatrix} = M(t^{l_1}, \dots, t^{l_n}),$$

$$M(\lambda, k', n') = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{r_{n'}} \\ \lambda^{r_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{r_{k'}} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{r_{k'+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{r_{n'-1}} & 0 \end{pmatrix} = M(t^{r_1}, \dots, t^{r_{n'}}).$$

Зрозуміло, що $\sum_{i=1}^n l_i = k$, $\sum_{i=1}^{n'} r_i = k'$ а рівність

$$M(\lambda, k, n)S = SM(\lambda, k', n')$$

те ж, що й

$$M(t^{l_1}, \dots, t^{l_n})S = SM(t^{r_1}, \dots, t^{r_{n'}}).$$

За твердженням 3.1 остання рівність виконується для деяких $s_i \geq 0$ ($i = 1, \dots, n$) тоді і тільки тоді, коли

$$\frac{n}{n'} = \frac{\sum_{i=1}^n l_i}{\sum_{i=1}^{n'} r_i}.$$

Тобто,

$$\frac{n}{n'} = \frac{k}{k'}.$$

де $s_i \geq 0$ ($i = 1, \dots, n$), така, що $MS = SM(\lambda, k', n')$ тоді і тільки тоді, коли $\frac{n}{n'} = \frac{k}{k'}$.

Твердження 3.6. Нехай $n'|n$, $\frac{n}{n'} = \frac{k}{k'}$. Тоді $k' < k$ і $M(\lambda, k, n)$ подібна (над $\mathbb{Z}[\lambda]$) до матриці форми

$$M = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{l_n} \\ \lambda^{l_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{l_{k'}} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{l_{k'+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{l_{n-1}} & 0 \end{pmatrix},$$

де $l_1 = \dots = l_{k'} = 0$, $l_{k'+1} = \dots = l_{k'+n-k} = 1$, $l_{k'+n-k+1} = \dots = l_n = 0$.

Доведення. Оскільки $\frac{k}{k'} = \frac{n}{n'} > 1$, то $k' < k$. Для доведення подібності матриці $M(\lambda, k, n)$ до вказаної достатньо розташуємо рядки та стовпці матриці $M(\lambda, k, n)$ у порядку $k - k' + 1, k - k' + 2, \dots, n, 1, 2, \dots, k - k'$. В результаті отримаємо подібну до матриці $M(\lambda, k, n)$ матрицю M :

$$M = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{l_n} \\ \lambda^{l_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{l_{k'}} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{l_{k'+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{l_{n-1}} & 0 \end{pmatrix},$$

де $l_1 = \dots = l_{k'} = 0$, $l_{k'+1} = \dots = l_{k'+n-k} = 1$, $l_{k'+n-k+1} = \dots = l_n = 0$. $\square$

Твердження 3.7. Нехай $n'|n$, $k' < k$.

$$M = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{l_n} \\ \lambda^{l_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{l_{k'}} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{l_{k'+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{l_{n-1}} & 0 \end{pmatrix},$$

де $l_1 = \dots = l_{k'} = 0$, $l_{k'+1} = \dots = l_{k'+n-k} = 1$, $l_{k'+n-k+1} = \dots = l_n = 0$.

Тоді існує $n \times n'$ -матриця

$$S = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & 0 \\ 0 & \lambda^{s_{n'+2}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_{2n'}} \\ \dots & \dots & \dots & \dots \\ \lambda^{s_{n-n'+1}} & 0 & \dots & 0 \\ 0 & \lambda^{s_{n-n'+2}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{s_n} \end{pmatrix},$$

де $s_i \geq 0$, $(i = n' + 1, \dots, n)$, така, що $MS = SM(\lambda, k', n')$ тоді і тільки тоді, коли $\frac{n}{n'} = \frac{k}{k'}$.

Доведення. Необхідність випливає із твердження 3.5.

Достатність. Припустимо, що $\frac{n}{n'} = \frac{k}{k'}$. Позначимо $r_1 = \dots = r_{k'} = 0$, $r_{k'+1} = \dots = r_{n'} = 1$ так щоб

$$M(\lambda, k', n') = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{r_{n'}} \\ \lambda^{r_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{r_{k'}} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{r_{k'+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{r_{n'-1}} & 0 \end{pmatrix}.$$

Доведемо, що для деяких $s_i \geq 0$, $i = n' + 2, \dots, n$ $M(\lambda, k, n)S = SM(\lambda, k', n')$. Залишається довести, що s_i задовольняють систему (3.1), де $s_1 = \dots = s_{k'} = s_{k'+1} = 0$. Покладемо

$$s_1 = 0, \quad s_{i+1} = l_i + s_i - r_{\delta_{n'}(i)} \quad (i = 1, \dots, n-1). \quad (3.5)$$

Тоді всі, крім можливо останнього рівняння, системи (3.1) задовольняються. З доведення лема 3.4 випливає, що і останнє рівняння системи (3.1) теж задовольняється.

Далі з рівності $\frac{n'-k'}{n-k} = \frac{n}{n'} = \frac{k}{k'} > 1$ випливає, що $n' - k' < n - k$ і

$$l_1 = \dots = l_{k'} = 0 = r_1 = \dots = r_{k'},$$

$$l_{k'+1} = \dots = l_{n'} = 1 = r_{k'+1} = \dots = r_{n'}.$$

Тому $l_i = r_i$ ($i = 1, \dots, n'$) і з (3.5) $s_{i+1} = s_i$ ($i = 1, \dots, n'$). Тобто, $s_1 = \dots = s_{n'} = s_{n'+1} = 0$.

Залишається довести, що побудовані $s_i \geq 0$ ($i = n' + 2, \dots, n$). Покладемо $s_{n+1} = s_1$. З (3.5), враховуючи останню рівність $l_n + s_n = s_1 + r_{n'}$

системи (3.1) або $s_{n+1} = l_n + s_n - r_{\delta_{n'}(n)}$, одержуємо $s_1 = s_{n+1} = 0$,

$$s_{i+1} = \sum_{j=1}^i l_j - \sum_{j=1}^i r_{\delta_{n'}(j)} \quad (i = 1, \dots, n). \quad (3.6)$$

Розглядаємо $s(i) = s_i$, як функцію натурального аргументу i ($1 \leq i \leq n+1$). Якщо $1 \leq i \leq n'+1$, то $s(i) = 0$. Тобто $s(i)$ стала. Якщо $n'+1 \leq i < i+1 \leq k' + n - k + 1$, то з (3.6) одержуємо $s(i+1) - s(i) = l_i - r_{\delta_{n'}(i)} = 1 - r_{\delta_{n'}(i)} \geq 0$. Тобто $s(i)$ неспадна і $s(i) \geq s(n'+1) = 0$. Якщо $k' + n - k + 1 \leq i < i+1 \leq n+1$, то з (3.6) одержуємо $s(i+1) - s(i) = l_i - r_{\delta_{n'}(i)} = 0 - r_{\delta_{n'}(i)} \leq 0$. Тобто $s(i)$ не зростає і $s(i) \geq s(n+1) = 0$. Отже, $s_i = s(i) \geq 0$ ($i = n'+2, \dots, n$). $\square$

Теорема 3.8. Нехай n, k — натуральні числа, $n > k$, $(n, k) > 1$. Тоді для будь-якого дільника $d > 1$ числа (n, k) матриця $M(\lambda, k, n) \in M(n, \mathbb{Z}[\lambda])$ подібний до матриці наступної форми

$$\begin{pmatrix} M(\lambda, k', n') & B \\ 0 & A \end{pmatrix} \in M(n, \mathbb{Z}[\lambda]),$$

де $k' = \frac{k}{d}$ і $n' = \frac{n}{d}$.

Доведення. За умовою теореми $0 < k < n$, $\frac{k}{k'} = \frac{n}{n'} = d > 1$ і $0 < n' < n$, $0 < k' < k$. Далі, з твердження 3.6 одразу одержуємо, що $M(\lambda, k, n)$ подібна (над $\mathbb{Z}[\lambda]$) до матриці форми

$$M = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 & \lambda^{l_n} \\ \lambda^{l_1} & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \lambda^{l_{k'}} & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & \lambda^{l_{k'+1}} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & \lambda^{l_{n-1}} & 0 \end{pmatrix},$$

$MS = SM(\lambda, k', n')$. Тобто матриця з перших n' стовпців матриці

$$C^{-1}MC = \begin{pmatrix} E_{n'} & 0 \\ S' & E_{n-n'} \end{pmatrix}^{-1} M \begin{pmatrix} E_{n'} & 0 \\ S' & E_{n-n'} \end{pmatrix} =$$

$$\begin{pmatrix} E_{n'} & 0 \\ -S' & E_{n-n'} \end{pmatrix} M \begin{pmatrix} E_{n'} & 0 \\ S' & E_{n-n'} \end{pmatrix}$$

рівна

$$\begin{pmatrix} E_{n'} & 0 \\ -S' & E_{n-n'} \end{pmatrix} M \begin{pmatrix} E_{n'} \\ S' \end{pmatrix} = \begin{pmatrix} E_{n'} & 0 \\ -S' & E_{n-n'} \end{pmatrix} \begin{pmatrix} E_{n'} \\ S' \end{pmatrix} M(\lambda, k', n') =$$

$$\begin{pmatrix} E_{n'} \\ 0 \end{pmatrix} M(\lambda, k', n') = \begin{pmatrix} M(\lambda, k', n') \\ 0 \end{pmatrix}.$$

Як наслідок отримаємо, що матриця M , а отже, і матриця $M(\lambda, k, n)$ подібна (над $\mathbb{Z}[\lambda]$) до матриці вигляду

$$\begin{pmatrix} M(\lambda, k', n') & B \\ 0 & A \end{pmatrix} \in M(n, \mathbb{Z}[\lambda]).$$

□

Теорема 3.9. *Нехай K — комутативне кільце, $t \in K$. Бімономіальна матриця $M(t, k, n)$ є спадково звідна, якщо k і n не є взаємно простими.*

Доведення. Теорема випливає з теореми 3.8 та існування гомоморфізма кілець $f : \mathbb{Z}[\lambda] \rightarrow K$, який визначається рівностями: $f(1) = 1$ і $f(\lambda) = t$. □

3.4. Незвідність бімономіальних матриць 7-го порядку

Розглядається бімономіальна матриця

$$M(t, k, n) = \begin{pmatrix} \overbrace{0 \dots 0}^k & 0 & 0 & \dots & 0 & t \\ 1 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & t & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & t & 0 \end{pmatrix}, \quad (3.7)$$

де $1 < k < n$ над комутативним локальним кільцем K , радикал Джекобсона якого $\text{Rad } K = tK \neq 0$ ($t \in K$). За теоремою 3.9 для $(n, k) > 1$ матриця $M(t, k, n)$ звідна над кільцем K . В [49] Р. Ф. Цімболинець (Динис) одержала, що для $n < 7$, $(n, k) = 1$ матриця $M(t, k, n)$ — незвідна. Якщо $t^2 = 0$ Р. Ф. Цімболинець (Динис) [49, 106] показала, що матриці $M(t, 3, 7)$, $M(t, 4, 7)$ звідні над кільцем K . Покажемо, що якщо $t^2 \neq 0$, то всі матриці $M(t, k, 7)$ ($0 < k < 7$) незвідні над кільцем K .

Теорема 3.10. *Нехай n і k натуральні числа, $k < n$, K — комутативне локальне кільце, радикал Джекобсона якого $\text{Rad } K = tK \neq 0$ ($t \in K$). Якщо матриця $M(t, k, n)$ подібна (над K) до матриці $N = \begin{pmatrix} D & B \\ 0 & A \end{pmatrix}$, де D — $m \times m$ -матриця ($0 < m < n$), тоді D подібна (над*

$K)$ до

$$\begin{pmatrix} \overbrace{0 \dots 0}^{k'} & td_{1,k'+1} & \dots & td_{1m} \\ 1 & \dots & 0 & td_{2,k'+1} & \dots & td_{2m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & td_{k'+1,k'+1} & \dots & td_{k'+1,m} \\ 0 & \dots & 0 & td_{k'+2,k'+1} & \dots & td_{k'+2,m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & td_{n,k'+1} & \dots & td_{mm} \end{pmatrix} \quad (3.8)$$

для деякого k' ($0 < k' < k$).

Доведення. Якщо матриця $M(t, k, n)$ подібна (над K) до матриці N , тоді над полем K/tK маємо подібність

$$\begin{pmatrix} J_{0,k+1} & 0 \\ 0 & 0 \end{pmatrix} = \overline{M(t, k, n)} \sim \begin{pmatrix} \overline{D} & \overline{B} \\ 0 & \overline{A} \end{pmatrix}, \quad (3.9)$$

де $J(\lambda, r)$ — Жорданова клітка порядку r з власним значенням λ над полем K/tK . Нехай φ — лінійний оператор скінченно вимірного лінійного простору L над полем K/tK з матрицею $\overline{M(t, k, n)}$ в деякому базисі $\{a_1, \dots, a_n\}$. Тоді $\text{Imm}\varphi$ має базис $\{a_2, \dots, a_{k+1}\}$, $\text{Ker}\varphi$ має базис $\{a_{k+1}, \dots, a_n\}$ і $\text{Ker}\varphi \cap \text{Imm}\varphi$ має базис $\{a_{k+1}\}$,

$$\text{Dim}(\text{Ker}\varphi \cap \text{Imm}\varphi) = 1. \quad (3.10)$$

З (3.9) випливає, що φ є лінійний оператор підпростору L' простору L над полем K/tK , що має матрицю $\overline{D}$ в деякому базисі $\{a'_1, \dots, a'_{k'}\}$ підпростору L' . Очевидно, матриця $\overline{M(t, k, n)}$ нільпотентна, оператор φ нільпотентний, і $\overline{D}$ також нільпотентна. Тоді $\overline{D}$ подібна (над полем K/tK) до своєї Жорданової нормальної форми з всіма нульовими влас-

ними значеннями. Тоді можна вважати, що $\overline{D}$ блочно діагональна матриця з Жордановими клітками на головній діагоналі. Якщо $\overline{D}$ має принаймні дві Жорданові клітки порядку більше 1, тоді

$$\overline{D} = \begin{pmatrix} J_{0,k'+1} & 0 & 0 \\ 0 & J_{0,k''+1} & 0 \\ 0 & 0 & * \end{pmatrix}$$

для деяких натуральних чисел k', k'' . Але $a'_{k'+1}, a'_{k'+k''+2} \in \text{Ker}\varphi \cap \text{Imm}\varphi$ і $\text{Dim}(\text{Ker}\varphi \cap \text{Imm}\varphi) \geq 2$, що суперечить (3.10).

З [106, лема 1, ст. 181] випливає, що $\overline{D}$ ненульова матриця і $\overline{D}$ має рівно одну Жорданову клітку порядку вище 1. Можна вважати, що $\overline{D} = \begin{pmatrix} J_{0,k'+1} & 0 \\ 0 & 0 \end{pmatrix}$ для деякого натурального k' . Очевидно, $k' = \text{rank}\overline{D} \leq \text{rank}\overline{M(t,k,n)} = k$. Якщо $k' = k$, тоді $\text{rank}\overline{D} = \text{rank}\overline{M(t,k,n)}$ і з (3.9) $\overline{A} = 0$, що неможливо. Отже, $0 < k' < k$.

Нехай $e_1, \dots, e_m$ — відповідні стовпчики одиничної матриці E_m . $e'_1 = e_1$, $e'_2 = De'_1$, $\dots$, $e'_{k'+1} = De'_{k'}$, $e'_{k'+2} = e_{k'+2}$, $\dots$, $e'_m = e_m$. Але $\overline{e'_2} = \overline{De'_1} = \overline{e_2}$, $\dots$, $\overline{e'_{k'+1}} = \overline{De'_{k'}} = \overline{e_{k'+1}}$. Отже, $\overline{e'_1} = \overline{e_1}$, $\dots$, $\overline{e'_m} = \overline{e_m}$ і $\det(e'_1 \dots e'_m) = \det(e_1 \dots e_m) = \det E_m = 1$. Оскільки кільце K локальне, то матриця $C = (e'_1 \dots e'_m)$ має оборотний детермінант і C оборотна над K .

Розглянемо

$$\begin{aligned} D' &= C^{-1}DC = C^{-1}D \times (e'_1 \dots e'_m) = C^{-1}(De'_1 \dots De'_m) = \\ &= C^{-1}(e'_2 \dots e'_{k'+1} De'_{k'+1} \dots De'_m) = \\ &= (C^{-1}e'_2 \dots C^{-1}e'_{k'+1} C^{-1}De'_{k'+1} \dots C^{-1}De'_m) = \\ &= (e_2 \dots e_{k'+1} C^{-1}De'_{k'+1} \dots C^{-1}De'_m). \end{aligned}$$

Очевидно, $\overline{C} = \overline{E_m}$ і $\overline{D'} = \overline{C^{-1}DC} = \overline{D} = (\overline{e_2} \dots \overline{e_{k'+1}} 0 \dots 0)$. Тоді D подібна до D' , що має форму (3.8). $\square$

Наслідок 3.11. Нехай n і k натуральні числа, $k < n$, K — комутативне локальне кільце, радикал Джексона якого $tK \neq 0$ ($t \in K$). Якщо матриця $M(t, k, n)$ звідна над K , тоді $M(t, k, n)$ подібна (над K) до матриці

$$\begin{pmatrix} D & B \\ 0 & A \end{pmatrix},$$

де D — $m \times m$ -матриця ($2 \leq m \leq \frac{n}{2}$).

Доведення. Із звідності над K матриці $M(t, k, n)$ одержимо, що матриця $M(t, k, n)$ подібна (над K) до матриці

$$N = \begin{pmatrix} D & B \\ 0 & A \end{pmatrix},$$

де D — $m \times m$ -матриця ($0 < m < n$). Очевидно, матриця

$$M(t, k, n)^T = \begin{pmatrix} 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & t & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & t \\ t & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

записом стовпців та відповідно рядків у зворотному порядку зводиться

до вигляду

$$\left(\begin{array}{ccc|ccc} & & & \overbrace{0 \dots 0}^k & & & \\ 0 & \dots & 0 & 0 & \dots & 0 & t \\ t & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline 0 & \dots & t & 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 1 & 0 \end{array} \right).$$

Перемістивши перші $n - k - 1$ стовпців без зміни їх взаємного положення та взаємного положення решти на останні положення і таким же переміщенням рядків отримаємо матрицю

$$\left(\begin{array}{cccccc|cc} & & & \overbrace{0 \dots 0}^k & & & & \\ 0 & \dots & 0 & 0 & \dots & 0 & t & \\ 1 & \dots & 0 & 0 & \dots & 0 & 0 & \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \\ 0 & \dots & 1 & 0 & \dots & 0 & 0 & \\ 0 & \dots & 0 & t & \dots & 0 & 0 & \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \\ 0 & \dots & 0 & 0 & \dots & t & 0 & \end{array} \right) = M(t, k, n).$$

Тобто $M(t, k, n)^T$ переставно подібна до $M(t, k, n)$. Але маємо також подібність

$$N^T = \begin{pmatrix} D^T & 0 \\ B^T & A^T \end{pmatrix} \sim \begin{pmatrix} A^T & B^T \\ 0 & D^T \end{pmatrix}.$$

Тобто, можна вважати, що $m \leq n - m$ або $m \leq \frac{n}{2}$. За теоремою 3.10 для деякого натурального числа k' $k' + 1 \leq m$. Тоді $2 \leq m$. $\square$

Нехай далі K — комутативне локальне кільце, радикал Джекобсона якого tK ($t \in K$, $t^2 \neq 0$). Покажемо незвідність матриць $M(t, k, 7)$ ($k = 1, \dots, 6$). Для $k = 1, 6$ незвідність $M(t, k, 7)$ слідує з теореми 1.11.

Лема 3.12. *Матриця $M(t, k, 7)$ ($1 < k < 6$) не є подібна над K до матриці вигляду*

$$N = \left(\begin{array}{cc|c} 0 & td_{12} & B \\ 1 & td_{22} & \\ \hline & 0 & A \end{array} \right).$$

Доведення. Якщо $d_{12} \in tK$, то $d_{12} = td'_{12}$ ($d'_{12} \in K$) і маємо подібність над K

$$\begin{pmatrix} 0 & td_{12} \\ 1 & td_{22} \end{pmatrix} \sim \begin{pmatrix} 1 & -td_{22} \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & t^2 d'_{12} \\ 1 & td_{22} \end{pmatrix} \begin{pmatrix} 1 & -td_{22} \\ 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & td_{22} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & t^2 d'_{12} \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} td_{22} & t^2 d'_{12} \\ 1 & 0 \end{pmatrix}.$$

Тоді над кільцем K/t^2K матриця $M(t, k, 7)$ подібна матриці з нульовим стовпчиком, який зміною порядку стовпчиків і відповідною зміною порядку рядків можна змістити на перше положення. Це означає, що над комутативним локальним кільцем K/t^2K , радикал Джекобсона якого $\text{Rad}(K/t^2K) = tK/t^2K \neq 0$ матриця $M(t, k, 7)$ після редукції за модулем t^2K звідна і в зведеному вигляді перший її квадратний діагональний блок розміру 1×1 рівний нулю і безперечно конгруентний нулю за модулем tK/t^2K , що суперечить теоремі 3.10.

Нехай тепер $d_{12} \in K^*$ і для деякої оборотної матриці $C = (c_{ij})$ порядку 7 над K

$$M(t, k, 7)C = CN. \quad (3.11)$$

Очевидно K/t^3K — комутативне локальне кільце, радикал Джекобсона якого $\text{Rad}(K/t^3K) = tK/t^3K$, $t^2 \notin t^3K$ а матриця незвідна після редукції за модулем t^3K є також незвідна над кільцем K . Тому для спрощення викладок, без втрати загальності, можна вважати, що $t^3 = 0$. Враховуючи, що $t^2 \neq 0$, дістанемо

$$\text{Ann } t = t^2K, \text{ Ann } t^2 = tK.$$

Позначимо через $(3.11)_{[i,j]}$ скалярну рівність $(M(t, 2, 7)C)_{ij} = (CN)_{ij}$. Тоді

$$\begin{aligned} (3.11)_{[1,1]} : \quad & tc_{71} = c_{12}, \\ (3.11)_{[2,1]} : \quad & c_{11} = c_{22}, \\ & \dots\dots\dots \\ (3.11)_{[k+1,1]} : \quad & c_{k1} = c_{k+1,2}, \\ (3.11)_{[k+2,1]} : \quad & tc_{k+1,1} = c_{k+2,2}, \\ & \dots\dots\dots \\ (3.11)_{[7,1]} : \quad & tc_{61} = c_{72}. \end{aligned}$$

Оскільки $t \in \text{Rad } K$, то $\bar{t} = 0$, $\overline{c_{12}} = \overline{c_{k+2,2}} = \dots = \overline{c_{72}} = 0$. Крім того,

$$\begin{aligned} (3.11)_{[1,2]} : \quad & tc_{72} = tc_{11}d_{12} + tc_{12}d_{22}, \\ (3.11)_{[2,2]} : \quad & c_{12} = tc_{21}d_{12} + tc_{22}d_{22}, \\ & \dots\dots\dots \\ (3.11)_{[k+1,2]} : \quad & c_{k2} = tc_{k+1,1}d_{12} + tc_{k+1,2}d_{22}, \\ (3.11)_{[k+2,2]} : \quad & tc_{k+1,2} = tc_{k+2,1}d_{12} + tc_{k+2,2}d_{22}, \\ & \dots\dots\dots \\ (3.11)_{[7,2]} : \quad & tc_{62} = tc_{71}d_{12} + tc_{72}d_{22}. \end{aligned}$$

Таким чином $\overline{c_{12}} = \dots = \overline{c_{k2}} = \overline{c_{k+2,2}} = \dots = \overline{c_{72}} = 0$. В силу оборотності детермінанта матриці $\overline{C}$ $c_{k+1,2} = c_{k1} \in K^*$.

Підставляючи $(3.11)_{[i,1]}$ у $(3.11)_{[i,2]}$ при $k = 2$ одержимо:

$$\left\{ \begin{array}{l} c_{11} = tc_{31}d_{12} + tc_{21}d_{22}, \\ tc_{21} = tc_{41}d_{12} + t^2c_{31}d_{22}, \\ t^2c_{31} = tc_{51}d_{12} + t^2c_{41}d_{22}, \\ t^2c_{41} = tc_{61}d_{12} + t^2c_{51}d_{22}, \\ t^2c_{51} = tc_{71}d_{12} + t^2c_{61}d_{22}, \\ t^2c_{61} = tc_{11}d_{12} + t^2c_{71}d_{22}, \\ tc_{71} = tc_{21}d_{12} + tc_{11}d_{22}. \end{array} \right.$$

З 1-го рівняння $c_{11} = tc_{31}d_{12} + tc_{21}d_{22}$, з останнього рівняння $t(c_{71} - c_{21}d_{12} - c_{11}d_{22}) = 0$. Звідси $c_{71} - c_{21}d_{12} - c_{11}d_{22} \in \text{Ann } t = t^2K$. Отже, $c_{71} - c_{21}d_{12} - c_{11}d_{22} = t^2c'_{71}$ ($c'_{71} \in K$) і $c_{71} = c_{21}d_{12} + c_{11}d_{22} + t^2c'_{71}$. Після підстановки отримаємо систему

$$\left\{ \begin{array}{l} tc_{21} = tc_{41}d_{12} + t^2c_{31}d_{22}, \\ t^2c_{31} = tc_{51}d_{12} + t^2c_{41}d_{22}, \\ t^2c_{41} = tc_{61}d_{12} + t^2c_{51}d_{22}, \\ t^2c_{51} = tc_{21}d_{12}^2 + t^2c_{61}d_{22} + t^2c_{31}d_{12}^2d_{22} + t^2c_{21}d_{12}d_{22}^2, \\ t^2c_{61} = t^2c_{31}d_{12}^2 + 2t^2c_{21}d_{12}d_{22}. \end{array} \right.$$

З 4-го рівняння оскільки $t \neq 0$ одержуємо $c_{21}d_{12}^2 \in tK$, що неможливо, бо $c_{21} = c_{k1} \in R^*$, $d_{12} \in K^*$.

Підставляючи (3.11)_[i,1] у (3.11)_[i,2] при $k = 3$ одержимо:

$$\left\{ \begin{array}{l} c_{11} = tc_{31}d_{12} + tc_{21}d_{22}, \\ c_{21} = tc_{41}d_{12} + tc_{31}d_{22}, \\ tc_{31} = tc_{51}d_{12} + t^2c_{41}d_{22}, \\ t^2c_{41} = tc_{61}d_{12} + t^2c_{51}d_{22}, \\ t^2c_{51} = tc_{71}d_{12} + t^2c_{61}d_{22}, \\ t^2c_{61} = tc_{11}d_{12} + t^2c_{71}d_{22}, \\ tc_{71} = tc_{21}d_{12} + tc_{11}d_{22}. \end{array} \right.$$

З 1-го та 2-го рівняння відповідно маємо: $c_{11} = tc_{31}d_{12} + tc_{21}d_{22}$, $c_{21} = tc_{41}d_{12} + tc_{31}d_{22}$, з останнього рівняння, оскільки $\text{Ann } t = t^2K$, дістанемо $c_{71} = c_{21}d_{12} + c_{11}d_{22} + t^2c'_{71}$ ($c'_{71} \in K$) і так само з 4-го рівняння оскільки $d_{12} \in K^*$ $c_{61} = tc_{41}d_{12}^{-1} - tc_{51}d_{12}^{-1}d_{22} + t^2c'_{61}$ ($c'_{61} \in K$). Після підстановки одержимо:

$$\begin{cases} 0 = t^2c_{31}d_{12}^2, \\ tc_{31} = tc_{51}d_{12} + t^2c_{41}d_{22}, \\ t^2c_{51} = t^2c_{41}d_{12}^3 + 2t^2c_{31}d_{12}^2d_{22}. \end{cases}$$

З 1-го рівняння оскільки $\text{Ann } t^2 = tK$ одержуємо $c_{31}d_{12}^2 \in tK$, що неможливо, бо $c_{31} = c_{k1} \in R^*$, $d_{12} \in K^*$.

Підставляючи $(3.11)_{[i,1]}$ у $(3.11)_{[i,2]}$ при $k = 4$ одержимо:

$$\begin{cases} c_{11} = tc_{31}d_{12} + tc_{21}d_{22}, \\ c_{21} = tc_{41}d_{12} + tc_{31}d_{22}, \\ c_{31} = tc_{51}d_{12} + tc_{41}d_{22}, \\ tc_{41} = tc_{61}d_{12} + t^2c_{51}d_{22}, \\ t^2c_{51} = tc_{71}d_{12} + t^2c_{61}d_{22}, \\ t^2c_{61} = tc_{11}d_{12} + t^2c_{71}d_{22}, \\ tc_{71} = tc_{21}d_{12} + tc_{11}d_{22}. \end{cases}$$

З 1-го, 2-го та 3-го рівняння відповідно маємо: $c_{11} = tc_{31}d_{12} + tc_{21}d_{22}$, $c_{21} = tc_{41}d_{12} + tc_{31}d_{22}$, $c_{31} = tc_{51}d_{12} + tc_{41}d_{22}$, з останнього рівняння, оскільки $\text{Ann } t = t^2K$, одержимо $c_{71} = c_{21}d_{12} + c_{11}d_{22} + t^2c'_{71}$ ($c'_{71} \in K$). Після підстановки отримаємо:

$$\begin{cases} tc_{41} = tc_{61}d_{12} + t^2c_{51}d_{22}, \\ t^2c_{51} = t^2c_{41}d_{12}^3 + t^2c_{61}d_{22}, \\ t^2c_{61} = 0. \end{cases}$$

З 3-го рівняння оскільки $\text{Ann } t^2 = tK$ одержуємо $c_{61} \in tK$, з 1-го рівняння, оскільки $c_{61} \in tK$, одержуємо $tc_{41} \in t^2K$. Тобто $c_{41} \in tK$, що

неможливо, бо $c_{41} = c_{k1} \in K^*$.

Підставляючи (3.11)_[i,1] у (3.11)_[i,1] при $k = 5$ одержимо:

$$\left\{ \begin{array}{l} c_{11} = tc_{31}d_{12} + tc_{21}d_{22}, \\ c_{21} = tc_{41}d_{12} + tc_{31}d_{22}, \\ c_{31} = tc_{51}d_{12} + tc_{41}d_{22}, \\ c_{41} = tc_{61}d_{12} + tc_{51}d_{22}, \\ tc_{51} = tc_{71}d_{12} + t^2c_{61}d_{22}, \\ t^2c_{61} = tc_{11}d_{12} + t^2c_{71}d_{22}, \\ tc_{71} = tc_{21}d_{12} + tc_{11}d_{22} \end{array} \right.$$

З 1-го, 2-го, 3-го та 4-го рівняння відповідно маємо: $c_{11} = tc_{31}d_{12} + tc_{21}d_{22}$, $c_{21} = tc_{41}d_{12} + tc_{31}d_{22}$, $c_{31} = tc_{51}d_{12} + tc_{41}d_{22}$, $c_{41} = tc_{61}d_{12} + tc_{51}d_{22}$, з останнього рівняння, оскільки $\text{Ann } t = t^2K$, маємо $c_{71} = c_{21}d_{12} + c_{11}d_{22} + t^2c'_{71}$ ($c'_{71} \in K$). Після підстановки отримаємо систему

$$\left\{ \begin{array}{l} tc_{5,1} = t^2c_{6,1}d_{2,2} \\ t^2c_{6,1} = 0 \end{array} \right.$$

З 1-го рівняння одержуємо $tc_{51} \in t^2K$. Тобто $c_{51} \in tK$, що неможливо, бо $c_{51} = c_{k1} \in K^*$. $\square$

Лема 3.13. Матриця $M(t, k, 7)$ ($1 < k < 6$) не є подібна над K до матриці вигляду

$$N = \left(\begin{array}{ccc|c} 0 & 0 & td_{13} & \\ 1 & 0 & td_{23} & B \\ 0 & 1 & td_{33} & \\ \hline & 0 & & A \end{array} \right)$$

для жодних $d_{13}, d_{23}, d_{33} \in K$.

Доведення. Якщо $d_{13} \in tK$, то $d_{13} = td'_{13}$ ($d'_{13} \in K$) і маємо подібність

над K

$$\begin{pmatrix} 0 & 0 & td_{13} \\ 1 & 0 & td_{23} \\ 0 & 1 & td_{33} \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -td_{33} \\ 0 & 0 & td_{33} \end{pmatrix}^{-1} \begin{pmatrix} 0 & 0 & t^2 d'_{13} \\ 1 & 0 & td_{23} \\ 0 & 1 & td_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -td_{33} \\ 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & td_{33} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & t^2 d'_{13} \\ 1 & 0 & td_{23} \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & t^2 d'_{13} \\ 1 & td_{33} & td_{23} \\ 0 & 1 & 0 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 0 & -td_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 0 & t^2 d'_{13} \\ 1 & td_{33} & td_{23} \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -td_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & td_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & t^2 d'_{13} \\ 1 & td_{33} & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & td_{23} & t^2 d'_{13} \\ 1 & td_{33} & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Тоді над кільцем $K/t^2 K$ матриця $M(t, k, 7)$, після редукції за модулем $t^2 K$, подібна матриці з нульовим стовпчиком. Тоді маємо протиріччя з теоремою 3.10. Отже, $d_{13} \in K^*$.

Нехай для деякої оборотної матриці $C = (c_{ij})$ порядку 7 над K

$$M(t, k, 7)C = CN. \quad (3.12)$$

Для спрощення викладок знову вважаємо, що $t^3 = 0$. Тоді:

$$\begin{aligned}
 (3.12)_{[1,1]} : \quad & tc_{71} = c_{12}, \\
 (3.12)_{[2,1]} : \quad & c_{11} = c_{22}, \\
 & \dots\dots\dots \\
 (3.12)_{[k,1]} : \quad & c_{k-1,1} = c_{k,2}, \\
 (3.12)_{[k+1,1]} : \quad & c_{k,1} = c_{k+1,2}, \\
 (3.12)_{[k+2,1]} : \quad & tc_{k+1,1} = c_{k+2,2}, \\
 & \dots\dots\dots \\
 (3.12)_{[7,1]} : \quad & tc_{61} = c_{72}, \\
 (3.12)_{[1,2]} : \quad & tc_{72} = c_{13}, \\
 (3.12)_{[2,2]} : \quad & c_{12} = c_{23}, \\
 & \dots\dots\dots \\
 (3.12)_{[k+1,2]} : \quad & c_{k2} = c_{k+1,3}, \\
 (3.12)_{[k+2,2]} : \quad & tc_{k+1,2} = c_{k+2,3}, \\
 & \dots\dots\dots \\
 (3.12)_{[7,2]} : \quad & tc_{62} = c_{73}.
 \end{aligned}$$

Таким чином $\overline{c_{13}} = \overline{c_{k+2,3}} = \dots = \overline{c_{73}} = 0$.

$$\begin{aligned}
 (3.12)_{[1,3]} : \quad & tc_{73} = tc_{11}d_{13} + tc_{12}d_{23} + tc_{13}d_{33}, \\
 (3.12)_{[2,3]} : \quad & c_{13} = tc_{21}d_{13} + tc_{22}d_{23} + tc_{23}d_{33}, \\
 & \dots\dots\dots \\
 (3.12)_{[k+1,3]} : \quad & c_{k3} = tc_{k+1,1}d_{13} + tc_{k+1,2}d_{23} + tc_{k+1,3}d_{33}, \\
 (3.12)_{[k+2,3]} : \quad & tc_{k+1,3} = tc_{k+2,1}d_{13} + tc_{k+2,2}d_{23} + tc_{k+2,3}d_{33}, \\
 & \dots\dots\dots \\
 (3.12)_{[7,3]} : \quad & tc_{63} = tc_{71}d_{13} + tc_{72}d_{23} + tc_{73}d_{33}.
 \end{aligned}$$

Таким чином $\overline{c_{13}} = \dots = \overline{c_{k3}} = \overline{c_{k+2,3}} = \dots = \overline{c_{73}} = 0$. В силу оборотності детермінанта матриці $\overline{C}$ $c_{k+1,3} = c_{k2} = c_{k-1,1} \in K^*$.

Підставляючи $(3.12)_{[i,1]}$ у $(3.12)_{[i,2]}$, а потім отримані рівності в

(3.12)_[i,3] при $k = 2$ одержимо:

$$\left\{ \begin{array}{l} 0 = tc_{61}d_{13} + t^2c_{51}d_{23}, \\ 0 = tc_{71}d_{13} + t^2c_{61}d_{23}, \\ 0 = tc_{11}d_{13} + t^2c_{71}d_{23}, \\ tc_{11} = tc_{41}d_{13} + t^2c_{31}d_{23} + t^2c_{21}d_{33}, \\ t^2c_{21} = tc_{51}d_{13} + t^2c_{41}d_{23}, \\ t^2c_{61} = tc_{21}d_{13} + tc_{11}d_{23} + t^2c_{71}d_{33}, \\ tc_{71} = tc_{31}d_{13} + tc_{21}d_{23} + tc_{11}d_{33} \end{array} \right.$$

З 3-го рівняння одержуємо $tc_{11}d_{13} \in t^2K$. Тобто $c_{11}d_{13} \in tK$, що неможливо, бо $c_{11} = c_{k-1,1} \in R^*$, $d_{13} \in K^*$.

Підставляючи (3.12)_[i,1] у (3.12)_[i,2], а потім отримані рівності в (3.12)_[i,3] при $k = 3$ одержимо:

$$\left\{ \begin{array}{l} 0 = tc_{71}d_{13} + t^2c_{61}d_{23}, \\ 0 = tc_{11}d_{13} + t^2c_{71}d_{23}, \\ c_{11} = tc_{41}d_{13} + tc_{31}d_{23} + tc_{21}d_{33}, \\ tc_{21} = tc_{51}d_{13} + t^2c_{41}d_{23} + t^2c_{31}d_{33}, \\ t^2c_{31} = tc_{61}d_{13} + t^2c_{51}d_{23}, \\ t^2c_{61} = tc_{21}d_{13} + tc_{11}d_{23} + t^2c_{71}d_{33}, \\ tc_{71} = tc_{31}d_{13} + tc_{21}d_{23} + tc_{11}d_{33}. \end{array} \right.$$

З 1-го рівняння $c_{11} \in tK$. Тоді з 6-го рівняння оскільки одержуємо $tc_{21}d_{13} \in t^2K$. Тобто $c_{21}d_{13} \in tK$, що неможливо, бо $c_{21} = c_{k-1,1} \in R^*$, $d_{13} \in K^*$.

Підставляючи (3.12)_[i,1] у (3.12)_[i,2], а потім отримані рівності в

(3.12)_[i,3] при $k = 4$ одержимо:

$$\left\{ \begin{array}{l} 0 = tc_{11}d_{13} + t^2c_{71}d_{23}, \\ c_{11} = tc_{41}d_{13} + tc_{31}d_{23} + tc_{21}d_{33}, \\ c_{21} = tc_{51}d_{13} + tc_{41}d_{23} + tc_{31}d_{33}, \\ tc_{31} = tc_{61}d_{13} + t^2c_{51}d_{23} + t^2c_{41}d_{33}, \\ t^2c_{41} = tc_{71}d_{13} + t^2c_{61}d_{23}, \\ t^2c_{61} = tc_{21}d_{13} + tc_{11}d_{23} + t^2c_{71}d_{33}, \\ tc_{71} = tc_{31}d_{13} + tc_{21}d_{23} + tc_{11}d_{33}. \end{array} \right.$$

З 2-го та 3-го рівняння відповідно маємо: $c_{11} = tc_{41}d_{13} + tc_{31}d_{23} + tc_{21}d_{33}$, $c_{21} = tc_{51}d_{13} + tc_{41}d_{23} + tc_{31}d_{33}$, з останнього рівняння оскільки $\text{Ann } t = t^2K$ $c_{71} = c_{31}d_{13} + c_{21}d_{23} + c_{11}d_{33} + t^2c'_{71}$ ($c'_{71} \in K$). Після підстановки отримаємо систему

$$\left\{ \begin{array}{l} 0 = t^2c_{41}d_{13}^2 + 2t^2c_{31}d_{13}d_{23}, \\ tc_{31} = tc_{61}d_{13} + t^2c_{51}d_{23} + t^2c_{41}d_{33}, \\ t^2c_{41} = tc_{31}d_{13}^2 + t^2c_{61}d_{23} + t^2c_{51}d_{13}^2d_{23} + \\ \quad t^2c_{41}d_{13}d_{23}^2 + t^2c_{41}d_{13}^2d_{33} + 2t^2c_{31}d_{13}d_{23}d_{33}, \\ t^2c_{61} = t^2c_{51}d_{13}^2 + 2t^2c_{41}d_{13}d_{23} + t^2c_{31}d_{23}^2 + 2t^2c_{31}d_{13}d_{33}. \end{array} \right.$$

З 3-го рівняння одержуємо $tc_{31}d_{13}^2 \in t^2K$. Тобто $c_{31}d_{13}^2 \in tK$, що неможливо, бо $c_{31} = c_{k-1,1} \in R^*$, $d_{13} \in K^*$.

Підставляючи (3.12)_[i,1] у (3.12)_[i,2], а потім отримані рівності в

(3.12)_[i,3] при $k = 5$ одержимо:

$$\left\{ \begin{array}{l} c_{11} = tc_{41}d_{13} + tc_{31}d_{23} + tc_{21}d_{33}, \\ c_{21} = tc_{51}d_{13} + tc_{41}d_{23} + tc_{31}d_{33}, \\ c_{31} = tc_{61}d_{13} + tc_{51}d_{23} + tc_{41}d_{33}, \\ tc_{41} = tc_{71}d_{13} + t^2c_{61}d_{23} + t^2c_{51}d_{33}, \\ t^2c_{51} = tc_{11}d_{13} + t^2c_{71}d_{23}, \\ t^2c_{61} = tc_{21}d_{13} + tc_{11}d_{23} + t^2c_{71}d_{33}, \\ tc_{71} = tc_{31}d_{13} + tc_{21}d_{23} + tc_{11}d_{33} \end{array} \right.$$

З 1-го, 2-го та 3-го рівняння відповідно маємо: $c_{11} = tc_{41}d_{13} + tc_{31}d_{23} + tc_{21}d_{33}$, $c_{21} = tc_{51}d_{13} + tc_{41}d_{23} + tc_{31}d_{33}$, $c_{31} = tc_{61}d_{13} + tc_{51}d_{23} + tc_{41}d_{33}$, з останнього рівняння оскільки $\text{Ann } t = t^2K$ $c_{71} = c_{31}d_{13} + c_{21}d_{23} + c_{11}d_{33} + t^2c'_{71}$ ($c'_{71} \in K$). Після підстановки отримаємо систему

$$\left\{ \begin{array}{l} tc_{41} = t^2c_{61}d_{13}^2 + t^2c_{61}d_{23} + 2t^2c_{51}d_{13}^2d_{23} + \\ \quad t^2c_{41}d_{13}d_{23}^2 + t^2c_{51}d_{33} + 2t^2c_{41}d_{13}^2d_{33}, \\ t^2c_{51} = t^2c_{41}d_{13}^2, \\ t^2c_{61} = t^2c_{51}d_{13}^2 + 2t^2c_{41}d_{13}d_{23}. \end{array} \right.$$

З 1-го рівняння одержуємо $tc_{41} \in t^2K$. Тобто $c_{41} \in tK$, що неможливо, бо $c_{41} = c_{k-1,1} \in K^*$. $\square$

Лема 3.14. Матриця $M(t, k, 7)$ ($1 < k < 6$) не є подібна над K до матриці вигляду

$$N = \left(\begin{array}{ccc|c} 0 & \boxed{td_{12}} & td_{13} & B \\ 1 & td_{22} & td_{23} & \\ 0 & td_{32} & td_{33} & \\ \hline & 0 & & A \end{array} \right)$$

для жодних $d_{12} \in K^*$, d_{22} , d_{32} , d_{13} , d_{23} , $d_{33} \in K$.

Доведення. Нехай для деякої оборотної матриці $C = (c_{ij})$ порядку 7 над K , для деякого k ($1 < k < 6$) і $d_{12} \in K^*$, $d_{22}, d_{32}, d_{13}, d_{23}, d_{33} \in K$

$$M(t, k, 7)C = CN. \quad (3.13)$$

Для спрощення викладок знову вважаємо, що $t^3 = 0$. Тоді:

$$\begin{aligned} (3.13)_{[1,1]} : & \quad tc_{71} = c_{12}, \\ (3.13)_{[2,1]} : & \quad c_{11} = c_{22}, \\ & \quad \dots\dots\dots \\ (3.13)_{[k,1]} : & \quad c_{k-1,1} = c_{k,2}, \\ (3.13)_{[k+1,1]} : & \quad c_{k,1} = c_{k+1,2}, \\ (3.13)_{[k+2,1]} : & \quad tc_{k+1,1} = c_{k+2,2}, \\ & \quad \dots\dots\dots \\ (3.13)_{[7,1]} : & \quad tc_{61} = c_{72}. \end{aligned}$$

Таким чином $\overline{c_{12}} = \overline{c_{k+2,2}} = \dots = \overline{c_{72}} = 0$.

$$\begin{aligned} (3.13)_{[1,2]} : & \quad tc_{72} = tc_{11}d_{12} + tc_{12}d_{22} + tc_{13}d_{32}, \\ (3.13)_{[2,2]} : & \quad c_{12} = tc_{21}d_{12} + tc_{22}d_{22} + tc_{23}d_{32}, \\ & \quad \dots\dots\dots \\ (3.13)_{[k+1,2]} : & \quad c_{k2} = tc_{k+1,1}d_{12} + tc_{k+1,2}d_{22} + tc_{k+1,3}d_{32}, \\ (3.13)_{[k+2,2]} : & \quad tc_{k+1,2} = tc_{k+2,1}d_{12} + tc_{k+2,2}d_{22} + tc_{k+2,3}d_{32}, \\ & \quad \dots\dots\dots \\ (3.13)_{[7,2]} : & \quad tc_{n-1,2} = tc_{71}d_{12} + tc_{72}d_{22} + tc_{73}d_{32}. \end{aligned}$$

Таким чином $\overline{c_{12}} = \dots = \overline{c_{k2}} = \overline{c_{k+2,2}} = \dots = \overline{c_{72}} = 0$. Крім того,

$$\begin{aligned}
 (3.13)_{[1,3]} : \quad & tc_{73} = tc_{11}d_{13} + tc_{12}d_{23} + tc_{13}d_{33}, \\
 (3.13)_{[2,3]} : \quad & c_{13} = tc_{21}d_{13} + tc_{22}d_{23} + tc_{23}d_{33}, \\
 & \dots\dots\dots \\
 (3.13)_{[k+1,3]} : \quad & c_{k3} = tc_{k+1,1}d_{13} + tc_{k+1,2}d_{23} + tc_{k+1,3}d_{33}, \\
 (3.13)_{[k+2,3]} : \quad & tc_{k+1,3} = tc_{k+2,1}d_{13} + tc_{k+2,2}d_{23} + tc_{k+2,3}d_{33}, \\
 & \dots\dots\dots \\
 (3.13)_{[7,3]} : \quad & tc_{n-1,3} = tc_{71}d_{13} + tc_{72}d_{23} + tc_{73}d_{33}.
 \end{aligned}$$

Також отримуємо $\overline{c_{13}} = \dots = \overline{c_{k3}} = 0$.

Крім того, маємо подібність матриць над K

$$\begin{aligned}
 & \begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & td_{23} \\ 0 & td_{32} & td_{33} \end{pmatrix} \sim \\
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -d_{12}^{-1}d_{13} \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & td_{23} \\ 0 & td_{32} & td_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -d_{12}^{-1}d_{13} \\ 0 & 0 & 1 \end{pmatrix} = \\
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & d_{12}^{-1}d_{13} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & td_{12} & 0 \\ 1 & td_{22} & t(d_{23} - d_{22}d_{12}^{-1}d_{13}) \\ 0 & td_{32} & t(d_{33} - d_{32}d_{12}^{-1}d_{13}) \end{pmatrix} = \\
 & \begin{pmatrix} 0 & td_{12} & 0 \\ 1 & t(d_{22} + d_{32}d_{12}^{-1}d_{13}) & t(d_{23} - d_{22}d_{12}^{-1}d_{13} + d_{33}d_{12}^{-1}d_{13} - d_{32}d_{12}^{-2}d_{13}^2) \\ 0 & td_{32} & t(d_{33} - d_{32}d_{12}^{-1}d_{13}) \end{pmatrix} = \\
 & \begin{pmatrix} 0 & td_{12} & 0 \\ 1 & td'_{22} & td'_{23} \\ 0 & td_{32} & td'_{33} \end{pmatrix}
 \end{aligned}$$

для деяких $d'_{22}, d'_{23}, d'_{33} \in K$. Не зменшуючи загальності, можна вважати, що $d_{13} = 0$. Тоді

$$(3.13)_{[1,3]} : \quad tc_{73} = tc_{12}d_{23} + tc_{13}d_{33},$$

$$(3.13)_{[k+2,3]} : \quad tc_{k+1,3} = tc_{k+2,2}d_{23} + tc_{k+2,3}d_{33},$$

.....

$$(3.13)_{[7,3]} : \quad tc_{n-1,3} = tc_{72}d_{23} + tc_{73}d_{33}.$$

Оскільки $\overline{c_{12}} = \overline{c_{13}} = 0$, $t \neq 0$, то з $(3.13)_{[1,3]}$ $\overline{c_{73}} = 0$. Оскільки $\overline{c_{72}} = \overline{c_{73}} = 0$, $t \neq 0$, то з $(3.13)_{[7,3]}$ $\overline{c_{63}} = 0$. Нехай $k+1 < i < n$ і $\overline{c_{i3}} = 0$. Враховуючи, що $i \neq k+1$ $\overline{c_{i,2}} = 0$ з $(3.13)_{[i,3]}$ $tc_{i-1,3} = tc_{i2}d_{23} + tc_{i3}d_{33}$ одержимо $\overline{c_{i-1,3}} = 0$. Таким чином $\overline{c_{k+1,3}} = \dots = \overline{c_{73}} = 0$. Отже, $\overline{c_{13}} = \dots = \overline{c_{k3}} = \overline{c_{k+1,3}} = \dots = \overline{c_{73}} = 0$. Що суперечить оборотності $\det \overline{C}$. $\square$

Лема 3.15. Матриця $M(t, k, 7)$ ($1 < k < 6$) не є подібна над K для жодного $d_{12} \in tK$ до матриці вигляду

$$N = \left(\begin{array}{ccc|c} 0 & \boxed{td_{12}} & td_{13} & \\ 1 & td_{22} & td_{23} & B \\ 0 & td_{32} & td_{33} & \\ \hline & 0 & & A \end{array} \right).$$

Доведення. Нехай для деякої оборотної матриці $C = (c_{ij})$ порядку 7 над K , для деякого k ($1 < k < 6$) і $d_{12} \in tK$ має місце

$$M(t, k, 7)C = CN. \quad (3.14)$$

Легко бачити подібність матриць над K

$$\begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & td_{23} \\ 0 & td_{32} & td_{33} \end{pmatrix} \sim$$

$$\begin{aligned}
& \begin{pmatrix} 1 & 0 & -td_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & td_{23} \\ 0 & td_{32} & td_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & -td_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \\
& \begin{pmatrix} 1 & 0 & td_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & 0 \\ 0 & td_{32} & td_{33} \end{pmatrix} = \begin{pmatrix} 0 & td_{12} + t^2 d_{23} d_{32} & td_{13} + t^2 d_{23} d_{33} \\ 1 & td_{22} & 0 \\ 0 & td_{32} & td_{33} \end{pmatrix} \sim \\
& \begin{pmatrix} 1 & -td_{22} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & td_{12} + t^2 d_{23} d_{32} & td_{13} + t^2 d_{23} d_{33} \\ 1 & td_{22} & 0 \\ 0 & td_{32} & td_{33} \end{pmatrix} \begin{pmatrix} 1 & -td_{22} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \\
& \begin{pmatrix} 1 & td_{22} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & td_{12} + t^2 d_{23} d_{32} & td_{13} + t^2 d_{23} d_{33} \\ 1 & 0 & 0 \\ 0 & td_{32} & td_{33} \end{pmatrix} = \\
& \begin{pmatrix} td_{22} & td_{12} + t^2 d_{23} d_{32} & td_{13} + t^2 d_{23} d_{33} \\ 1 & 0 & 0 \\ 0 & td_{32} & td_{33} \end{pmatrix}.
\end{aligned}$$

Якщо

$$\begin{vmatrix} d_{12} & d_{13} \\ d_{32} & d_{33} \end{vmatrix} \in tK,$$

тоді над кільцем K/t^2K матриця $M(t, k, 7)$ подібна матриці з нульовим стовпчиком, що за теоремою 3.10 неможливе. Отже,

$$\begin{vmatrix} d_{12} & d_{13} \\ d_{32} & d_{33} \end{vmatrix} \in K^*.$$

Тоді $d_{12} \in K^*$ або $d_{32} \in K^*$.

За умовою леми $d_{12} \in tK$, тому $d_{32} \in K^*$. Маємо подібність матриць над K

$$\begin{aligned}
 & \begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & td_{23} \\ 0 & td_{32} & td_{33} \end{pmatrix} \sim \\
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -d_{32}^{-1}d_{33} \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & td_{23} \\ 0 & td_{32} & td_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -d_{32}^{-1}d_{33} \\ 0 & 0 & 1 \end{pmatrix} = \\
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & d_{32}^{-1}d_{33} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & td_{12} & td_{13} - td_{12}d_{32}^{-1}d_{33} \\ 1 & td_{22} & td_{23} - td_{22}d_{32}^{-1}d_{33} \\ 0 & td_{32} & 0 \end{pmatrix} = \\
 & \begin{pmatrix} 0 & td_{12} & td_{13} - td_{12}d_{32}^{-1}d_{33} \\ 1 & td_{22} + td_{33} & td_{23} - td_{22}d_{32}^{-1}d_{33} \\ 0 & td_{32} & 0 \end{pmatrix} = \begin{pmatrix} 0 & td_{12} & td'_{13} \\ 1 & td'_{22} & td'_{23} \\ 0 & td_{32} & 0 \end{pmatrix} \sim \\
 & \begin{pmatrix} 1 & 0 & -td'_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & td_{12} & td'_{13} \\ 1 & td'_{22} & td'_{23} \\ 0 & td_{32} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -td'_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \\
 & \begin{pmatrix} 1 & 0 & td'_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & td_{12} & td'_{13} \\ 1 & td'_{22} & 0 \\ 0 & td_{32} & 0 \end{pmatrix} = \begin{pmatrix} 0 & td_{12} + t^2d'_{23}d_{32} & td'_{13} \\ 1 & td'_{22} & 0 \\ 0 & td_{32} & 0 \end{pmatrix}
 \end{aligned}$$

для деяких $d'_{22}, d'_{13}, d'_{23} \in K$. Оскільки $d_{12} \in tK$, то також $d_{12} + td'_{23}d_{32} \in tK$. Не зменшуючи загальності, можна вважати, що $d_{23} = d_{33} = 0$, тоді враховуючи, що

$$\begin{vmatrix} d_{12} & d_{13} \\ d_{32} & d_{33} \end{vmatrix} \in K^*,$$

$d_{13} \in K^*$.

Для спрощення викладок знову вважаємо, що $t^3 = 0$. Тоді:

$$\begin{aligned}
 (3.14)_{[1,1]} : \quad & tc_{71} = c_{12}, \\
 (3.14)_{[2,1]} : \quad & c_{11} = c_{22}, \\
 & \dots\dots\dots \\
 (3.14)_{[k,1]} : \quad & c_{k-1,1} = c_{k,2}, \\
 (3.14)_{[k+1,1]} : \quad & c_{k,1} = c_{k+1,2}, \\
 (3.14)_{[k+2,1]} : \quad & tc_{k+1,1} = c_{k+2,2}, \\
 & \dots\dots\dots \\
 (3.14)_{[7,1]} : \quad & tc_{61} = c_{72}.
 \end{aligned}$$

Таким чином $\overline{c_{12}} = \overline{c_{k+2,2}} = \dots = \overline{c_{72}} = 0$.

$$\begin{aligned}
 (3.14)_{[1,2]} : \quad & tc_{72} = tc_{11}d_{12} + tc_{12}d_{22} + tc_{13}d_{32}, \\
 (3.14)_{[2,2]} : \quad & c_{12} = tc_{21}d_{12} + tc_{22}d_{22} + tc_{23}d_{32}, \\
 & \dots\dots\dots \\
 (3.14)_{[k+1,2]} : \quad & c_{k2} = tc_{k+1,1}d_{12} + tc_{k+1,2}d_{22} + tc_{k+1,3}d_{32}, \\
 (3.14)_{[k+2,2]} : \quad & tc_{k+1,2} = tc_{k+2,1}d_{12} + tc_{k+2,2}d_{22} + tc_{k+2,3}d_{32}, \\
 & \dots\dots\dots \\
 (3.14)_{[7,2]} : \quad & tc_{n-1,2} = tc_{71}d_{12} + tc_{72}d_{22} + tc_{73}d_{32}.
 \end{aligned}$$

Таким чином $\overline{c_{12}} = \dots = \overline{c_{k2}} = \overline{c_{k+2,2}} = \dots = \overline{c_{72}} = 0$. Крім того,

$$\begin{aligned}
 (3.14)_{[1,3]} : \quad & tc_{73} = tc_{11}d_{13}, \\
 (3.14)_{[2,3]} : \quad & c_{13} = tc_{21}d_{13}, \\
 & \dots\dots\dots \\
 (3.14)_{[k+1,3]} : \quad & c_{k3} = tc_{k+1,1}d_{13}, \\
 (3.14)_{[k+2,3]} : \quad & tc_{k+1,3} = tc_{k+2,1}d_{13}, \\
 & \dots\dots\dots \\
 (3.14)_{[7,3]} : \quad & tc_{n-1,3} = tc_{71}d_{13}.
 \end{aligned}$$

Також отримуємо $\overline{c_{13}} = \dots = \overline{c_{k3}} = 0$. В силу оборотності детермінанта матриці $\overline{C}$ $c_{k+1,2} = c_{k1} \in K^*$.

Підставляючи $(3.14)_{[i,1]}$ у $(3.14)_{[i,2]}$ разом з $(3.14)_{[i,3]}$ при $k = 2$ одержимо:

$$\left\{ \begin{array}{l} c_{11} = tc_{21}d_{22} + tc_{33}d_{32} + t^2c_{31}d'_{12}, \\ c_{13} = tc_{21}d_{13}, \\ tc_{21} = t^2c_{31}d_{22} + tc_{43}d_{32} + t^2c_{41}d'_{12}, \\ c_{23} = tc_{31}d_{13}, \\ t^2c_{31} = t^2c_{41}d_{22} + tc_{53}d_{32} + t^2c_{51}d'_{12}, \\ tc_{33} = tc_{41}d_{13}, \\ t^2c_{41} = t^2c_{51}d_{22} + tc_{63}d_{32} + t^2c_{61}d'_{12}, \\ tc_{43} = tc_{51}d_{13}, \\ t^2c_{51} = t^2c_{61}d_{22} + tc_{73}d_{32} + t^2c_{71}d'_{12}, \\ tc_{53} = tc_{61}d_{13}, \\ t^2c_{61} = t^2c_{71}d_{22} + tc_{13}d_{32} + t^2c_{11}d'_{12}, \\ tc_{63} = tc_{71}d_{13}, \\ tc_{71} = tc_{11}d_{22} + tc_{23}d_{32} + t^2c_{21}d'_{12}, \\ tc_{73} = tc_{11}d_{13}. \end{array} \right.$$

З 1-го, 2-го та 4-го рівняння відповідно одержимо $c_{11} = tc_{31}d_{12} + tc_{21}d_{22} + tc_{33}d_{32}$, $c_{13} = tc_{21}d_{13}$, $c_{23} = tc_{31}d_{13}$. З 12-го, 13-го та 14-го рівняння оскільки $\text{Ann } t = t^2K$ відповідно одержуємо $c_{63} = c_{71}d_{13} + t^2c'_{63}$, $c_{71} = c_{11}d_{22} + c_{23}d_{32} + tc_{21}d'_{12} + t^2c'_{71}$, $c_{73} = c_{11}d_{13} + t^2c'_{73}$ для деяких

$c'_{63}, c'_{71}, c'_{73} \in K$. Після підстановки одержимо:

$$\left\{ \begin{array}{l} tc_{21} = t^2c_{31}d_{22} + tc_{43}d_{32} + t^2c_{41}d'_{12}, \\ t^2c_{31} = t^2c_{41}d_{22} + tc_{53}d_{32} + t^2c_{51}d'_{12}, \\ tc_{33} = tc_{41}d_{13}, \\ t^2c_{41} = t^2c_{51}d_{22} + t^2c_{21}d_{13}d_{22}^2d_{32} + t^2c_{31}d_{13}^2d_{32}^2 + \\ \quad t^2c_{33}d_{13}d_{22}d_{32}^2 + t^2c_{61}d'_{12} + t^2c_{21}d_{13}d_{32}d'_{12}, \\ tc_{43} = tc_{51}d_{13}, \\ t^2c_{51} = t^2c_{61}d_{22} + t^2c_{21}d_{13}d_{22}d_{32} + t^2c_{33}d_{13}d_{32}^2, \\ tc_{53} = tc_{61}d_{13}, \\ t^2c_{61} = t^2c_{21}d_{13}d_{32}. \end{array} \right.$$

З 7-го та 8-го рівняння оскільки $\text{Ann } t = t^2K, \text{Ann } t^2 = tK$ відповідно одержуємо $c_{53} = c_{61}d_{13} + t^2c'_{53}$, $c_{61} = c_{21}d_{13}d_{32} + tc'_{61}$ для деяких $c'_{53}, c'_{61} \in K$. Після підстановки отримаємо систему

$$\left\{ \begin{array}{l} tc_{21} = t^2c_{31}d_{22} + tc_{43}d_{32} + t^2c_{41}d'_{12}, \\ t^2c_{31} = t^2c_{41}d_{22} + tc_{21}d_{13}^2d_{32}^2 + t^2d_{13}d_{32}c'_{61} + t^2c_{51}d'_{12}, \\ tc_{33} = tc_{41}d_{13}, \\ t^2c_{41} = t^2c_{51}d_{22} + t^2c_{21}d_{13}d_{22}^2d_{32} + t^2c_{31}d_{13}^2d_{32}^2 + \\ \quad t^2c_{33}d_{13}d_{22}d_{32}^2 + 2t^2c_{21}d_{13}d_{32}d'_{12}, \\ tc_{43} = tc_{51}d_{13}, \\ t^2c_{51} = 2t^2c_{21}d_{13}d_{22}d_{32} + t^2c_{33}d_{13}d_{32}^2. \end{array} \right.$$

з 2-го рівнянням $tc_{21}d_{13}^2d_{32}^2 \in t^2K$. Тобто $c_{21}d_{13}^2d_{32}^2 \in tK$, що суперечить умовам $c_{21} = c_{k1} \in K^*, d_{13}, d_{32} \in K^*$.

Підставляючи (3.14)_[i,1] у (3.14)_[i,2] разом з (3.14)_[i,3] при $k = 3$ одер-

ЖИМО:

$$\left\{ \begin{array}{l} c_{11} = tc_{21}d_{22} + tc_{33}d_{32} + t^2c_{31}d'_{12}, \\ c_{13} = tc_{21}d_{13}, \\ c_{21} = tc_{31}d_{22} + tc_{43}d_{32} + t^2c_{41}d'_{12}, \\ c_{23} = tc_{31}d_{13}, \\ tc_{31} = t^2c_{41}d_{22} + tc_{53}d_{32} + t^2c_{51}d'_{12}, \\ c_{33} = tc_{41}d_{13}, \\ t^2c_{41} = t^2c_{51}d_{22} + tc_{63}d_{32} + t^2c_{61}d'_{12}, \\ tc_{43} = tc_{51}d_{13}, \\ t^2c_{51} = t^2c_{61}d_{22} + tc_{73}d_{32} + t^2c_{71}d'_{12}, \\ tc_{53} = tc_{61}d_{13}, \\ t^2c_{61} = t^2c_{71}d_{22} + tc_{13}d_{32} + t^2c_{11}d'_{12}, \\ tc_{63} = tc_{71}d_{13}, \\ tc_{71} = tc_{11}d_{22} + tc_{23}d_{32} + t^2c_{21}d'_{12}, \\ tc_{73} = tc_{11}d_{13}. \end{array} \right.$$

З 1-го, 2-го 3-го, 4-го та 6-го рівняння відповідно одержимо $c_{11} = tc_{21}d_{22} + tc_{33}d_{32} + t^2c_{31}d'_{12}$, $c_{13} = tc_{21}d_{13}$, $c_{21} = tc_{31}d_{22} + tc_{43}d_{32} + t^2c_{41}d'_{12}$, $c_{23} = tc_{31}d_{13}$, $c_{33} = tc_{41}d_{13}$. З 13-го та 14-го рівняння оскільки $\text{Ann } t = t^2K$ відповідно одержуємо $c_{71} = c_{11}d_{22} + c_{23}d_{32} + tc_{21}d'_{12} + t^2c'_{71}$, $c_{73} = c_{11}d_{13} + t^2c'_{73}$. для деяких $c'_{71}, c'_{73} \in K$. Після підстановки одержимо:

$$\left\{ \begin{array}{l} tc_{31} = t^2c_{41}d_{22} + tc_{61}d_{13}d_{32} + t^2c_{51}d'_{12}, \\ t^2c_{41} = t^2c_{51}d_{22} + tc_{63}d_{32} + t^2c_{61}d'_{12}, \\ tc_{43} = tc_{51}d_{13}, \\ t^2c_{51} = t^2c_{61}d_{22}, \\ t^2c_{61} = 0, \\ tc_{63} = t^2c_{31}d_{13}^2d_{32}. \end{array} \right.$$

З 5-го та 1-го рівняння оскільки $\text{Ann } t = t^2K$ відповідно одержуємо $c_{61} =$

tc'_{61} , $c_{31} = tc_{41}d_{22} + tc'_{61}d_{13}d_{32} + tc_{51}d'_{12} + tc'_{31}$ для деяких $c'_{31}, c'_{61} \in K$, що неможливо, бо $c_{31} = c_{k1} \in K^*$.

Підставляючи $(3.14)_{[i,1]}$ у $(3.14)_{[i,2]}$ разом з $(3.14)_{[i,3]}$ при $k = 4$ одержимо:

$$\left\{ \begin{array}{l} c_{11} = tc_{21}d_{22} + tc_{33}d_{32} + t^2c_{31}d'_{12}, \\ c_{13} = tc_{21}d_{13}, \\ c_{21} = tc_{31}d_{22} + tc_{43}d_{32} + t^2c_{41}d'_{12}, \\ c_{23} = tc_{31}d_{13}, \\ c_{31} = tc_{41}d_{22} + tc_{53}d_{32} + t^2c_{51}d'_{12}, \\ c_{33} = tc_{41}d_{13}, \\ tc_{41} = t^2c_{51}d_{22} + tc_{63}d_{32} + t^2c_{61}d'_{12}, \\ c_{43} = tc_{51}d_{13}, \\ t^2c_{51} = t^2c_{61}d_{22} + tc_{73}d_{32} + t^2c_{71}d'_{12}, \\ tc_{53} = tc_{61}d_{13}, \\ t^2c_{61} = t^2c_{71}d_{22} + tc_{13}d_{32} + t^2c_{11}d'_{12}, \\ tc_{63} = tc_{71}d_{13}, \\ tc_{71} = tc_{11}d_{22} + tc_{23}d_{32} + t^2c_{21}d'_{12}, \\ tc_{73} = tc_{11}d_{13} \end{array} \right.$$

Підставляючи 1-е та 4-е рівняння в 13-е одержимо $tc_{71} = t^2c_{21}d_{22}^2 + t^2c_{31}d_{13}d_{32} + t^2c_{33}d_{22}d_{32} + t^2c_{21}d'_{12}$. Тоді, враховуючи, що $\text{Ann } t = t^2K$, $c_{71} = tc_{21}d_{22}^2 + tc_{31}d_{13}d_{32} + tc_{33}d_{22}d_{32} + tc_{21}d'_{12} + t^2c'_{71}$ ($c'_{71} \in K$). Підставляючи отримане рівняння в 12-е, одержимо $tc_{63} = t^2c_{21}d_{13}d_{22}^2 + t^2c_{31}d_{13}^2d_{32} + t^2c_{33}d_{13}d_{22}d_{32} + t^2c_{21}d_{13}d'_{12}$. Тоді, враховуючи, що $\text{Ann } t = t^2K$, $c_{63} = tc_{21}d_{13}d_{22}^2 + tc_{31}d_{13}^2d_{32} + tc_{33}d_{13}d_{22}d_{32} + tc_{21}d_{13}d'_{12} + t^2c'_{63}$; ($c'_{63} \in K$). Підставляючи отримане рівняння в 7-е, одержимо $tc_{41} = t^2c_{51}d_{22} + t^2c_{21}d_{13}d_{22}^2d_{32} + t^2c_{31}d_{13}^2d_{32}^2 + t^2c_{33}d_{13}d_{22}d_{32}^2 + t^2c_{61}d'_{12} + t^2c_{21}d_{13}d_{32}d'_{12}$. Тоді $tc_{41} \in t^2K$ або $c_{41} \in tK$, що неможливо, бо $c_{41} = c_{k1} \in K^*$.

Підставляючи $(3.14)_{[i,1]}$ у $(3.14)_{[i,2]}$ разом з $(3.14)_{[i,3]}$ при $k = 5$ одержимо:

$$\left\{ \begin{array}{l} c_{11} = tc_{21}d_{22} + tc_{33}d_{32} + t^2c_{31}d'_{12}, \\ c_{13} = tc_{21}d_{13}, \\ c_{21} = tc_{31}d_{22} + tc_{43}d_{32} + t^2c_{41}d'_{12}, \\ c_{23} = tc_{31}d_{13}, \\ c_{31} = tc_{41}d_{22} + tc_{53}d_{32} + t^2c_{51}d'_{12}, \\ c_{33} = tc_{41}d_{13}, \\ c_{41} = tc_{51}d_{22} + tc_{63}d_{32} + t^2c_{61}d'_{12}, \\ c_{43} = tc_{51}d_{13}, \\ tc_{51} = t^2c_{61}d_{22} + tc_{73}d_{32} + t^2c_{71}d'_{12}, \\ c_{53} = tc_{61}d_{13}, \\ t^2c_{61} = t^2c_{71}d_{22} + tc_{13}d_{32} + t^2c_{11}d'_{12}, \\ tc_{63} = tc_{71}d_{13}, \\ tc_{71} = tc_{11}d_{22} + tc_{23}d_{32} + t^2c_{21}d'_{12}, \\ tc_{73} = tc_{11}d_{13}. \end{array} \right.$$

Підставляючи 1-е рівняння в 14-е одержимо $tc_{73} = t^2c_{21}d_{13}d_{22} + t^2c_{33}d_{13}d_{32}$. Тоді, враховуючи, що $\text{Ann } t = t^2K$, $c_{73} = tc_{21}d_{13}d_{22} + tc_{33}d_{13}d_{32} + t^2c'_{73}$ ($c'_{73} \in K$). Підставляючи отримане рівняння в 9-е одержимо $tc_{51} = t^2c_{61}d_{22} + t^2c_{21}d_{13}d_{22}d_{32} + t^2c_{33}d_{13}d_{32}^2 + t^2c_{71}d'_{12}$. Тоді $tc_{51} \in t^2K$ або $c_{51} \in tK$, що неможливо, бо $c_{51} = c_{k1} \in K^*$. $\square$

Теорема 3.16. *Нехай K — комутативне локальне кільце, радикал Джексона якого tK ($t \in K$, $t^2 \neq 0$). Матриця $M(t, k, 7)$ незвідна над K для жодного k ($0 < k < 7$).*

Доведення. За теоремою 1.11 достатньо розглянути випадки $1 < k < 6$.

Припустимо матриця $M(t, k, 7)$ звідна. Тоді маємо подібність над K

$$M(t, k, 7) \sim \begin{pmatrix} D & B \\ 0 & A \end{pmatrix}, \quad (3.15)$$

де D — $m \times m$ -матриця. За наслідком 3.11 можна вважати, що $m = 2$ або $m = 3$. За теоремою 3.10 можна вважати, що

$$D = \begin{pmatrix} 0 & td_{13} \\ 1 & td_{23} \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 & td_{13} \\ 1 & 0 & td_{23} \\ 0 & 1 & td_{33} \end{pmatrix} \text{ або}$$

$$D = \begin{pmatrix} 0 & td_{12} & td_{13} \\ 1 & td_{22} & td_{23} \\ 0 & td_{32} & td_{33} \end{pmatrix}$$

для деяких $d_{ij} \in K$. У першому випадку маємо протиріччя з лемою 3.12, у другому випадку — з лемою 3.13, у третьому випадку — з лемами 3.14 та 3.15. $\square$

3.5. Висновки до розділу

У цьому розділі вводиться поняття мономіальних матриць та їх видів: канонічних циклічних, t -циклічних, бімономіальних та описуються деякі їх очевидні чи відомі властивості. В підрозділі 3.2 введено поняття спадкової звідності t -циклічних матриць, та встановлено одну достатню умову їх спадкової звідності над комутативним кільцем. Аналогічне встановлено в підрозділі 3.3 для бімономіальних матриць над комутативним кільцем. А саме доведено, що така матриця спадково звідна, коли її порядок і кількість одиниць у вигляді не взаємно прості. В підрозділі 3.4 показана незвідність всіх бімономіальних матриць 7-го порядку над комутативним локальним кільцем довжини $l > 2$.

Ключовим поняттям розділу є спадкова звідність t -циклічних матриць та бімономіальних матриць.

Результати цього розділу анонсовано в [47, 103, 215, 216] та опубліковано в [17, 48, 49, 84, 106, 107].

РОЗДІЛ 4.

УНІМОНОМІАЛЬНІ ЗОБРАЖЕННЯ ГРУП НАД ЛОКАЛЬНИМИ КІЛЬЦЯМИ СКІНЧЕНОЇ ДОВЖИНИ

Як завжди в дисертації розглядаються тільки кільця з одиницями. Всюди, якщо не вказано інше, у межах розділу через K будемо позначати комутативне локальне кільце головних ідеалів, що не є полем; через K^* групу його оборотних елементів відносно множення. Тоді єдиний максимальний ідеал (радикал Джекобсона) $\text{Rad } K$ кільця K є головним ідеалом породженим деяким ненульовим елементом t кільця K . Елемент t визначається однозначно з точністю до оборотного множника, а будь-який ненульовий елемент $x \in K$ набуде вигляду εt^s , де $\varepsilon \in K^*$ і $s \geq 0$ (див. [56, ст. 282]). Число s (яке не залежить від вибору t) називаємо *вагою елемента x* і позначаємо через $w(x)$. Елемент ε вже залежить від t ; крім того, для нецілісного кільця K , навіть при фіксованому t , він визначається елементом x неоднозначно, а саме $\varepsilon t^s = \varepsilon' t^s$ тоді і тільки тоді, коли ε і ε' конгруентні за модулем $\text{Ann}(t^s) = \{y \in K \mid yt^s = 0\}$, тобто $\varepsilon - \varepsilon' \in \text{Ann}(t^s)$. Степінь нільпотентності елемента t позначаємо через $l(\text{Rad } K)$. Якщо K — область цілісності, то $l(\text{Rad } K) = \infty$ і навпаки. Якщо K не є область цілісності, то K називають локальним кільцем довжини $l(\text{Rad } K)$. В розділі досліджується число нееквівалентних незвідних на нерозкладних матричних зображень спеціального вигляду циклічних p -груп над кільцем K .

Теоретичні обчислення цього розділу також частково підтверджуються та доповнюються обчисленнями в системі комп'ютерної алгебри GAP 4.10.1 (див. <https://www.gap-system.org/index.html>). Одна її компо-

нента є спеціальна мова, за допомогою якої можна створювати власні програми і розширювати систему.

4.1. Означення та елементарні властивості унімономіальних зображень

Нехай G — скінченно породжена група з деякою фіксованою системою твірних елементів $a_1, \dots, a_r$. Будь-яке матричне зображення групи G над довільним комутативним кільцем K з одиницею еквівалентне до $\Gamma: a_i \rightarrow E_n + M_i$ ($i = 1, \dots, r$), де E_n — одинична $n \times n$ -матриця, M_i — мономіальна матриця порядку n ($i = 1, \dots, r$), назовемо *унімономіальним* (це поняття запропонував В. М. Бондаренко). Поняття, взагалі кажучи, залежить від вибору твірних елементів скінченно породженої групи. Далі в межах розділу ми завжди будемо припускати, що $H = \langle a \rangle$ — циклічна p -група з деяким фіксованим твірним елементом a , K — комутативне локальне кільце головних ідеалів, що не є полем. Очевидно, питання про звідність та розкладність унімономіального зображення

$$\Gamma: a \rightarrow \Gamma(a) = E_n + M,$$

актуальне, лише коли M — канонічно циклічна матриця. Тобто

$$M = M(a_1, \dots, a_n) = \begin{pmatrix} 0 & \dots & 0 & a_n \\ a_1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & a_{n-1} & 0 \end{pmatrix},$$

де $a_i \neq 0$ ($i = 1, \dots, n$). Зрозуміло, що $a_i = \varepsilon_i t^{s_i}$, де $s_i = w(a_i)$ і $\varepsilon_i \in K^*$ (які, згідно з викладеним вище, визначаються a_i неоднозначно). В цьому випадку матрицю $M(a_1, \dots, a_n)$ позначаємо також через $M(\overline{w}, \overline{\varepsilon})$,

де $\bar{w} = (s_1, \dots, s_n)$ і $\bar{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$. Очевидно

$$M(a_1, \dots, a_n) = M(t^{s_1}, \dots, t^{s_n}) \cdot \text{diag}[\varepsilon_1, \dots, \varepsilon_n].$$

Твердження 4.1. *Нехай $H = \langle a \rangle$ — циклічна p -група, K — комутативне локальне кільце характеристики p радикал Джексона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$, E_n — одинична $n \times n$ -матриця, $s_i \in \mathbb{N} \cup \{0\}$ і $\varepsilon_i \in K^*$ ($i = 1, \dots, n$).
Відображення*

$$\Gamma_{\bar{w}, \bar{\varepsilon}}: a \rightarrow \Gamma_{\bar{w}, \bar{\varepsilon}}(a) = E_n + M(\bar{w}, \bar{\varepsilon}) = E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n})$$

є зображенням групи H тоді і тільки тоді, коли $M(t^{s_1}, \dots, t^{s_n})^{|H|} = 0$.

Доведення. Очевидно H є зображенням групи H тоді і тільки тоді, коли $(E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}))^{|H|} = E_n$. Враховуючи, що p — характеристика кільця K , остання умова еквівалентна $M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n})^{|H|} = 0$. Або, що одне і теж,

$$(M(t^{s_1}, \dots, t^{s_n}) \cdot \text{diag}[\varepsilon_1, \dots, \varepsilon_n])^{|H|} = 0. \quad (4.1)$$

Враховуючи, що

$$M(t^{s_1}, \dots, t^{s_n}) \cdot \text{diag}[\varepsilon_1, \dots, \varepsilon_n] = \text{diag}[\varepsilon_n, \varepsilon_1, \dots, \varepsilon_{n-1}] \cdot M(t^{s_1}, \dots, t^{s_n}),$$

рівність (4.1) еквівалентна

$$M(t^{s_1}, \dots, t^{s_n})^{|H|} \cdot \text{diag}[\delta_1, \dots, \delta_n] = 0$$

для деяких $\delta_i \in K^*$ ($i = 1, \dots, n$). Або, що одне і теж,

$$M(t^{s_1}, \dots, t^{s_n})^{|H|} = 0.$$

□

Твердження 4.2. Нехай K — комутативне локальне кільце головних ідеалів, радикал якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l > 1$, $s_i \in \mathbb{N} \cup \{0\}$ ($i = 1, \dots, n$), m — натуральне число.

$$M(t^{s_1}, \dots, t^{s_n})^m = 0 \quad (4.2)$$

тоді і тільки тоді, коли

$$\sum_{j=0}^{m-1} s_{i+j} \geq l \quad (i = 1, \dots, n)$$

при цьому індекси $i + j$ треба замінити на індекси $i + j - kn$ якщо $i + j > kn$, де k — максимально можливе натуральне число (тобто тут індекси розглядаються за модулем n).

Доведення. Очевидно, $M(t^{s_1}, \dots, t^{s_n}) = M(1, \dots, 1) \cdot \text{diag}[t^{s_1}, \dots, t^{s_n}]$. Враховуючи, що $M(1, \dots, 1) \cdot \text{diag}[t^{s_1}, \dots, t^{s_n}] = \text{diag}[t^{s_n}, t^{s_1}, \dots, t^{s_{n-1}}] \cdot M(1, \dots, 1)$ одержимо

$$M(t^{s_1}, \dots, t^{s_n})^m = (M(1, \dots, 1) \cdot \text{diag}[t^{s_1}, \dots, t^{s_n}])^m = \\ M(1, \dots, 1)^m \cdot \prod_{j=0}^{m-1} \text{diag}[t^{s_1}, \dots, t^{s_n}],$$

де $\text{diag}[t^{s_1}, \dots, t^{s_n}] = [\underset{j}{t^{s_j \bmod n+1}}, \dots, t^{s_n}, t^{s_1}, \dots, t^{s_j \bmod n}]$. Враховуючи, що індекси розглядаються за модулем n одержимо

$$M(t^{s_1}, \dots, t^{s_n})^m = M(1, \dots, 1)^m \cdot \prod_{j=0}^{m-1} \text{diag}[t^{s_1+j}, \dots, t^{s_n}, t^{s_1}, \dots, t^{s_j}] = \\ = M(1, \dots, 1)^m \cdot \text{diag} \left[\prod_{j=0}^{m-1} t^{s_1+j}, \prod_{j=0}^{m-1} t^{s_2+j}, \dots, \prod_{j=0}^{m-1} t^{s_{n+j}} \right].$$

Оскільки $M(1, \dots, 1)^m$ оборотна матриця, то рівність (4.2) еквівалентна

$$\prod_{j=0}^{m-1} t^{s_{i+j}} = 0 \quad (i = 1, \dots, n)$$

або, що одне і те ж

$$t^{\sum_{j=0}^{m-1} s_{i+j}} = 0 \quad (i = 1, \dots, n).$$

Тобто рівність (4.2) еквівалентна

$$\sum_{j=0}^{m-1} s_{i+j} \geq l \quad (i = 1, \dots, n).$$

□

Наслідок 4.3. Нехай $H = \langle a \rangle$ — циклічна p -група, K — комутативне локальне кільце характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нілпотентний елемент степеня $l = l(\text{Rad } K) > 1$, E_n — одинична матриця порядку $n \leq |H|$, $s_i \in \mathbb{N} \cup \{0\}$ і $\varepsilon_i \in K^*$ ($i = 1, \dots, n$). Якщо $\sum_{j=1}^n s_j \geq l$, то відображення

$$\Gamma_{\bar{w}, \bar{\varepsilon}}: a \rightarrow \Gamma_{\bar{w}, \bar{\varepsilon}}(a) = E_n + M(\bar{w}, \bar{\varepsilon}) = E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}) \quad (4.3)$$

є зображенням групи H .

Доведення. За твердженням 4.2 $M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_{n-1} t^{s_{n-1}})^n = 0$, бо

$$\sum_{j=0}^{n-1} s_{i+j} = \sum_{j=1}^n s_j \geq l \quad (i = 1, \dots, n).$$

Тоді $0 = M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n})^n = M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n})^{|H|}$. За твердженням 4.1 відображення (4.3) є зображенням групи H . □

Безпосередньо з тверджень 4.1 та 4.2 отримуємо таку теорему.

Теорема 4.4. Нехай $H = \langle a \rangle$ — циклічна p -група, K — комутативне локальне кільце характеристики p , радикал Джекобсона якого

$\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$,
 E_n — одинична $n \times n$ -матриця, $s_i \in \mathbb{N} \cup \{0\}$ і $\varepsilon_i \in K^*$ ($i = 1, \dots, n$).

Відображення

$$\Gamma_{\bar{w}, \bar{\varepsilon}}: a \rightarrow \Gamma_{\bar{w}, \bar{\varepsilon}}(a) = E_n + M(\bar{w}, \bar{\varepsilon}) = E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n})$$

є зображенням групи H тоді і тільки тоді, коли

$$\sum_{j=0}^{|H|-1} s_{i+j} \geq l (i = 1, \dots, n).$$

4.2. Про число нерозкладних унімономіальних зображень для двозв'язних циклів циклічних p -груп над локальним кільцем характеристики p^s з точністю до еквівалентності

Назвемо послідовність $\bar{x} = (x_1, x_2, \dots, x_n)$ з елементами з довільної множини *двозв'язним циклом*, якщо вона циклічно еквівалентна послідовності вигляду $(a, \dots, a, b, \dots, b)$, де a і b різні елементи присутні в послідовності принаймні один раз кожний.

Нехай K — комутативне локальне кільце, $\text{Rad } K = tK \neq 0$

$$M = M(t^{s_1}, t^{s_2}, \dots, t^{s_n}) = \begin{pmatrix} 0 & \dots & 0 & t^{s_n} \\ t^{s_1} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & t^{s_{n-1}} & 0 \end{pmatrix}$$

канонічно t -циклічна матриця, де $t^{s_i} \neq 0, s_i \geq 0$ ($i = 1, \dots, n$),
 $\bar{w} = (s_1, \dots, s_n) \in$ двозв'язним циклом. Тоді M переставно подібна до $M_1 = M(\bar{w}_1)$, де $\bar{w}_1 = (s', \dots, s', s, \dots, s)$, s', s елементи присутні в послідовності принаймні один раз кожний, $0 \leq s' < s$. Матриця M є

нерозкладна над K тоді і тільки тоді, коли нерозкладною буде матриця $M(t^{s'}, \dots, t^{s'}, t^s, \dots, t^s) = t^{s'} M(1, \dots, 1, t^{s-s'}, \dots, t^{s-s'})$ або, що одне і теж, нерозкладною буде матриця $M(1, \dots, 1, t^{s-s'}, \dots, t^{s-s'})$ після редукції за модулем ідеалу $\text{Ann } t^{s'}$. Зрозуміло $t^{s-s'} \notin \text{Ann } t^{s'}$, $K/\text{Ann } t^{s'}$ комутативне локальне кільце, радикал якого породжується $t + \text{Ann } t^{s'} \neq \text{Ann } t^{s'}$. Таким чином матриця M є нерозкладна над K тоді і тільки тоді, коли матриця $M_2 = M(0, \dots, 0, s, \dots, s)$, де $0, s$ елементи присутні в параметрах принаймні один раз кожний, $0 < s$, після редукції за модулем ідеалу $\text{Ann } t^{s'}$. Остання задача вимагає розгляд нерозкладності матриці $M_3 = M(0, \dots, 0, s, \dots, s)$, де $0, s$ елементи присутні в параметрах принаймні один раз кожний, $t^s \neq 0, s > 0$, над комутативне локальне кільцем K , $\text{Rad } K = tK \neq 0$. Зрозуміло, що для довільних $x, y, z, w \in K$ з умов $x = t^s y$, $t^s z = t^s w$ випливає відповідно $x \equiv 0 \pmod{tK}$, $z \equiv w \pmod{tK}$. Використовуючи останні елементарні зауваження Р. Ф. Цімболинець (Динис) було показано [105], що підкільце кільця $M(n, K)$ тих матриць, які комутують з M_3 локальне, а отже, не містить ідемпотентів X ($X(X - E_n) = 0$) відмінних від E_n та 0 , які завжди існують для розкладної матриці. Звідси одержуємо таку теорему.

Теорема 4.5 ([105]). *Нехай K — комутативне локальне кільце, $\text{Rad } K = tK \neq 0$ канонічно t -циклічна матриця*

$$M = M(t^{s_1}, t^{s_2}, \dots, t^{s_n}) = \begin{pmatrix} 0 & \dots & 0 & t^{s_n} \\ t^{s_1} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & t^{s_{n-1}} & 0 \end{pmatrix},$$

де $s_i \geq 0$ ($i = 1, \dots, n$) є нерозкладна над K , якщо $\bar{w} = (s_1, \dots, s_n)$ є двов'язним циклом.

Застосуємо теорему для побудови нерозкладних зображень скінченних p -груп над комутативним локальним кільцем K характеристики p^s , $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$. Легко бачити, що відображення

$$\Gamma_A: a \rightarrow \Gamma_A(a) = E_n + t^{l-1}A,$$

де E_n — одинична $n \times n$ -матриця над кільцем K , A — довільна $n \times n$ -матриця над кільцем K , є матричним зображенням циклічної нетривіальної циклічної p -групи $H = \langle a \rangle$ над кільцем K . Дійсно в кільці K характеристики p^s число сполучень з p по i , де $1 < i < p$, $C_p^i \in \text{Rad } K = tK$ а $(t^{l-1})^2 = t^{2l-2} = 0$, бо $2l - 2 = l + (l - 2) \geq l$. Тому

$$\begin{aligned} (E_n + t^{l-1}A)^p &= E_n + \sum_{i=1}^{p-1} C_p^i t^{(l-1)i} A^i + t^{(l-1)p} A^p = \\ &= E_n + \sum_{i=1}^{p-1} C_p^i t t^{(l-1)i-1} A^i + t^{(l-1)2} t^{(l-1)(p-2)} A^p = E_n. \end{aligned}$$

Тобто Γ_A є матричним зображенням групи H над кільцем K . З [46] випливає, що потужність нееквівалентних нерозкладних зображень Γ_A фіксованого степеня n не менше ніж потужність $|K/\text{Rad } K|$ поля лишків кільця K . Для доведення використовувалися зображення $\Gamma_{J_n(\lambda)}$, які є нерозкладні і не еквівалентні при різних $\lambda \in K$ за модулем $\text{Rad } K$.

Теорема 4.6. *Нехай K — комутативне локальне кільце характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) = 2$. Тоді для будь-якої циклічної p -групи G і $n \geq |G|$, потужність нееквівалентних нерозкладних унімономіальних зображень фіксованого степеня n не менша, ніж $|G| - 2$.*

Доведення. При $0 < k < n$ відображення $\Lambda_k: a \rightarrow \Lambda_k(a) = E_n + M_k = E_n + M(\underbrace{1, \dots, 1}_k, t, \dots, t) = E_n + M(\bar{w}, \bar{\varepsilon})$, де $\bar{w} = (\underbrace{0, \dots, 0}_k, 1, \dots, 1)$, $\bar{\varepsilon} =$

$(1, \dots, 1)$ є зображенням циклічної групи $G = \langle a \rangle$ над кільцем K якщо $0 < k < |G| - 1 \leq n - 1$. Дійсно при вказаних умовах $n - k \geq 2$ і сума довільних $|G| \geq k + 2$ послідовних елементів послідовності

$$\underbrace{0, \dots, 0}_k, \underbrace{1, \dots, 1}_{n-k}, \underbrace{0, \dots, 0}_k, \underbrace{1, \dots, 1}_{n-k}, \dots$$

буде не менша, ніж 2. За теоремою 4.4 Λ_k є зображенням групи G над кільцем K .

За умовою $0 < k < |G| - 1$ кількість розглядуваних зображень Λ_k дорівнює $|G| - 2$. Зображення Λ_k нерозкладні за теоремою 4.5 та нееквівалентні оскільки M_k має ранг k за модулем $\text{Rad } K = tK$. $\square$

Теорема 4.7. *Нехай K — комутативне локальне кільце характеристики p^s , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$. Тоді для циклічної p -групи G деякого порядку N (отже, і більшого порядку), потужність нееквівалентних нерозкладних унімономіальних зображень фіксованого степеня n не менша, ніж $n - 1$ для будь-якого $n > 1$.*

Доведення. Нехай S — $n \times n$ -матриця над K , яка є нільпотентна за модулем $\text{Rad } K = tK$, тоді $S^n \equiv 0 \pmod{tK}$. Легко бачити, що відображення $\Delta_S : a \rightarrow \Delta_S(a) = E_n + t^{l-2}S$ є зображенням циклічної p -групи $G = \langle a \rangle$ порядку $p^{r-1} > n$, $r > 2$ над кільцем K . Дійсно в кільці K $C_{p^{r-1}}^i \in \text{Rad } K = tK$, де $1 < i < p^{r-1}$. Тому

$$(E_n + t^{l-2}S)^{p^{r-1}} = E_n + \sum_{i=1}^{p^{r-1}-1} C_{p^{r-1}}^i t^{(l-2)i} S^i + t^{(l-2)p^{r-1}} S^{p^{r-1}} = E_n + t^{l-1}S'$$

для деякої $n \times n$ -матриці S' над кільцем K . Тоді

$$(E_n + t^{l-2}S)^{p^r} = (E_n + t^{l-1}S')^p = E_n.$$

Тобто Δ_S є матричним зображенням групи H над кільцем K .

Зображення Δ_S є нерозкладним тоді і тільки, коли є нерозкладною матриця S за модулем ідеалу $\text{Ann } t^{l-2} = \{x \in K \mid t^{m-2}x = 0\} = t^2K$, а зображення Δ_S і $\Delta_{S'}$ еквівалентні тоді і тільки тоді, коли матриці S і S' подібні за модулем t^2K . Розглянемо зображення Δ_{M_k} , $k = 1, 2, \dots, n-1$, що відповідають матрицям $M_k = M(1, \dots, 1, t, \dots, t)$, де 1 зустрічається серед параметрів k разів. Вони нееквівалентні, оскільки M_k має ранг k за модулем $\text{Rad } K = tK$, і є нерозкладними за теоремою 4.5 (з урахуванням що $\text{Rad}(K/\text{Ann } t^{l-2}) = t^2K$ є головним ідеалом K/t^2K , породжений $t + t^2K \neq t^2K$). $\square$

Окремий випадок теореми 4.7 при $n \geq 4$ з висновком, про існування принаймні 3 нееквівалентних нерозкладних матричних зображень отримано раніше здобувачем у [90]. Більш точні оцінки числа нееквівалентних нерозкладних унімономіальних матричних зображень циклічних p -груп над комутативним локальним кільцем характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$, фіксованого степеня n для малих n наведено в наступному підрозділі.

4.3. Про число нерозкладних унімономіальних зображень циклічних p -груп над локальним кільцем характеристики p з точністю до еквівалентності

Легко бачити, що відображення вигляду

$$\Gamma_{\bar{w}, \bar{\varepsilon}}: a \rightarrow \Gamma_{\bar{w}, \bar{\varepsilon}}(a) = E_n + M(\bar{w}, \bar{\varepsilon}) = E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}) \quad (4.4)$$

є нерозкладним унімономіальним зображенням циклічної p -груп $H = \langle a \rangle$ над комутативним локальним кільце K характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$, E_n — одинична $n \times n$ -матриця, $s_i \in \mathbb{N} \cup \{0\}$ і $\varepsilon_i \in K^*$ ($i = 1, \dots, n$) тоді і тільки тоді, коли відображення $\Gamma_{\bar{w}, \bar{\varepsilon}}$ задає зображення групи H і матриця $M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n})$ нерозкладна. Зокрема, відображення вигляду 4.4 є нерозкладним унімономіальним зображенням групи H над кільцем K , якщо

- 1) $\sum_{j=0}^{|H|-1} s_{i+j} \geq l$ ($i = 1, \dots, n$) (теорема 4.4),
- 2) послідовність $\bar{w}$ неперіодична (теорема 1.10).

Крім того, зображення вигляду 4.4 еквівалентні тоді і тільки тоді, коли відповідні матриці $M(\bar{w}, \bar{\varepsilon})$ подібні. Тобто, за теоремою 1.9, коли $\bar{w}$ та $\bar{w}'$ циклічно еквівалентні а елементи $\varepsilon = \prod_{i=1}^n \varepsilon_i$ і $\varepsilon' = \prod_{i=1}^n \varepsilon'_i$ кільця K рівні за модулем $\text{Ann}(t^s)$, де s — найбільший член вагової послідовності $\bar{w}$.

Обчислення неперіодичних послідовностей з точністю до циклічної еквівалентності можна замінити розглядом тільки неперіодичних послідовностей, кожна з яких найменша в лексикографічному порядку серед собі циклічно еквівалентних. Зрозуміло, що число циклічно еквівалентних послідовностей до неперіодичних послідовності рівне її довжині.

З'ясуємо спочатку число $U(l, n)$ неперіодичних послідовностей $\bar{w} = (s_1, s_2, \dots, s_n)$, кожна з яких найменша в лексикографічному порядку серед собі циклічно еквівалентних, де s_i — вага ненульового елемента кільця K , тобто $s_i \in \{0, 1, \dots, l-1\}$ ($i = 1, 2, \dots, n$). Нагадаємо, що послідовність $\bar{x} = (x_1, x_2, \dots, x_n)$ з елементами з довільної множини називається *періодичною*, якщо для деякого натурального $k < n$ $\bar{x} = (x_{k+1}, \dots, x_n, x_1, \dots, x_k)$. В цьому випадку k назвемо періодом по-

слідовності $\bar{x}$.

Лема 4.8. *Найменший період k періодичної послідовності $\bar{x} = (x_1, x_2, \dots, x_n)$ з елементами з довільної множини є дільником n , для довільних $i, j \in \{1, \dots, n\}$ з конгруенції $i \equiv j \pmod{k}$ випливає $x_i = x_j$.*

Доведення. Зрозуміло, що $k < n$, бо $\bar{x}$ володіє деяким періодом меншим за n . Розглянемо клас W послідовностей циклічно еквівалентних $\bar{x}$. На W природно розглянути дію циклічної групи H порядку $|H| = n$, яка перетворить W в одну H -орбіту. Послідовність $\bar{x}$ періодична, тоді і тільки тоді, коли в неї нетривіальний стабілізатор, який, очевидно, буде циклічною підгрупою групи H . А отже, найменший період k послідовності $\bar{x}$ ділить n та довільний інший період послідовності $\bar{x}$. Крім того, з рівності

$$(x_1, x_2, \dots, x_n) = (x_{k+1}, \dots, x_n, x_1, \dots, x_k)$$

одержуємо $x_i = x_j$ для довільних $i, j \in \{1, \dots, n\}$ таких, що $i - j = k$. Після припущення $i > j$, що не обмежує загальність, індукцією за $i - j$ легко показати, що $x_i = x_j$ для довільних $i, j \in \{1, \dots, n\}$ таких, що $i \equiv j \pmod{k}$. $\square$

Таким чином, в одному класі циклічно еквівалентних неперіодичних послідовностей є рівно n послідовностей, оскільки будь-які різні циклічні зсуви послідовності $(s_1, \dots, s_n)$ генерують відмінні послідовності.

Очевидно, $U(2, 6)$ є числом неперіодичних послідовностей $\bar{w} = (s_1, s_2, s_3, s_4, s_5, s_6)$ $s_i \in \{0, 1\}$ ($i = 1, 2, \dots, 6$), що $\bar{w}$ — найменша в лексикографічному порядку серед їй циклічно еквівалентних. Тоді, очевидно $s_1 = 0, s_6 = 1$. Перебір таких послідовностей дасть

$$(0, 0, 0, 0, 0, 1), (0, 0, 0, 0, 1, 1), (0, 0, 0, 1, 0, 1), (0, 0, 0, 1, 1, 1), (0, 0, 1, 0, 1, 1),$$

$$(0, 0, 1, 1, 1, 1), (0, 0, 1, 1, 0, 1), (0, 1, 0, 1, 1, 1), (0, 1, 1, 1, 1, 1).$$

Таким чином $U(2, 6) = 9$.

При $l = 2$, $n = 6$ число $U(l, n)$ також можна обчислити, наприклад, серією команд, яка наведена в додатку А.1, системи GAP 4.10.1.

Зокрема, для порівняння з проведеними обчисленнями наведемо результати обчислення $U(l, n)$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$l = 2$	1	2	3	6	9	18	30
$l = 3$	3	8	18	48	116	312	810
$l = 4$	6	20	60	204	670	2340	8160
$l = 5$	10	40	150	624	2580	11160	48750
$l = 6$	15	70	315	1554	7735	39990	209790
$l = 7$	21	112	588	3360	19544	117648	720300
$l = 8$	28	168	1008	6552	43596	299592	2096640

З'ясуємо число нерозкладних матриць $M(\overline{w}, \overline{\varepsilon})$ з точністю до подібності над скінченним комутативним локальним кільцем K довжини $l > 1$.

Лема 4.9. *Нехай K — комутативне локальне кільце, радикал якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l > 1$. Кільце K скінченне тоді і тільки тоді, коли поле лишків $K/\text{Rad } K$ кільця K скінченне. Крім того, в останньому випадку $|t^i K/t^j K| = k^{j-i}$ ($0 \leq i < j \leq l$), зокрема, $|K| = k^l$, $|K/t^j K| = k^j$ ($0 < j \leq l$), де $k = |K/\text{Rad } K|$.*

Доведення. Необхідність очевидна. Нехай поле лишків $K/\text{Rad } K$ кільця K скінченне, $|K/\text{Rad } K| = k$. Якщо $0 \leq i < l$, то $\varphi: x \rightarrow t^i x/t^{i+1} K$ є гомоморфізмом адитивних груп $\varphi: K \rightarrow t^i K/t^{i+1} K$ з ядром $\text{Rad } K = tK$ і, зокрема, $|t^i K/t^{i+1} K| = |K/\text{Rad } K| = k$. Крім того, якщо $0 \leq i < j \leq l$,

то $|t^i K / t^j K| = |t^i K / t^{i+1} K| \cdot |t^{i+1} K / t^{i+2} K| \cdots |t^{j-1} K / t^j K| = \underbrace{k \cdot k \cdots k}_{j-i} = k^{j-i}$.

Звідси $|K| = |K / \{0\}| = |t^0 K / t^l K| = k^{l-0} = k^l$, $|K / t^j K| = |t^0 K / t^j K| = k^{j-0} = k^j$. $\square$

З'ясуємо тепер число нерозкладних матриць $M(\bar{w}, \bar{\varepsilon})$ порядку $n > 1$ розглядуваних з точністю до подібності над скінченним локальним кільцем K довжини $l > 1$ з порядком $k = |K / \text{Rad } K|$ поля лишків кільця K . Враховуючи теорему 1.10 це число буде не менше числа $V(k, l, n)$ матриць $M(\bar{w}, \bar{\varepsilon})$ з точністю до подібності над кільцем K з неперіодичними ваговими послідовностями $\bar{w}$. Але неперіодичною буде і будь-яка послідовність отримана з $\bar{w}$ циклічним зсувом. Тому всі матриці $M(\bar{w}', \bar{\varepsilon}')$ з послідовністю $\bar{w}'$ циклічно еквівалентною $\bar{w}$ теж нерозкладні. З теореми 1.9 випливає, що всіх матриць $M(\bar{w}', \bar{\varepsilon}')$ з точністю до подібності з послідовністю $\bar{w}'$ циклічно еквівалентною $\bar{w}$ є стільки скільки є значень $\varepsilon_1 \varepsilon_2 \cdots \varepsilon_n$ з точністю до конгруентності за модулем $\text{Ann}(t^s)$, де s — найбільший елемент вагової послідовності $\bar{w}$. Очевидно, $\varepsilon_1 \varepsilon_2 \cdots \varepsilon_n$ може бути довільним оборотним елементом у кільці K . Тому число матриць $M(\bar{w}', \bar{\varepsilon}')$ з точністю до подібності з послідовністю $\bar{w}'$ циклічно еквівалентною фіксованій неперіодичній послідовності $\bar{w}$ рівне

$$|(K / \text{Ann}(t^s)) \setminus (tK / \text{Ann}(t^s))| = |(K / t^{l-s} K) \setminus (tK / t^{l-s} K)| = k^{l-s} - k^{l-s-1} = (k-1) k^{l-s-1}.$$

Очевидно, $V(k, 4, 3)$ є числом послідовностей $(s_1, s_2, s_3, \varepsilon)$, де $s_i \in \{0, 1, 2, 3\}$ ($i = 1, 2, 3$), ε належить множині оборотних представників всіх різних суміжних класів $K / \text{Ann}(t^s) = K / t^{4-s} K$ ($s = \max(s_1, s_2, s_3)$), $\bar{w} = (s_1, s_2, s_3)$ — неперіодична послідовність, найменша в лексикографічному порядку серед її циклічно еквівалентних. Оскільки за лемою

4.8 період періодичної послідовності ділить її довжину а 3 просте число, то $\overline{w}$ є неперіодичною тоді і тільки тоді, коли містить принаймні 2 різні елементи. Якщо $\overline{w}$ найменша в лексикографічному порядку серед її циклічно еквівалентних, то $s_1 = \min(s_1, s_2, s_3)$. Перебір таких послідовностей $(s_1, s_2, s_3, \varepsilon)$ разом з s та кількістю варіантів для ε дасть.

$$(0, 0, 1, \varepsilon)\text{-}1\text{--}(k-1)k^2, \quad (0, 1, 1, \varepsilon)\text{-}1\text{--}(k-1)k^2, \quad (0, 0, 2, \varepsilon)\text{-}2\text{--}(k-1)k,$$

$$(0, 1, 2, \varepsilon)\text{-}2\text{--}(k-1)k, \quad (0, 2, 1, \varepsilon)\text{-}2\text{--}(k-1)k, \quad (0, 2, 2, \varepsilon)\text{-}2\text{--}(k-1)k,$$

$$(1, 1, 2, \varepsilon)\text{-}2\text{--}(k-1)k, \quad (1, 2, 2, \varepsilon)\text{-}2\text{--}(k-1)k, \quad (0, 0, 3, \varepsilon)\text{-}3\text{--}(k-1),$$

$$(0, 1, 3, \varepsilon)\text{-}3\text{--}(k-1), \quad (0, 2, 3, \varepsilon)\text{-}3\text{--}(k-1), \quad (0, 3, 1, \varepsilon)\text{-}3\text{--}(k-1),$$

$$(0, 3, 2, \varepsilon)\text{-}3\text{--}(k-1), \quad (0, 3, 3, \varepsilon)\text{-}3\text{--}(k-1), \quad (1, 1, 3, \varepsilon)\text{-}3\text{--}(k-1),$$

$$(1, 2, 3, \varepsilon)\text{-}3\text{--}(k-1), \quad (1, 3, 2, \varepsilon)\text{-}3\text{--}(k-1), \quad (1, 3, 3, \varepsilon)\text{-}3\text{--}(k-1),$$

$$(2, 2, 3, \varepsilon)\text{-}3\text{--}(k-1), \quad (2, 3, 3, \varepsilon)\text{-}3\text{--}(k-1).$$

Таким чином $V(k, 4, 3) = (k-1)(2k^2 + 6k + 12) = 2k^3 + 4k^2 + 6k - 12$.

число $V(k, l, n)$ також можна обчислити, наприклад, серією команд, яка наведена в додатку А.1, системи GAP 4.10.1.

В результаті обчислень також одержуємо $V(k, 4, 3) = 2k^3 + 4k^2 + 6k - 12$. Тут подано обчислення $V(k, l, n)$ при деяких значеннях l, n .

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
$l = 2$	$k - 1$	$2k - 2$	$3k - 3$	$6k - 6$	$9k - 9$
$l = 3$	$k^2 + k - 2$	$2k^2 + 4k - 6$	$3k^2 + 12k - 15$	$6k^2 + 36k - 42$	$9k^2 + 98k - 107$
$l = 4$	$k^3 + k^2 + k - 3$	$2k^3 + 4k^2 + 6k - 12$	$3k^3 + 12k^2 + 27k - 42$	$6k^3 + 36k^2 + 114k - 156$	$9k^3 + 98k^2 + 447k - 554$
$l = 5$	$k^4 + k^3 + k^2 + k - 4$	$2k^4 + 4k^3 + 6k^2 + 8k - 20$	$3k^4 + 12k^3 + 27k^2 + 48k - 90$	$6k^4 + 36k^3 + 114k^2 + 264k - 420$	$9k^4 + 98k^3 + 447k^2 + 1356k - 1910$
$l = 6$	$k^5 + k^4 + k^3 + k^2 + k - 5$	$2k^5 + 4k^4 + 6k^3 + 8k^2 + 10k - 30$	$3k^5 + 12k^4 + 27k^3 + 48k^2 + 75k - 165$	$6k^5 + 36k^4 + 114k^3 + 264k^2 + 510k - 930$	$9k^5 + 98k^4 + 447k^3 + 1356k^2 + 3245k - 5155$

Можливості системи дозволяють також обчислювати громіздкі значення $V(k, l, n)$, які не наводимо в таблиці, наприклад, $V(k, 7, 8) = 30k^6 + 750k^5 + 6570k^4 + 33240k^3 + 120450k^2 + 349470k - 510510$.

З'ясуємо тепер число нерозкладних модулярних зображень з точністю до еквівалентності циклічної p -груп над скінченним комутативним локальним кільцем K головних ідеалів характеристики p .

Відображення

$$\Gamma_{\bar{w}, \bar{\varepsilon}}: a \rightarrow \Gamma_{\bar{w}, \bar{\varepsilon}}(a) = E_n + M(\bar{w}, \bar{\varepsilon}) = E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}) \quad (4.5)$$

є нерозкладним унімономіальним зображенням p -групи $H = \langle a \rangle$ порядку $|H| = m > 1$ над комутативним локальним кільцем K характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$, E_n — одинична $n \times n$ -матриця, $s_i \in \mathbb{N} \cup \{0\}$ і $\varepsilon_i \in K^*$ ($i = 1, \dots, n$) якщо

1) $\sum_{j=0}^{|H|-1} s_{i+j} \geq l$ ($i = 1, \dots, n$) (теорема 4.4),

2) послідовність $\bar{w}$ неперіодична (теорема 1.10).

Крім того, за теоремою 1.9 два зображення вигляду (4.5) є еквівалентними над кільцем K тоді і тільки тоді, коли відповідні $\bar{w}$ циклічно еквівалентні а добутки елементів відповідних $\bar{\varepsilon}$ конгруентні за модулем $\text{Ann}(t^s)$, де s — найбільший член вагової довільної з циклічно еквівалентних послідовностей $\bar{w}$.

Таким чином число зображень вигляду (4.5) у випадку, коли m є деяким степенем простої характеристики p кільця K , не менше числа $W(k, l, m, n)$ послідовностей $(s_1, s_2, \dots, s_n, \varepsilon)$, $s_i \in \{0, 1, \dots, l-1\}$, $\sum_{j=0}^{m-1} s_{i+j} \geq l$ ($i = 1, 2, \dots, n$), таких, що ε належить множині оборотних представників всіх різних суміжних класів $K/\text{Ann}(t^s) = K/t^{l-s}K$ ($s = \max(s_1, s_2, \dots, s_n)$), $\bar{w} = (s_1, s_2, \dots, s_n)$ — неперіодична послідовність, найменша в лексикографічному порядку серед її циклічно еквівалентних. (Для зручності ми знаходитимемо $W(k, l, m, n)$ і у випадку, коли m не є степенем жодного простого числа.)

Очевидно, $W(k, 4, 2, 3)$ є числом послідовностей $(s_1, s_2, s_3, \varepsilon)$, де $s_i \in \{0, 1, 2, 3\}$ ($i = 1, 2, 3$), $s_1 + s_2 \geq 4$, $s_2 + s_3 \geq 4$, $s_3 + s_1 \geq 4$, ε належить множині оборотних представників всіх різних суміжних класів $K/\text{Ann}(t^s) = K/t^{4-s}K$ ($s = \max(s_1, s_2, s_3)$), $\bar{w} = (s_1, s_2, s_3)$ містить принаймні 2 різні елементи. Якщо $\bar{w}$ найменша в лексикографічному порядку серед її циклічно еквівалентних, то $s_1 = \min(s_1, s_2, s_3)$. Перебір таких послідовностей $(s_1, s_2, s_3, \varepsilon)$ разом з s та кількістю варіантів для ε дасть $(1, 3, 3, \varepsilon)$ -3-($k-1$), $(2, 2, 3, \varepsilon)$ -3-($k-1$), $(2, 3, 3, \varepsilon)$ -3-($k-1$). Таким чином $W(k, 4, 2, 3) = 3k - 3$.

Число $W(k, l, m, n)$ також можна обчислити, наприклад, серією команд, яка наведена в додатку A.1, системи GAP 4.10.1. В результаті обчислень також одержуємо $W(k, 4, 2, 3) = 3k - 3$. В таблицях A.1–A.9 наведено результати обчислень при деяких значеннях m та n і відповідно для $l = 2, \dots, 10$.

Зокрема, для порівняння з проведеними обчисленнями наведемо результати обчислення $W(k, 4, m, n)$ при деяких значеннях m, n .

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
$m = 2$	$2k - 2$	$3k - 3$	$5k - 5$	$11k - 11$	$19k - 19$
$m = 3$	$k^2 + k - 2$	$3k^2 + 8k - 11$	$3k^2 + 21k - 24$	$5k^2 + 63k - 68$	$7k^2 + 186k - 193$
$m = 4$	$2k^2 + k - 3$	$3k^2 + 8k - 11$	$11k^2 + 30k - 41$	$19k^2 + 104k - 123$	$34k^2 + 354k - 388$
$m = 5$	$2k^2 + k - 3$	$5k^2 + 6k - 11$	$11k^2 + 30k - 41$	$k^3 + 36k^2 + 118k - 155$	$k^3 + 68k^2 + 432k - 501$

4.4. Про число нерозкладних унімономіальних зображень циклічних p -груп над локальним кільцем характеристики p з точністю до $*$ -еквівалентності

В модулярному випадку часто серію нееквівалентних нерозкладних матричних зображень можна отримати з одного додаючи у вигляді деяких елементів матриць наявність оборотного множника. В підрозділі пропонується строгий підхід до абстрагування від таких множників при оцінці потужності нееквівалентних нерозкладних матричних зображень циклічної p -групи над комутативним локальним кільцем K характеристики

p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$. Це дає змогу деякого аналізу потужності побудованих нееквівалентних нерозкладних матричних зображень, навіть, коли поле його лишків нескінченне. Підкреслимо, що вивчення матриць чи матричних зображень з точністю до спеціальних (не класичних) еквівалентностей виникають при дослідженні різних задач (див., наприклад, [45, 68, 95]).

Означення 4.10. Назвемо $n \times n$ -матрицю A над кільцем K $*$ -подібну до $n \times n$ -матриці B над тим же кільцем, якщо $A = P^{-1} \text{diag}(\delta_1, \dots, \delta_n) B \text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P$, для деякої підстановочної матриці порядку n над кільцем K та $\delta_i \in K^*$ ($i = 1, \dots, 2n$). В іншому випадку матрицю A назвемо $*$ -неподібною матриці B .

Покажемо, що відношення $*$ -подібності є відношенням еквівалентності. Дійсно, одинична матриця E_n порядку n над кільцем K є і підстановочною матрицею $E_n = P_e$ тотожної підстановки e n -го степеня і діагональною матрицею $E_n = \text{diag}(1, \dots, 1)$ з n одиницями на діагоналі. Тому для довільної $n \times n$ -матриці A над кільцем K

$$P_e^{-1} \text{diag}(1, \dots, 1) A \text{diag}(1, \dots, 1) P_e = E_n^{-1} E_n A E_n E_n = A.$$

Тому A $*$ -подібна до A і $*$ -подібність є рефлексивним відношенням.

Очевидно,

$$\text{diag}(\delta_1, \dots, \delta_n) P_\varphi = P_\varphi \text{diag}(\delta_{\varphi(1)}, \dots, \delta_{\varphi(n)}), \quad (4.6)$$

де P_φ — підстановочна матриця підстановки n -го степеня φ , $\delta_i \in K^*$ ($i = 1, \dots, n$). Якщо $n \times n$ -матриця A над кільцем K $*$ -подібна до $n \times n$ -матриці B над тим же кільцем, то

$$A = P_\varphi^{-1} \text{diag}(\delta_1, \dots, \delta_n) B \text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P_\varphi,$$

для деякої підстановочної матриці P_φ підстановки n -го степеня φ , та $\delta_i \in K^*$ ($i = 1, \dots, 2n$). Тоді

$$\begin{aligned} P_\varphi A P_\varphi^{-1} &= \text{diag}(\delta_1, \dots, \delta_n) B \text{diag}(\delta_{n+1}, \dots, \delta_{2n}), \\ \text{diag}(\delta_1^{-1}, \dots, \delta_n^{-1}) P_\varphi A P_\varphi^{-1} \text{diag}(\delta_{n+1}^{-1}, \dots, \delta_{2n}^{-1}) &= B, \\ \text{diag}(\delta_1^{-1}, \dots, \delta_n^{-1}) P_\varphi A (\text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P_\varphi)^{-1} &= B. \end{aligned}$$

Враховуючи 4.6 одержимо

$$\begin{aligned} P_\varphi \text{diag}(\delta_{\varphi(1)}^{-1}, \dots, \delta_{\varphi(n)}^{-1}) A (P_\varphi \text{diag}(\delta_{n+\varphi(1)}, \dots, \delta_{n+\varphi(n)}))^{-1} &= B, \\ P_{\varphi^{-1}}^{-1} \text{diag}(\delta_{\varphi(1)}^{-1}, \dots, \delta_{\varphi(n)}^{-1}) A \text{diag}(\delta_{n+\varphi(1)}^{-1}, \dots, \delta_{n+\varphi(n)}^{-1}) P_{\varphi^{-1}} &= B. \end{aligned}$$

Тому матриця B $*$ -подібними до A і $*$ -подібність є симетричним відношенням.

Якщо $n \times n$ -матриця A над кільцем K $*$ -подібними до $n \times n$ -матриці B над тим же кільцем а матриця B $*$ -подібними до $n \times n$ -матриці C над тим же кільцем, то

$$\begin{aligned} A &= P_\varphi^{-1} \text{diag}(\delta_1, \dots, \delta_n) B \text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P_\varphi, \\ B &= P_\psi^{-1} \text{diag}(\delta_{2n+1}, \dots, \delta_{3n}) C \text{diag}(\delta_{3n+1}, \dots, \delta_{4n}) P_\psi, \end{aligned}$$

для деяких підстановочних матриці P_φ , P_ψ підстановок n -го степеня φ , ψ відповідно та $\delta_i \in K^*$ ($i = 1, \dots, 4n$). Тоді

$$\begin{aligned} A &= P_\varphi^{-1} \text{diag}(\delta_1, \dots, \delta_n) P_\psi^{-1} \text{diag}(\delta_{2n+1}, \dots, \delta_{3n}) C \times \\ &\quad \text{diag}(\delta_{3n+1}, \dots, \delta_{4n}) P_\psi \text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P_\varphi. \\ A &= P_\varphi^{-1} \text{diag}(\delta_1, \dots, \delta_n) P_{\psi^{-1}} \text{diag}(\delta_{2n+1}, \dots, \delta_{3n}) C \times \\ &\quad \text{diag}(\delta_{3n+1}, \dots, \delta_{4n}) P_\psi \text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P_\varphi. \end{aligned}$$

Враховуючи 4.6 одержимо

$$\begin{aligned}
 A &= P_\varphi^{-1} P_{\psi^{-1}} \operatorname{diag}(\delta_{\psi^{-1}(1)}, \dots, \delta_{\psi^{-1}(n)}) \operatorname{diag}(\delta_{2n+1}, \dots, \delta_{3n}) C \times \\
 &\quad \operatorname{diag}(\delta_{3n+1}, \dots, \delta_{4n}) \left(\operatorname{diag}(\delta_{n+1}^{-1}, \dots, \delta_{2n}^{-1}) P_{\psi^{-1}} \right)^{-1} P_\varphi = \\
 &\quad (P_\psi P_\varphi)^{-1} \operatorname{diag}(\delta_{\psi^{-1}(1)} \delta_{2n+1}, \dots, \delta_{\psi^{-1}(n)} \delta_{3n}) C \times \\
 &\quad \operatorname{diag}(\delta_{3n+1}, \dots, \delta_{4n}) \left(P_{\psi^{-1}} \operatorname{diag}(\delta_{n+\psi^{-1}(1)}^{-1}, \dots, \delta_{n+\psi^{-1}(n)}^{-1}) \right)^{-1} P_\varphi = \\
 &\quad (P_{\psi\varphi})^{-1} \operatorname{diag}(\delta_{\psi^{-1}(1)} \delta_{2n+1}, \dots, \delta_{\psi^{-1}(n)} \delta_{3n}) C \times \\
 &\quad \operatorname{diag}(\delta_{3n+1}, \dots, \delta_{4n}) \operatorname{diag}(\delta_{n+\psi^{-1}(1)}, \dots, \delta_{n+\psi^{-1}(n)}) P_\psi P_\varphi = \\
 &\quad (P_{\psi\varphi})^{-1} \operatorname{diag}(\delta_{\psi^{-1}(1)} \delta_{2n+1}, \dots, \delta_{\psi^{-1}(n)} \delta_{3n}) C \times \\
 &\quad \operatorname{diag}(\delta_{3n+1} \delta_{n+\psi^{-1}(1)}, \dots, \delta_{4n} \delta_{n+\psi^{-1}(n)}) P_{\psi\varphi}.
 \end{aligned}$$

Тому матриця A $*$ -подібними до C і $*$ -подібність є транзитивним відношенням. Отже, $*$ -подібність є відношенням еквівалентності.

Зрозуміло, що подібні матриці не обов'язково $*$ -подібні і навпаки.

Лема 4.11. *Клітки жордана $J_n(\lambda_1)$ та $J_n(\lambda_2)$ порядку n з відповідно елементами $\lambda_1, \lambda_2 \in K$ на головній діагоналі $*$ -подібні тоді і тільки тоді, коли елементи λ_1, λ_2 асоційовані в кільці K (тобто відрізняються оборотним множником).*

Доведення. Дійсно, якщо $\lambda = \varepsilon t^s$, де $\varepsilon \in K^*$ і $0 \leq s \leq l(\operatorname{Rad} K)$, то маємо серію $*$ -подібних матриць

$$J_n(\lambda) = J_n(\varepsilon t^s) = \begin{pmatrix} \varepsilon t^s & 1 & 0 & \dots & 0 \\ 0 & \varepsilon t^s & 1 & \dots & 0 \\ 0 & 0 & \varepsilon t^s & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \varepsilon t^s \end{pmatrix} \sim \begin{pmatrix} t^s & \varepsilon^{-1} & 0 & \dots & 0 \\ 0 & \varepsilon t^s & 1 & \dots & 0 \\ 0 & 0 & \varepsilon t^s & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \varepsilon t^s \end{pmatrix} \sim$$

$$\begin{aligned}
& \sim \begin{pmatrix} t^s & 1 & 0 & \dots & 0 \\ 0 & \varepsilon^2 t^s & 1 & \dots & 0 \\ 0 & 0 & \varepsilon t^s & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \varepsilon t^s \end{pmatrix} \sim \dots \sim \begin{pmatrix} t^s & 1 & 0 & \dots & 0 \\ 0 & t^s & 1 & \dots & 0 \\ 0 & 0 & t^s & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \varepsilon^n t^s \end{pmatrix} \sim \\
& \begin{pmatrix} t^s & 1 & 0 & \dots & 0 \\ 0 & t^s & 1 & \dots & 0 \\ 0 & 0 & t^s & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & t^s \end{pmatrix} = J_n(t^s).
\end{aligned}$$

При різних s ($0 \leq s \leq l(\text{Rad } K)$) клітки жордана $J_n(t^s)$ не є $*$ -подібні. Дійсно, якщо $0 \leq s_1 < s_2 \leq l(\text{Rad } K)$ $J_n(t^{s_1}) = P^{-1} \text{diag}(\delta_1, \dots, \delta_n) J_n(t^{s_2}) \text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P$, для деякої підстановочної матриці P порядку n над кільцем K та $\delta_i \in K^*$ ($i = 1, \dots, 2n$), то $P J_n(t^{s_1}) P^{-1} = \text{diag}(\delta_1, \dots, \delta_n) J_n(t^{s_2}) \text{diag}(\delta_{n+1}, \dots, \delta_{2n})$ є верхньотрикутною матрицею. Оскільки $P J_n(t^{s_1}) P^{-1} = P(t^{s_1} E_n + J_n(0)) P^{-1} = E_n + P J_n(0) P^{-1} E_n$, то $P J_n(0) P^{-1}$ є також верхньотрикутною матрицею (тут E_n — одинична $n \times n$ -матриця). Нехай P — підстановочна матриця підстановки φ , e_i — стовпчик висоти n , з єдиним ненульовим елементом у i -товій позиції, який рівний 1 ($i = 1, \dots, n$) та $2 \leq j \leq n$. Тоді

$$P J_n(0) P^{-1} e_{\varphi(j)} = P J_n(0) e_j P^{-1} = P e_{j-1} J_n(0) P^{-1} = e_{\varphi(j-1)} P J_n(0) P^{-1}.$$

Так-як матриця $P J_n(0) P^{-1}$ верхньотрикутна, то $\varphi(j-1) \leq \varphi(j)$ ($j = 2, \dots, n$). Отже, не спадна підстановка φ тотожна, а $P = E_n$. Але, тоді, $J_n(t^{s_1}) = \text{diag}(\delta_1, \dots, \delta_n) J_n(t^{s_2}) \text{diag}(\delta_{n+1}, \dots, \delta_{2n})$ і $t^{s_1} = \delta_1 t^{s_2} \delta_{n+1}$, що неможливо. $\square$

Добре відомо, що жорданові клітки $J_n(\lambda)$ при різних значеннях λ над областю цілісності K не є подібні. Однак, при асоційованих значеннях і тільки при них вони $*$ -подібні. Тобто при різних але асоційованих значеннях λ відповідні клітки $J_n(\lambda)$ не є подібні але є $*$ -подібні. Зауважимо, що над довільним кільцем K жорданові клітки $J_n(\lambda)$ при різних значеннях λ можуть бути подібні. Так якщо 2 — характеристика кільцем K в якому $t \neq 0$, $t^2 = 0$, то $J_n(t)$ подібна $J_n(0)$. Дійсно

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} J_n(t) \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \begin{pmatrix} t & 1 \\ 0 & t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \\ \begin{pmatrix} t & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = J_n(0).$$

Над цим же кільцем K $J_n(t)$ та $J_n(0)$ не є $*$ -подібні, бо t та 0 неасоційовні.

Лема 4.12. Матриці $M = M(\bar{w}, \bar{\varepsilon})$ і $M' = M(\bar{w}', \bar{\varepsilon}')$, де $\bar{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_{n-1}, \varepsilon_n)$, $\bar{\varepsilon}' = (\varepsilon'_1, \dots, \varepsilon'_{n-1}, \varepsilon'_n)$ $*$ -подібні тоді і лише тоді, коли $\bar{w}$ та $\bar{w}'$ циклічно еквівалентні.

Доведення. Достатність. Припустимо, що $\bar{w}$ та $\bar{w}'$ є циклічно еквівалентними. Зразу з означення 4.10 маємо $*$ -подібність матриці $M = M(\bar{w}, \bar{\varepsilon}) = M(t^{s_1}, \dots, t^{s_n}) \cdot \text{diag}[\varepsilon_1, \dots, \varepsilon_n] \sim M(t^{s_1}, \dots, t^{s_n}) = M(\bar{w}, (1, \dots, 1))$, де $\bar{w} = (s_1, s_2, \dots, s_n)$. Аналогічно також $M' = M(\bar{w}', \bar{\varepsilon}') \sim M(\bar{w}', (1, \dots, 1))$, де $\bar{w}' = (s'_1, s'_2, \dots, s'_n)$. За твердженням 1.8, коли $\bar{w}$ та $\bar{w}'$ є циклічно еквівалентними, то $M(\bar{w}, (1, \dots, 1)) = M(t^{s_1}, \dots, t^{s_n})$ та $M(\bar{w}', (1, \dots, 1)) = M(t^{s'_1}, \dots, t^{s'_n})$ переставно подібні, тобто для деякої підстановочної матриці P порядку n над кільцем K маємо $M(t^{s_1}, \dots, t^{s_n}) = P^{-1}M(t^{s'_1}, \dots, t^{s'_n})P$. Тоді $M(\bar{w}, (1, \dots, 1))$ та $M(\bar{w}', (1, \dots, 1))$ $*$ -подібні, а отже, M та M' є $*$ -подібними.

Необхідність. Нехай M та M' $*$ -подібні. Як і раніше, це еквівалентне тому, що $M(\bar{w}, (1, \dots, 1))$ та $M(\bar{w}', (1, \dots, 1))$ $*$ -подібні також, і $M(\bar{w}, (1, \dots, 1)) = P^{-1} \text{diag}(\delta_1, \dots, \delta_n) M(\bar{w}', (1, \dots, 1)) \text{diag}(\delta_{n+1}, \dots, \delta_{2n}) P$ для деякої підстановочної матриці P порядку n над кільцем K та $\delta_i \in K^*$ ($i = 1, \dots, 2n$). Тоді

$$M(\bar{w}, (1, \dots, 1)) = P^{-1} \text{diag}(\delta_1, \dots, \delta_n) M(\bar{w}', (\delta_{n+1}, \dots, \delta_{2n})) P = \\ P^{-1} M(\bar{w}', (\delta_1 \delta_{n+1}, \dots, \delta_n \delta_{2n}, \delta_1 \delta_{2n})) P$$

Але, тоді, $M(\bar{w}, (1, \dots, 1))$ та $M(\bar{w}', (\delta_1 \delta_{n+1}, \dots, \delta_n \delta_{2n}, \delta_1 \delta_{2n}))$ подібні і за теоремою 1.9 $\bar{w}$ та $\bar{w}'$ циклічно еквівалентні. $\square$

З теореми 1.9 випливає, що подібні матриці $M = M(\bar{w}, \bar{\varepsilon}) \in *$ -подібні. Крім того, $*$ -подібні матриці $M = M(\bar{w}, \bar{\varepsilon})$ та $M' = M(\bar{w}', \bar{\varepsilon}')$ є подібними тоді і тільки тоді, коли елементи $\varepsilon = \varepsilon_1 \cdots \varepsilon_{n-1} \varepsilon_n$ та $\varepsilon' = \varepsilon'_1 \cdots \varepsilon'_{n-1} \varepsilon'_n$ кільця K конгруентні за модулем $\text{Ann}(t^s)$, де s — найбільший член вагової послідовності $\bar{w} = (s_1, s_2, \dots, s_n)$. Тому потужність множини матриць заданого вигляду, що $*$ -подібні матриці $M = M(\bar{w}, \bar{\varepsilon})$, яка розглядається з точністю до подібності рівна $|K / \text{Ann}(t^s)| - |R / \text{Ann}(t^s)| = |K / t^{l(\text{Rad } K) - s} K| - |R / t^{l(\text{Rad } K) - s} K|$ і є не менша ніж потужність $|K / \text{Rad } K| - |R / \text{Rad } K| = |K / \text{Rad } K| - 1$ мультиплікативної групи поля лишків кільця K .

За теоремою 1.10 якщо послідовність $\bar{w}$ — неперіодична, то матриця $M(\bar{w}, \bar{\varepsilon})$ нерозкладна. Але неперіодичною буде і довільна послідовність $\bar{w}'$ отримана з $\bar{w}$ циклічним зсувом. Тому всі матриці $M(\bar{w}', \bar{\varepsilon}')$ $*$ -подібні матриці $M(\bar{w}, \bar{\varepsilon})$ теж нерозкладні.

З'ясуємо потужність множини нерозкладних матриць $M(\bar{w}, \bar{\varepsilon})$ розглядувану з точністю до $*$ -подібності з неперіодичною ваговою послі-

довність $\bar{w}$ над комутативним локальним кільцем K довжини $l = l(\text{Rad } K) > 1$. Очевидно, вона скінченна і рівна числу $U(l, n)$ класів циклічно еквівалентних неперіодичних послідовностей $\bar{w} = (s_1, s_2, \dots, s_n)$, де s_i — вага ненульового елемента кільця K , тобто $s_i \in \{0, 1, \dots, l - 1\}$ ($i = 1, 2, \dots, n$). Це число вже знаходилося програмними засобами серією команд, яка наведена в додатку А.1, системи GAP 4.10.1.

Для числа $U(l, n)$, однак, можна вивести аналітичну формулу. Нехай спочатку для простоти $n = q^r$, де q — просте число, $r > 0$. Тоді

$$U(l, n) = U(l, q^r) = \left(l^{q^r} - \sum_{i=0}^{r-1} q^i \cdot U(l, q^i) \right) / q^r$$

або

$$\sum_{i=0}^r q^i \cdot U(l, q^i) = l^{q^r}.$$

$$\text{Отже, } U(l, n) = U(l, q^r) = l^{q^r} - l^{q^{r-1}}.$$

Теорема 4.13. *Нехай $n = q_1^{r_1} q_2^{r_2} \dots q_m^{r_m}$, де q_i — різні прості числа, $r_i > 0$ ($i = 1, \dots, m$). Число класів $*$ -подібних нерозкладних матриць $M(\bar{w}, \bar{\varepsilon})$ з неперіодичною ваговою послідовністю $\bar{w}$ над комутативним локальним кільцем K довжини $l = l(\text{Rad } K)$ скінченне і рівне*

$$\left(l^n + \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} (-1)^k l^{\frac{n}{q_{i_1} q_{i_2} \dots q_{i_k}}} \right) / n.$$

Доведення. Зауважмо, що довільна матриця $M(\bar{w}, \bar{\varepsilon})$ з неперіодичною ваговою послідовністю $\bar{w}$ нерозкладна а число класів $*$ -подібних таких нерозкладних матриць скінченне і рівна числу $U(l, n)$ класів циклічно еквівалентних неперіодичних послідовностей $\bar{w} = (s_1, s_2, \dots, s_n)$, де $s_i \in \{0, 1, \dots, l - 1\}$ ($i = 1, \dots, n$). Розглянемо множини P_x всіх періодичних послідовностей з періодом x . Будь-яка періодична послідовність довжини

n з елементами з множини $\{0, 1, \dots, l-1\}$ має період менший за n , що є дільником n . Тому вона належить принаймні одній множині $P_{\frac{n}{q_i}}$ ($i = 1, \dots, m$). Отже,

$$n \cdot U(l, n) = l^n - |\cup_{i=1}^m P_{\frac{n}{q_i}}|.$$

Оскільки $|P_x| = l^x$, $P_x \cap P_y = P_{(x,y)}$, то за формулою включень-виключень

$$n \cdot U(l, n) = l^n + \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} (-1)^k |P_{\frac{n}{q_{i_1}}} \cap P_{\frac{n}{q_{i_2}}} \cap \dots \cap P_{\frac{n}{q_{i_k}}}| =$$

$$l^n + \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} (-1)^k |P_{\frac{n}{q_{i_1} q_{i_2} \dots q_{i_k}}}| = l^n + \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} (-1)^k l^{\frac{n}{q_{i_1} q_{i_2} \dots q_{i_k}}}.$$

Отже,

$$U(l, n) = \left(l^n + \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq m} (-1)^k l^{\frac{n}{q_{i_1} q_{i_2} \dots q_{i_k}}} \right) / n. \quad \square$$

При $l = 3$, $n = 12 = 2^2 \cdot 3^1$ одержуємо

$$U(3, 12) = \frac{3^{12} - 3^{\frac{12}{2}} - 3^{\frac{12}{3}} + 3^{\frac{12}{6}}}{12} = \frac{3^{12} - 3^6 - 3^4 + 3^2}{12} = 44220.$$

Зокрема, для порівняння з проведеними обчисленнями наведемо результати обчислення $U(l, n)$ проведених вже згадуваною серією команд, яка наведена в додатку А.1, системи GAP 4.10.1.

	$n = 9$	$n = 10$	$n = 11$	$n = 12$	$n = 13$	$n = 14$
$l = 2$	56	99	186	335	630	1161
$l = 3$	2184	5880	16104	44220	122640	341484
$l = 4$	29120	104754	381300	1397740	5162220	19172790
$l = 5$	217000	976248	4438920	20343700	93900240	435959820
$l = 6$	1119720	6045837	32981550	181394535	1004668770	5597420295

Нехай K — комутативне локальне кільце характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$. Легко бачити, що відображення

$$\Gamma_A: a \rightarrow \Gamma_A(a) = E_n + t^{l-1}A,$$

де E_n — одинична $n \times n$ -матриця над кільцем K , A — довільна $n \times n$ -матриця над кільцем K , є матричним зображенням циклічної нетривіальної циклічної p -групи $H = \langle a \rangle$ над кільцем K . З [46] випливає, що потужність нееквівалентних нерозкладних зображень Γ_A фіксованого степеня n не менше ніж потужність $|K/\text{Rad } K|$ поля лишків кільця K . Для доведення використовувалися зображення $\Gamma_{J_n(\lambda)}$, які є нерозкладні і не еквівалентні при не конгруентних $\lambda \in K$ за модулем $\text{Rad } K$.

Означення 4.14. *Нехай E_n — одинична $n \times n$ -матриця над кільцем K . Назвемо зображенням Γ і Δ степеня n нетривіальної циклічної p -групи $H = \langle a \rangle$ над кільцем K $*$ -еквівалентними, якщо $\Gamma(a) - E_n$ та $\Delta(a) - E_n$ $*$ -подібні. В іншому випадку зображенням Γ і Δ назвемо $*$ -нееквівалентними.*

Якщо для деякої $n \times n$ -матриці A над кільцем K відображення $\Gamma: a \rightarrow E_n + A$ є зображенням, то для $*$ -подібної матриці, взагалі кажучи, може й не бути. Це, однак, не так для зображень Γ_A . Два такі зображення є $*$ -еквівалентні, якщо відповідні матриці $t^{l-1}A$ $*$ -подібні, або, що одне і те ж відповідні матриці A $*$ -подібні за модулем $\text{Ann}(t^{l-1}) = tK = R$, тобто, у полі $K/\text{Rad } K$. За лемою 1 матриці $J_n(\lambda)$ $*$ -подібні за модулем $\text{Rad } K$ тоді і тільки тоді, коли відповідні $\lambda \in K$ асоційовані за модулем модулем $\text{Rad } K$, тобто одночасно належать радикалу $\text{Rad } K$ або одночасно йому не належать. Отже, у множині зображень $\Gamma_{J_n(\lambda)}$ є тільки два зображення з точністю до $*$ -еквівалентності.

Відображення

$$\Gamma_{\bar{w}, \bar{\varepsilon}}: a \rightarrow \Gamma_{\bar{w}, \bar{\varepsilon}}(a) = E_n + M(\bar{w}, \bar{\varepsilon}) = E_n + M(\varepsilon_1 t^{s_1}, \dots, \varepsilon_n t^{s_n}) \quad (4.7)$$

є нерозкладним унімономіальним зображенням p -групи $H = \langle a \rangle$ порядку $|H| = m > 1$ над комутативним локальним кільцем K характеристики p , радикал Джекобсона якого $\text{Rad } K = tK$, t — нільпотентний елемент степеня $l \Rightarrow 1$, $s_i \in \mathbb{N} \cup \{0\}$ і $\varepsilon_i \in K^*$ ($i = 1, \dots, n$) якщо

$$1) \sum_{j=0}^{|H|-1} s_{i+j} \geq l \quad (i = 1, \dots, n) \quad (\text{теорема 4.4}),$$

$$2) \text{ послідовність } \bar{w} \text{ неперіодична (теорема 1.10).}$$

Крім того, зображення вигляду (4.7) $*$ -еквівалентні тоді і тільки тоді, коли відповідні матриці $M(\bar{w}, \bar{\varepsilon})$ $*$ -подібні. Тобто, за лемою 4.12, коли $\bar{w}$ та $\bar{w}'$ циклічно еквівалентні.

Зауважимо, що відображення (4.7) є зображенням циклічної p -групи $H = \langle a \rangle$ над кільцем K характеристики p тоді і тільки тоді, коли для $\bar{w} = (s_1, \dots, s_n)$ виконується умови $\sum_{j=0}^{|H|-1} s_{i+j} \geq l$ ($i = 1, \dots, n$). Останні умови не міняються під час циклічного зсуву послідовності $(s_1, \dots, s_n)$. А отже, відображення $\Gamma_{\bar{w}, \bar{\varepsilon}}$ є зображенням тоді і тільки тоді, коли для $*$ -подібної матриці $M' = M(\bar{w}', \bar{\varepsilon}')$ до $M = M(\bar{w}, \bar{\varepsilon})$ відображення

$$\Gamma_{\bar{w}', \bar{\varepsilon}'}: a \rightarrow \Gamma_{\bar{w}', \bar{\varepsilon}'}(a) = E_n + M(\bar{w}', \bar{\varepsilon}') = E_n + M(\varepsilon'_1 t^{s'_1}, \dots, \varepsilon'_n t^{s'_n})$$

є зображенням групи H над кільцем K .

Якщо послідовність $\bar{w}$ — неперіодична, то неперіодичною буде і довільна послідовність отримана з $\bar{w}$ циклічним зсувом. Тому всі зображення $*$ -еквівалентні зображенню $\Gamma_{\bar{w}, \bar{\varepsilon}}$ теж нерозкладні. З теореми 1.9

впливає, що один клас $*$ -еквівалентних зображень вигляду (4.7) розбивається на неперетинаючіся класи еквівалентних зображень з конгруентними значенням $\prod_{i=1}^n \varepsilon_i$ за модулем $\text{Ann}(t^s)$ в одному класі та неконгруентними в різних, де s — найбільший елемент вагової послідовності $\bar{w}$. Тому потужність множини класів еквівалентних зображень, що містяться в одному класі $*$ -еквівалентних зображень вигляду (4.7) рівна $|(K / \text{Ann}(t^s)) \setminus (tK / \text{Ann}(t^s))| = |K/t^{l(\text{Rad } K)-s}K \setminus tK/t^{l(\text{Rad } K)-s}K|$. Порахуємо з точністю до $*$ -еквівалентності число нерозкладних зображень групи H над кільцем K вигляду (4.7) з неперіодичною послідовністю $\bar{w}$. Воно є не менше числа $X(l, m, n)$ послідовностей $(s_1, \dots, s_n)$, таких, що $s_i \in \{0, 1, \dots, l-1\}$, $\sum_{j=0}^{m-1} s_{i+j} \geq l$ ($i = 1, \dots, n$), $(s_1, \dots, s_n)$ — найменша в лексикографічному порядку серед її циклічно еквівалентних.

При $l = 2$, $m = 4$, $n = 8$ число $X(2, 4, 8)$ є числом класів циклічно еквівалентних неперіодичних послідовностей

$$(s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8), \quad (4.8)$$

де $s_i \in \{0, 1\}$ ($i = 1, \dots, 8$) таких, що

$$s_1 + s_2 + s_3 + s_4 \geq 2;$$

$$s_2 + s_3 + s_4 + s_5 \geq 2;$$

$$\dots\dots\dots$$

$$s_8 + s_1 + s_2 + s_3 \geq 2.$$

Очевидно, $X(2, 4, 8)$ є числом неперіодичних послідовностей (4.8), кожна з яких найменша в лексикографічному порядку серед її циклічно еквівалентних. Тоді, очевидно $s_1 = 0$, $s_8 = 1$. Перебір таких послідовностей дасть

$$(0, 0, 1, 1, 0, 1, 1, 1), (0, 0, 1, 1, 1, 0, 1, 1), (0, 0, 1, 1, 1, 1, 1, 1), (0, 1, 0, 1, 0, 1, 1, 1),$$

$(0, 1, 0, 1, 1, 0, 1, 1), (0, 1, 0, 1, 1, 1, 1, 1), (0, 1, 1, 0, 1, 1, 1, 1), (0, 1, 1, 1, 1, 1, 1, 1).$

Таким чином $X(2, 4, 8) = 8$. Число $X(k, l, m, n)$ також можна обчислити, наприклад, серією команд, яка наведена в додатку А.1, системи GAP 4.10.1. В результаті обчислень також одержуємо $X(2, 4, 8) = 8$. Крім того, наприклад, одержуємо $X(3, 3, 12) = 2665$ ($U(3, 12) = 44220$). В таблицях А.10–А.13 наведено результати обчислень при деяких значеннях m та n і відповідно для $l = 2, \dots, 5$.

Зокрема, для порівняння з проведеними обчисленнями наведемо результати обчислення $X(2, m, n)$ при деяких значеннях m, n .

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$
$m = 3$	0	1	1	1	1	2	2	3	4
$m = 4$	1	1	2	3	3	6	8	14	20
$m = 5$	1	1	2	5	6	10	15	27	43
$m = 6$	1	2	2	5	8	14	21	37	63
$m = 7$	1	2	2	5	8	17	26	45	77
$m = 8$	1	2	3	5	8	17	29	51	87

4.5. Про число спадково незвідних унімономіальних зображення циклічних p -груп над локальним кільцем характеристики p з точністю до еквівалентності

Циклічну матрицю M над кільцем K подібну над кільцем K матриці

$$\begin{pmatrix} M_1 & T \\ 0 & M_2 \end{pmatrix},$$

де M_1 або M_2 — канонічно циклічна матриця над кільцем K назвемо *спадково звідною* над кільцем K і *спадково незвідною* над кільцем K в іншому випадку.

Для доведення спадкової незвідності канонічно циклічної матриці

$$M = M(\overline{w}, \overline{\varepsilon}) = \begin{pmatrix} 0 & \dots & 0 & \varepsilon_n t^{s_n} \\ \varepsilon_1 t^{s_1} & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \varepsilon_{n-1} t^{s_{n-1}} & 0 \end{pmatrix},$$

де $s_i \geq 0$, $\varepsilon_i \in K^*$ ($i = 1, \dots, n$); $\overline{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_{n-1}, \varepsilon_n)$, $\overline{w} = (s_1, \dots, s_n)$, у деяких випадках використовуватимемо аналіз її характеристичного многочлена. Для обчислення останнього використаємо розклад за першим рядком:

$$\begin{vmatrix} -\lambda & 0 & \dots & 0 & \varepsilon_n t^{s_n} \\ \varepsilon_1 t^{s_1} & -\lambda & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & -\lambda & 0 \\ 0 & 0 & \dots & \varepsilon_{n-1} t^{s_{n-1}} & -\lambda \end{vmatrix} =$$

$$-\lambda \begin{vmatrix} -\lambda & \dots & 0 & 0 \\ \varepsilon_2 t^{s_2} & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & \varepsilon_{n-1} t^{s_{n-1}} & -\lambda \end{vmatrix} + (-1)^{n+1} \varepsilon_n t^{s_n} \begin{vmatrix} \varepsilon_1 t^{s_1} & -\lambda & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & -\lambda \\ 0 & 0 & \dots & \varepsilon_{n-1} t^{s_{n-1}} \end{vmatrix} =$$

$$(-\lambda)^n + (-1)^{n+1} \varepsilon t^{\sum_{i=1}^n s_i} = (-1)^n (\lambda^n - \varepsilon t^s), \quad (4.9)$$

де $\varepsilon = \prod_{i=1}^n \varepsilon_i$, $s = \sum_{i=1}^n s_i$. Нам буде корисна лема.

Лема 4.15. *Нехай для натуральних чисел n', n та невід'ємних цілих чисел s', s , $ns' \neq n's$, $t^s \neq 0$, то многочлен $\lambda^n - \varepsilon t^s$ від неві-*

домої λ над кільцем K не ділиться на многочлен $\lambda^{n'} - \varepsilon' t^{s'}$ для жодних елементів $\varepsilon, \varepsilon' \in K^*$.

Доведення. Нехай для деякого $\varepsilon' \in K^*$

$$\begin{aligned} f(\lambda) &= \beta_0 \lambda^n + \beta_1 \lambda^{n-1} + \dots + \beta_{n-1} \lambda + \beta_n = \\ &= (\lambda^{n'} - \varepsilon' t^{s'}) (\alpha_0 \lambda^{n-n'} + \alpha_1 \lambda^{n-n'-1} + \dots + \alpha_{n-n'-1} \lambda + \alpha_{n-n'}) \quad (\alpha_i, \beta_i \in K). \end{aligned}$$

Тоді

$$\beta_i = \begin{cases} \alpha_i, & \text{якщо} \quad 0 \leq i < n', \\ \alpha_i - \varepsilon' t^{s'} \alpha_{i-n'}, & \text{якщо} \quad n' \leq i \leq n - n', \\ -\varepsilon' t^{s'} \alpha_{i-n'}, & \text{якщо} \quad n - n' < i \leq n, \end{cases} \quad (4.10)$$

Припустимо $f(\lambda) = \lambda^n - \varepsilon t^s$ для деякого $\varepsilon \in K^*$. Тобто $\beta_0 = 1$, $\beta_1 = \dots = \beta_{n-1} = 0$, $\beta_n = -\varepsilon t^s$. Для будь-якого j ($0 < j < n'$) одержуємо $j < n$, $\beta_j = 0$ і за (4.10) $\alpha_j = \beta_j = 0$. Тобто,

$$\alpha_1 = \dots = \alpha_{n'-1} = 0. \quad (4.11)$$

Якщо $0 \leq j \leq n - 2n'$ (випадок $n < 2n'$, при якому жодного j не існує, не виключається з розгляду), то $0 < j + n' < n$, $\beta_{j+n'} = 0$. Крім того, $n' \leq j + n' \leq n - n'$ і за (4.10) $\alpha_{j+n'} = \varepsilon' t^{s'} \alpha_j$. Звідси враховуючи (4.11) $\alpha_i = 0$, ($i \not\equiv 0 \pmod{n'}$), $i = 1, \dots, n - n'$). Оскільки, згідно (4.10), $\varepsilon' t^{s'} \alpha_{n-n'} = \beta_n = -\varepsilon t^s \neq 0$, то $\alpha_{n-n'} \neq 0$ і $n \equiv n - n' \equiv 0 \pmod{n'}$. Нехай $n = n'd$ для відповідного цілого d . Зрозуміло $d > 1$. Крім того, $\beta_{in'} = 0$ ($i = 1, \dots, d - 1$). Тому згідно (4.10), $\alpha_0 = \beta_0 = 1$, $\alpha_{in'} = \varepsilon' t^{s'} \alpha_{(i-1)n'}$ ($i = 1, \dots, d - 1$), $-\varepsilon' t^{s'} \alpha_{n-n'} = \beta_n = -\varepsilon t^s$. Тоді $\alpha_0 = 1$, $\alpha_{in'} = \varepsilon' t^{s'} \alpha_{(i-1)n'}$ ($i = 1, \dots, d - 1$), $\varepsilon' t^{s'} \alpha_{n-n'} = \varepsilon t^s$. Звідки $\varepsilon'^d t^{s'd} = \varepsilon t^s$. Оскільки $t^s \neq 0$, то $s'd = s$ і $ns' = n'ds' = n's$, що суперечить умові. $\square$

Теорема 4.16. Матриця $M(\overline{w}, \overline{\varepsilon})$ спадково незвідна, якщо послідовність $\overline{w} = (s_1, \dots, s_n)$ задовольняє умови $(s, n) = 1$, $t^s \neq 0$, де $s = \sum_{i=1}^n s_i$.

Доведення. Характеристичний многочлен $\lambda^n - \varepsilon t^s$ ($\varepsilon \in K^*$, t — твірний елемент радикала кільця K) канонічно циклічної матриці $M = M(\overline{w}, \overline{\varepsilon})$ у випадку спадкової звідності ділиться на характеристичний многочлен $\lambda^{n'} - \varepsilon' t^{s'}$ ($\varepsilon' \in K^*$, s' — невід'ємне ціле число) канонічно циклічної матриці порядку $n' < n$. Тоді за лемою 4.15 $ns' = n's$. Оскільки $(s, n) = 1$, то n ділить n' , $n \leq n'$, що неможливо. $\square$

Зауважимо, що з теореми 3.3 випливає спадкова звідність матриці $M(\overline{w}, \overline{\varepsilon})$, якщо послідовність $\overline{w} = (s_1, \dots, s_n)$ задовольняє умову $(s, n) > 1$, де $s = \sum_{i=1}^n s_i$ а послідовність $\overline{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$ задовольняє умову $\prod_{i=1}^n \varepsilon_i = 1$.

Для подальших обчислень нам буде корисна лема.

Лема 4.17. Нехай $(\sum_{i=1}^n s_i, n) = 1$, де n — натуральне число, $s_i \geq 0$, $\varepsilon_i \in K^*$ ($i = 1, \dots, n$). Послідовність $(s_1, \dots, s_n)$ неперіодична.

Доведення. Припустимо послідовність $(s_1, \dots, s_n)$ періодична. Тоді, за лемою 4.8 найменший період k послідовності $(s_1, \dots, s_n)$ ділить n і

$$\left(\sum_{i=1}^n s_i, n \right) = \left(\frac{n}{k} \sum_{i=1}^k s_i, \frac{n}{k} k \right) \geq \frac{n}{k}.$$

За означенням періода $k < n$, тому останнє неможливе. Отже, $(s_1, \dots, s_n)$ неперіодична. $\square$

Нехай тепер K — довільне комутативне кільце з одиницею, G — скінченно породжена група з деякою фіксованою системою твірних елементів. Будь-яке звідне унімономіальне зображення групи G над кільцем K ,

у зведеному вигляді якого на діагональних блоках утворюється хоч одне унімономіальне зображення, назовемо *спадково звідним* над кільцем K і *спадково незвідним* в іншому випадку.

Нехай K — комутативне локальне кільце характеристики p радикал Джекобсона якого $\text{Rad } K = tK$, де p — просте число, t — нільпотентний елемент степеня $l = l(\text{Rad } K) > 1$, $|H| = m$. Побудуємо з точністю до еквівалентності серію (відповідних до вибору a) спадково незвідних унімономіальні зображення групи H над кільцем K . Легко бачити, що будь-яке таке зображення групи H еквівалентне до

$$\Gamma_{\bar{w}, \bar{\varepsilon}} : a \rightarrow \Gamma_{\bar{w}, \bar{\varepsilon}}(a) = E_n + M(\bar{w}, \bar{\varepsilon}), \quad (4.12)$$

де E_n — одинична $n \times n$ -матриця, $M(\bar{w}, \bar{\varepsilon})$ — спадково незвідна канонічно циклічна матриця порядку n . За теоремою 4.16 матриця $M(\bar{w}, \bar{\varepsilon})$ спадково незвідна, якщо послідовність $\bar{w} = (s_1, \dots, s_n)$ задовольняє умови $(s, n) = 1$, $t^s \neq 0$, де $s = \sum_{i=1}^n s_i$.

За теоремою 4.9 два зображення вигляду 4.12 над кільцем K еквівалентні тоді і лише тоді, коли відповідні $\bar{w}$ циклічно еквівалентні а відповідні елементи $\varepsilon = \prod_{i=1}^n \varepsilon_i$ кільця K конгруентні за модулем $\text{Ann}(t^s)$, де s — найбільший член вагової послідовності $\bar{w}$.

Нехай $K/\text{Rad } K$ — скінченне поле з k елементів. За лемою 4.9 $|K| = k^l$, $|K/t^i K| = k^i$, $|(K/t^i K)^*| = (k-1)k^{i-1}$ ($i = 1, \dots, l$). Таким чином число спадково незвідних нееквівалентних унімономіальні зображення групи H вигляду (4.12) у випадку, коли m є деяким степенем числа p , не менше числа $Y(k, l, m, n)$ послідовностей $(s_1, \dots, s_n, \varepsilon)$, таких, що $s_i \in \{0, 1, \dots, l-1\}$, $(\sum_{i=1}^n s_i, n) = 1$, $\sum_{i=1}^n s_i < l$, $\sum_{j=0}^{m-1} s_{i+j} \geq l$ ($i = 1, \dots, n$), ε належить множині представників всіх різних суміжних класів $(K/\text{Ann}(t^s))^* = (K/t^{l-s} K)^*$, $s = \max_{i=1}^n (s_i)$, $\bar{w} = (s_1, \dots, s_n)$ —

найменша в лексикографічному порядку серед її циклічно еквівалентних.

Очевидно, $Y(k, 5, 8, 3)$ є числом послідовностей $(s_1, s_2, s_3, \varepsilon)$, де $0 \leq s_i < 5$ ($i = 1, \dots, 3$), $(s_1 + s_2 + s_3, 3) = 1$,

$$s_1 + s_2 + s_3 < 5, \quad 3s_1 + 3s_2 + 2s_3 \geq 5,$$

$$2s_1 + 3s_2 + 3s_3 \geq 5, \quad 3s_1 + 2s_2 + 3s_3 \geq 5,$$

ε належить множині представників всіх різних суміжних класів $(K/t^{5-s}K)^*$ ($s = \max_{i=1}^n(s_i)$), $\bar{w} = (s_1, s_2, s_3)$ — найменша в лексикографічному порядку серед її циклічно еквівалентних. Легко бачити, що для розглядуваних послідовностей $s_1 + s_2 + s_3 \in \{2, 4\}$. Перебір таких послідовностей $(s_1, s_2, s_3, \varepsilon)$ разом з s та кількістю варіантів для ε дасть $(0, 1, 1, \varepsilon)$ -1- $(k-1)k^3$, $(0, 0, 4, \varepsilon)$ -4- $(k-1)$, $(0, 1, 3, \varepsilon)$ -3- $(k-1)k$, $(0, 2, 2, \varepsilon)$ -2- $(k-1)k^2$, $(0, 3, 1, \varepsilon)$ -3- $(k-1)k$, $(1, 1, 2, \varepsilon)$ -2- $(k-1)k^2$. Таким чином $Y(k, 5, 8, 3) = (k-1)(k^3 + 2k^2 + 2k + 1) = k^4 + k^3 - k - 1$.

При $l = 5$, $m = 8$, $n = 3$ число $Y(k, l, m, n)$ також можна обчислити, наприклад, серією команд, яка наведена в додатку А.3, системи GAP 4.10.1. В таблицях А.14–А.21 наведено результати обчислень при деяких значеннях m та n і відповідно для $l = 3, \dots, 10$.

Зокрема, для порівняння з проведеними обчисленнями наведемо результати обчислення $Y(k, 5, m, n)$ при деяких значеннях m та n .

	$n = 2$	$n = 3$	$n = 4$	$n = 5$
$m = 5$	$k^3 - k$	$2k^3 - 2k$	0	0
$m = 6$	$k^3 - k$	$2k^3 - k - 1$	0	0
$m = 7$	$k^3 - k$	$2k^3 - k - 1$	$k^4 - k^3$	$k^4 + 2k^3 - 3k^2$
$m = 8$	$k^3 - k$	$k^4 + k^3 - k - 1$	$k^4 + 2k^3 - 2k^2 - k$	$k^4 + 6k^3 - 5k^2 - 2k$
$m = 9$	$k^3 - k$	$k^4 + 2k^3 - k^2 - k - 1$	$k^4 + 2k^3 - 2k^2 - k$	$3k^4 + 5k^3 - 4k^2 - 4k$
$m = 10$	$k^4 - k$	$k^4 + 2k^3 - k^2 - k - 1$	$k^4 + 2k^3 - 2k^2 - k$ $k^4 + 2k^3 - 2k^2 - k$	$3k^4 + 9k^3 - 7k^2 - 4k - 1$

4.6. Висновки до розділу

У цьому розділі вводиться поняття унімономіальних зображень скінченно породжених груп (підрозділ 4.1) над комутативним кільцем з одиницею та досліджується потужність множини нерозкладних та множини незвідних унімономіальних зображень з точністю до еквівалентності циклічної p -групи над комутативним локальним кільцем скінченної довжини характеристики p .

В підрозділі 4.2 будується серія нерозкладних унімономіальних зображень циклічної p -групи, що відповідають двозв'язним циклам, над комутативним локальним кільцем скінченної довжини характеристики p^s , та оцінюється знизу число побудованих зображень заданого степеня з точністю до еквівалентності для груп з деяким достатньо великим порядком. В підрозділі 4.3 будується серія нерозкладних унімономіальних зображень циклічної p -групи над скінченним комутативним локальним кільцем скінченної довжини характеристики p , та підраховується число побудованих зображень заданого степеня з точністю до еквівалент-

ності для кожної групи та кільця, зі скінченним полем лишків, окремо. В підрозділі 4.4 вводиться поняття $*$ -еквівалентності унімономіальних зображень циклічної групи над комутативним локальним кільцем головних ідеалів, будується серія нерозкладних унімономіальних зображень циклічної p -групи над довільним комутативним локальним кільцем скінченної довжини характеристики p та підраховується число побудованих зображень заданого степеня з точністю до $*$ -еквівалентності для кожної групи та кільця окремо. В підрозділі 4.5 вводиться поняття спадково незвідних унімономіальних зображень циклічної групи над комутативним локальним кільцем головних ідеалів, будується серія спадково незвідних унімономіальних зображень циклічної p -групи над скінченним комутативним локальним кільцем головних ідеалів характеристики p , та підраховується число побудованих зображень заданого степеня з точністю до еквівалентності для кожної групи та кільця, зі скінченним полем лишків, окремо.

Ключовим поняттям розділу є унімономіальне зображення скінченно породженої групи.

Результати цього розділу анонсовано в [50, 91, 104, 136, 220] та опубліковано в роботах [87–90, 90, 105].

РОЗДІЛ 5.

УНІПОТЕНТНІ ПІДГРУПИ ЛІНІЙНИХ ГРУП НАД КОМУТАТИВНИМИ КІЛЬЦЯМИ

Всюди протягом розділу K позначає комутативне кільце з одиницею, $M(n, K)$ — *повне матричне кільце* степеня n над кільцем K (кільце $n \times n$ -матриць ($n > 0$) над кільцем K), $T(n, K)$ — *кільце верхніх трикутних матриць* порядку $n > 0$ над кільцем K з нулями на головній діагоналі, $GL(n, K)$ — *повну лінійну групу* степеня n над кільцем K (мультиплікативну групу оборотних матриць порядку $n > 0$ над кільцем K), $SL(n, K)$ — *спеціальну лінійну групу* степеня n над кільцем K (мультиплікативну групу матриць з детермінантом 1 порядку $n > 0$ над кільцем K), $UT(n, K)$ — *унітрикутну групу* степеня n над кільцем K (мультиплікативну групу верхніх трикутних матриць порядку $n > 0$ над кільцем K з одиницями на головній діагоналі). Також елемент $t + \text{rad } K$ факторкільця $K/\text{rad } K$ позначаємо через $\tilde{t}$ і для (довільної) матриці $T = (t_{ij})$ над кільцем K покладемо $\tilde{T} = (\tilde{t}_{ij})$.

5.1. Вступ

Підгрупи P та Q деякої групи G (наприклад, лінійної групи) називають *спряженими*, якщо для деякого $C \in G$

$$C^{-1}PC = \{C^{-1}MC \mid M \in P\} = Q.$$

Очевидно, спряження зберігає властивості груп такі, як бути p -підгрупою чи уніпотентною підгрупою. Нагадаємо, підгрупа довільної групи називається *p -підгрупою*, якщо порядок кожного її елемента є степенем простого числа p , підгрупа довільної лінійної групи називається

уніпотентною підгрупою, якщо всі її елементи уніпотентні матриці. Під уніпотентною матрицею розуміємо $n \times n$ -матрицю A ($n > 0$), для якої $A - E_n$ — нільпотентна матриця, де E_n — одинична матриця того ж порядку n , що й матриця A . Прикладом уніпотентної підгрупи повної лінійної групи $GL(n, K)$ є унітрикутна група $UT(n, K)$. Дійсно, для будь-якої $A \in UT(n, K)$

$$A - E_n = \begin{pmatrix} 0 & \alpha_{12} & \alpha_{13} & \dots & \alpha_{1n} \\ 0 & 0 & \alpha_{23} & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

($\alpha_{ij} \in K$; $i = 1, \dots, n-1$; $j = i+1, \dots, n$) є нільпотентною матрицею степеня нільпотентності не більше n .

Підгрупу довільної групи з деякою властивістю τ , яка не міститься в жодній іншій підгрупі з властивістю τ цієї ж групи називають *максимальною підгрупою з властивістю τ* . Прийнято максимальні p -підгрупи довільної групи називати *силовськими p -підгрупами* цієї групи. Зрозуміло, що спряжена до максимальної уніпотентної підгрупи лінійної групи є максимальною уніпотентною підгрупою тої ж групи. Те ж стосується і силовських p -підгруп довільних груп. Навпаки, для деяких класів лінійних груп будь-які дві максимальні уніпотентні підгрупи (силовські p -підгрупи) лінійної групи спряжені. В цьому розділі встановлюються нові класи повної та спеціальної лінійних груп, що максимальні уніпотентні підгрупи попарно спряжені. Отримані результати застосовуються до вивчення силовських p -підгруп тих же груп над кільцем K , якщо характеристика кільця K рівна p^s ($s \in \mathbb{N}$).

5.2. Максимальні уніпотентні підгрупи повної лінійної групи

Ми називаємо комутативну область цілісності з одиницею *кільцем Безу*, якщо будь-який скінченно породжений його ідеал є головним.

Теорема 5.1. *Нехай K — кільце Безу. Будь-яка максимальна уніпотентна підгрупа групи $GL(n, K)$ спряжена з $UT(n, K)$.*

Доведення. Нехай F — поле відношень кільця K , а P — максимальна уніпотентна підгрупа групи $GL(n, K)$. Очевидно P — це уніпотентна підгрупа групи $GL(n, F)$. Розглянемо множину Ω уніпотентних підгруп групи $GL(n, F)$, які містять P . Очевидно, Ω є частково впорядкованою множиною відносно відношення включення. Ясно, що об'єднання лінійно впорядкованої множини уніпотентних підгруп групи $GL(n, F)$, які містять P , є уніпотентною підгрупою групи $GL(n, F)$, яка містить P . Згідно принципу максимуму Ω містить максимальний елемент, який є максимальною уніпотентною підгрупою групи $GL(n, F)$, яка містить P . Отже, P міститься в деякій максимальній уніпотентній підгрупі групи $GL(n, F)$, яка за теоремою 1.15 спряжена з $UT(n, F)$ у групі $GL(n, F)$. Тому для деякої матриці $C \in GL(n, F)$ $C^{-1}PC \subset UT(n, F)$.

Тоді перший стовпчик матриці $C^{-1}AC$, а отже, і матриці AC є нульовий, для будь-якої $n \times n$ -матриці A , такої, що $E_n + A \in P$, де E_n — одинична $n \times n$ -матриця. Нехай

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

— перший стовпець матриці C ($x_i \in K$, $i = 1, \dots, n$). Тоді $AX = 0$, для будь-якої $n \times n$ -матриці A , такої, що $E_n + A \in P$. Так-як F — поле відношень кільця K , то $x_i = ax_i^{(0)}$ для деякого $a \in F$ ($x_i^{(0)} \in K$, $i = 1, \dots, n$). Тоді $X = aX^{(0)}$, де

$$X^{(0)} = \begin{pmatrix} x_1^{(0)} \\ x_2^{(0)} \\ \vdots \\ x_n^{(0)} \end{pmatrix}.$$

Оскільки матриця C оборотна, то $X \neq 0$, а отже, $X^{(0)} \neq 0$, $a \neq 0$. Враховуючи, що K — область цілісності, $aAX^{(0)} = AaX^{(0)} = AX = 0$, то для будь-якої матриці $E_n + A \in P$ $AX^{(0)} = 0$.

Покажемо, що існує стовпець

$$X^{(k)} = \begin{pmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \vdots \\ x_n^{(k)} \end{pmatrix}$$

над кільцем K , що містить не менше k нулів ($0 \leq k \leq n - 1$), $X^{(k)} = D'X^{(0)}$ для деякої матриці $D' \in GL(n, K)$. Застосуємо індукцію за числом k . При $k = 0$ доводити нема чого. Припустимо тепер, що $0 \leq k < n - 1$ і $X^{(k)}$ містить не менше k нулів. Залишилося показати, що для деякої матриці $D'' \in GL(n, K)$ $D''X^{(k)}$ містить принаймні $k + 1$ нуль. Якщо стовпчик $X^{(k)}$ не містить принаймні $k + 1$ нулів, то, враховуючи, що $k \leq n - 2$, він містить принаймні два ненульові елементи. Ми можемо припустити, що $x_1^{(k)} \neq 0$, $x_2^{(k)} \neq 0$. Для кільця Безу K скінченно породжений ідеал $x_1^{(k)}K + x_2^{(k)}K$ є головним. Нехай $x_1^{(k)}K + x_2^{(k)}K = xK$ ($x \in K$, $x \neq 0$). Нехай α, β, γ і δ — елемент кільця K , що $x_1^{(k)}\alpha + x_2^{(k)}\beta = x$,

$x_1^{(k)} = \gamma x$ і $x_2^{(k)} = \delta x$. Легко бачити, що $x(\alpha\gamma + \beta\delta) = x$, $x(\gamma x_2^{(k)} - \delta x_1^{(k)}) = 0$. Звідси випливає, що $\alpha\gamma + \beta\delta = 1$, $\gamma x_2^{(k)} - \delta x_1^{(k)} = 0$. Отже,

$$M = \begin{pmatrix} \alpha & \beta \\ -\delta & \gamma \end{pmatrix} \in GL(2, R),$$

бо $\det M = \alpha\gamma + \beta\delta = 1$. Крім того,

$$M \begin{pmatrix} x_1^{(k)} \\ x_2^{(k)} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\delta & \gamma \end{pmatrix} \begin{pmatrix} x_1^{(k)} \\ x_2^{(k)} \end{pmatrix} = \begin{pmatrix} \alpha x_1^{(k)} + \beta x_2^{(k)} \\ -\delta x_1^{(k)} + \gamma x_2^{(k)} \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}.$$

Таким чином,

$$X^{(k+1)} = \begin{pmatrix} M & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix} X^{(k)}$$

містить не менше $k + 1$ нулів.

З індукції випливає, що для деякої матриці $D \in GL(n, K)$ $DX^{(0)}$ містить не менше $n - 1$ нуль. Не зменшуючи загальності, можна вважати, що

$$DX^{(0)} = \begin{pmatrix} \varepsilon \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

($\varepsilon \in K$). Оскільки $X^{(0)} \neq 0$, то $\varepsilon \neq 0$, і

$$X^{(0)} = D^{-1} \begin{pmatrix} \varepsilon \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \varepsilon D^{-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \varepsilon Y,$$

де Y — перший стовпець матриці $S = D^{-1}$. Так-як $AX^{(0)} = AY = 0$, то перший стовпці матриць AS і, отже, $S^{-1}AS$ дорівнюють нулю для будь-якої $n \times n$ -матриці A , такої, що $E_n + A \in P$. Отже, довільна матриця групи $S^{-1}PS$ має вигляд:

$$\begin{pmatrix} 1 & \alpha_{12} & \dots & \alpha_{1n} \\ 0 & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}$$

($\alpha_{ij} \in K$; $i = 1, \dots, n$; $j = 2, \dots, n$).

Нескладною індукцією за n можна показати, що P є спряжена з деякою підгрупою групи $UT(n, K)$. В силу уніпотентності підгрупи $UT(n, K)$ і максимальності уніпотентної підгрупи P остання спряжена з групою $UT(n, K)$. $\square$

Лема 5.2. Нехай $\varphi: X \rightarrow \widetilde{X}$.

- 1) Відображення φ : задає епіморфізм кільця $M(n, K)$ на $M(n, K/\text{rad } K)$.
- 2) Для довільної матриці $X \in M(n, K)$ матриця $\widetilde{X}$ оборотна тоді і тільки тоді, коли X оборотна матриця.
- 3) Для довільної матриці $X \in M(n, K)$ матриця $\widetilde{X}$ уніпотентна тоді і тільки тоді, коли X уніпотентна матриця.
- 4) При цьому відображенні повний прообраз будь-якої максимальної уніпотентної підгрупи групи $GL(n, K/\text{rad } K)$ є максимальною уніпотентною підгрупою групи $GL(n, K)$ і навпаки, будь-яка максимальна уніпотентна підгрупа групи $GL(n, K)$ є пов-

ний прообразом деякої максимальної уніпотентної підгрупи групи $GL(n, K/\text{rad } K)$.

- 5) Дві максимальні уніпотентні підгрупи групи $GL(n, K)$ спряжені тоді і тільки тоді, коли їх образи при гомоморфізмі φ є спряженими максимальними уніпотентними підгрупами групи $GL(n, K/\text{rad } K)$.

Доведення. Дійсно сюр'єктивність та кільцева гомоморфна властивість відображення φ очевидні. Властивість 1) виконується.

Легко бачити (див., наприклад, [175, ст. 118, вправа 10.25 (2)]), що ядро $M(n, \text{rad } K)$ гомоморфізма φ двосторонній ідеал кільця $M(n, K)$, що складається з нільпотентних матриць. Нехай $X \in M(n, K)$. Якщо X оборотна матриця, то оборотна і $\widetilde{X}$ ($\widetilde{X}^{-1} = \widetilde{X^{-1}}$). Якщо $\widetilde{X}$ оборотна матриця, то $\det \widetilde{X} \in (K/\text{rad } K)$ оборотний елемент кільця $K/\text{rad } K$ і для деякого $\alpha \in K$ $(\det X)\alpha = 1 + r$, де $r \in \text{rad } K$. Однак r — нільпотентний елемент і для достатньо великого s $r^s = 0$, $(1 + r)(1 - r + r^2 - \dots + (-1)^{s-1}r^{s-1}) = 1 + (-1)^{s-1}r^s = 1$. Отже, $1 + r$, а тому і $\det X$ оборотні елементи кільця K а X оборотна матриця. Отже, властивість 2) виконується.

Нехай знову $X \in GL(n, K)$. Якщо X уніпотентна матриця, то $X - E_n$ нільпотентна матриця. Оскільки $k \rightarrow k + \text{rad } K = \widetilde{k}$ канонічний епіморфізм кілець $K \rightarrow K/\text{rad } K$, то $\widetilde{X - E_n} = \widetilde{X} - \widetilde{E_n}$ нільпотентна матриця, $\widetilde{X} = \varphi(X)$ уніпотентна матриця. Якщо $\varphi(X) = \widetilde{X}$ уніпотентна матриця, то для одиничної матриці E_n порядку n матриця $\widetilde{X} - \widetilde{E_n} = \widetilde{X - E_n}$ нільпотентна. Звідси $(\widetilde{X - E_n})^m = \widetilde{0}$ для деякого натурального m і $(X - E_n)^m$ складається з елементів ідеалу $\text{rad } K$, тобто попадає в ядро епіморфізма φ . Тому матриця $(X - E_n)^m$, а отже, і $X - E_n$ нільпотентна.

Тоді матриця X уніпотентна. Отже, властивість 3) виконується.

Якщо P підгрупа групи $GL(n, K)$, $P' = \varphi(X)$ підгрупа групи $GL(n, K/\text{rad } K)$, то за властивістю 3) P уніпотентна підгрупа групи $GL(n, K)$ тоді і тільки тоді, коли P' уніпотентна підгрупа групи $GL(n, K/\text{rad } K)$. Нехай тепер P' — довільна максимальна уніпотентна підгрупа групи $GL(n, K/\text{rad } K)$ тоді повний прообраз P групи P' при гомоморфізмі φ є уніпотентна підгрупою групи $GL(n, K)$. Якщо Q уніпотентна підгрупа групи $GL(n, K)$, що містить P , то $P' = \varphi(P) \subset \varphi(Q)$. Оскільки P' максимальна уніпотентна підгрупа групи $GL(n, K/\text{rad } K)$, $\varphi(Q)$ уніпотентна підгрупа групи $GL(n, K/\text{rad } K)$, то $P' = \varphi(Q)$. Так-як P повний прообраз групи P' при гомоморфізмі φ , то $Q \subset P$. Отже, P максимальна уніпотентна підгрупа групи $GL(n, K)$.

Нехай тепер P — максимальна уніпотентна підгрупа групи $GL(n, K)$. Тоді $\varphi(P)$ — уніпотентна підгрупа групи $GL(n, K/\text{rad } K)$. Користуючись стандартним застосуванням принципу максимуму для деякої максимальної уніпотентної підгрупи Q' групи $GL(n, K/\text{rad } K)$, $Q' \supset \varphi(P)$. Нехай Q — повний прообраз групи Q' при гомоморфізмі φ . За властивістю 3) Q — уніпотентна підгрупа групи $GL(n, K)$. Очевидно, $Q \supset P$. Оскільки P — максимальна уніпотентна підгрупа групи $GL(n, K)$, то $Q = P$, $Q' = \varphi(P)$ і P є повним прообразом максимальної уніпотентної підгрупи $\varphi(P)$ групи $GL(n, K/\text{rad } K)$ при гомоморфізмі φ . Отже, властивість 4) виконується.

Нехай P і Q — максимальні уніпотентні підгрупи групи $GL(n, K)$, тоді їх образи при гомоморфізмі φ відповідно P' і Q' є максимальними уніпотентними підгрупами групи $GL(n, K/\text{rad } K)$. Припустимо спочатку, що підгрупи P' і Q' групи $GL(n, K/\text{rad } K)$ спряжені. Тоді для деякої матриці $\tilde{C} \in GL(n, K/\text{rad } K)$ $\tilde{C}^{-1}P'\tilde{C} = Q'$. Оскільки φ — епіморфне

відображення групи $GL(n, K)$ на групу $GL(n, K/\text{rad } K)$, то для деякої матриці $C \in GL(n, K)$ $\varphi(C) = \tilde{C}$. Отже, $\varphi(C^{-1}PC) = \tilde{C}^{-1}P'\tilde{C} = Q'$. За доведеним Q — повний прообраз групи Q' при гомоморфізмі φ , тому $C^{-1}PC \subset Q$. Так як P — максимальна уніпотентна підгрупа групи $GL(n, K)$, а Q — її уніпотентна підгрупа, то $C^{-1}PC = Q$ і підгрупи P і Q групи $GL(n, K)$ спряжені.

Припустимо тепер, що підгрупи P і Q групи $GL(n, K)$ спряжені. Тому для деякої матриці $C \in GL(n, K)$ $C^{-1}PC = Q$. Очевидно, $\bar{C} \in GL(n, K/\text{rad } K)$ і $\bar{C}^{-1}P'\bar{C} = Q'$. Отже, властивість 5) виконується. $\square$

Наслідок 5.3. *Нехай K — комутативне кільце з одиницею. Якщо $K/\text{rad } K$ кільце Безу, то будь-яка максимальна уніпотентна підгрупа групи $GL(n, K)$ спряжена до групи*

$$P = \{X \in GL(n, K) \mid \tilde{X} \in UT(n, K/\text{rad } K)\}.$$

Доведення. За лемою 5.2 $\varphi : X \rightarrow \tilde{X}$ епіморфізм матричних кілець $M(n, K)$ в $M(n, K/\text{rad } K)$, який зберігає властивість нільпотентності чи ненільпотентності матриць. Те ж стосується оборотності чи необоротності. Тому φ можна розглядати як епіморфізмом груп $GL(n, K)$ в $GL(n, K/\text{rad } K)$ а повний прообраз максимальної уніпотентної підгрупи групи $GL(n, K/\text{rad } K)$ є максимальною уніпотентною підгрупою групи $GL(n, K)$. Зокрема, $P = \{X \in M(n, K) \mid \tilde{X} \in UT(n, K/\text{rad } K)\}$ є максимальною уніпотентною підгрупою групи $GL(n, K)$, бо є повним прообразом групи $UT(n, K/\text{rad } K)$, яка за теоремою 5.1 є максимальною уніпотентною підгрупою групи $GL(n, K/\text{rad } K)$. За теоремою 5.1 максимальні уніпотентні підгрупи групи $GL(n, K/\text{rad } K)$ попарно спряжені. Тоді за лемою 5.2 властивість 5) максимальні уніпотентні під-

групи групи $GL(n, K)$ попарно спряжені, і будь-яка з них спряжена до $P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$. $\square$

Теорема 5.4. *Нехай K — комутативне кільце з одиницею, для якого $K/\text{rad } K$ — скінченна пряма сума кілець Безу. Тоді будь-яка максимальна уніпотентна підгрупа групи $GL(n, K)$ спряжена до групи*

$$P = \{X \in GL(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

Доведення. Неважко помітити, що можна вважати $\text{rad } K = 0$. Оскільки K — скінченна пряма сума кілець Безу, то $K = K_1 \oplus \dots \oplus K_k$ — пряма ортогональна сума деяких ідеалів K_i кільця K , які є кільцями Безу ($i = 1, \dots, k$). Тоді відповідно

$$GL(n, K) = GL(n, K_1) \times \dots \times GL(n, K_k) \quad (5.1)$$

буде прямим добутком груп $GL(n, K_i)$ ($i = 1, \dots, k$). Якщо $A \in GL(n, K)$, то $A = A_1 + \dots + A_k$ для єдиних $A_i \in GL(n, K_i)$ ($i = 1, \dots, k$). Зрозуміло, що A уніпотентна матриця тоді і тільки тоді, коли A_i уніпотентні матриці ($i = 1, \dots, k$). Очевидно, що будь-яка максимальна уніпотентна підгрупа Q групи $GL(n, K)$ має відповідно до розкладу (5.1) уніпотентні проєкції $Q_i = \{A_i | A \in Q\}$ на групи $GL(n, K_i)$ ($i = 1, \dots, k$). Крім того, $Q \subset Q_1 \times \dots \times Q_k$ а $Q_1 \times \dots \times Q_k$ — уніпотентна підгрупа групи $GL(n, K)$. Оскільки група Q максимальна уніпотентна підгрупа групи $GL(n, K)$, то $Q = Q_1 \times \dots \times Q_k$. З максимальності уніпотентної підгрупи Q групи $GL(n, K)$ зразу одержуємо максимальність уніпотентних підгруп Q_i груп $GL(n, K_i)$ ($i = 1, \dots, k$).

Очевидно підгрупа Q групи $GL(n, K)$ є спряжена з $UT(n, K) = UT(n, K_1) \times \dots \times UT(n, K_k)$, якщо підгрупи Q_i групи $GL(n, K_i)$ спряжені з $UT(n, K_i)$ ($i = 1, \dots, k$). За теоремою 5.1 будь-яка максимальна уніпотентна підгрупа групи $GL(n, K_i)$ спряжена до $UT(n, K_i)$ ($i = 1, \dots, k$). Тому будь-яка максимальна уніпотентна підгрупа групи $GL(n, K)$ спряжених до $UT(n, K)$. $\square$

Прикладом комутативного кільця K , такого, що $K/\text{rad } K$ є скінченною прямою сумою кілець Безу є кільце многочленів $\mathbb{Z}_{p^s}[x]$ та формальних степеневих рядів $\mathbb{Z}_{p^s}[[x]]$ від невідомої x з коефіцієнтами з кільця $\mathbb{Z}_{p^s}$ класів лишків за модулем p^s , де p — довільне просте число, $s > 0$ (а також скінченні прямі суми екземплярів таких кілець). Ясно, що $\text{rad } \mathbb{Z}_{p^s}[x] = \text{rad } \mathbb{Z}_{p^s}[[x]] = \text{rad } \mathbb{Z}_{p^s} = p\mathbb{Z}_{p^s}$. А фактор-кільця за первісними радикалами кілець $\mathbb{Z}_{p^s}[x]$, $\mathbb{Z}_{p^s}[[x]]$ будуть ізоморфні відповідно $\mathbb{Z}_p[x]$, $\mathbb{Z}_p[[x]]$ і є областями головних ідеалів (тобто кільцями Безу).

5.3. Максимальні уніпотентні підгрупи спеціальної лінійної групи

В цьому підрозділі досліджуються максимальні уніпотентні підгрупи спеціальної лінійної групи над комутативним кільцем.

Позначимо через $\text{diag}[\alpha_1, \dots, \alpha_n]$ діагональну матрицю порядку n з діагональними елементами $\alpha_1, \dots, \alpha_n$.

Теорема 5.5. *Нехай K — комутативне кільце, $\text{rad } K = 0$. Група $UT(n, K)$ є максимальною уніпотентною підгрупою групи $GL(n, K)$.*

Доведення. Ідея доведення теореми аналогічна ідеї доведення теореми 1.21, яка увійшла в результати кандидатської дисертації здобувача. $\square$

Теорема 5.6. *Нехай K — комутативне кільце.*

$$P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$$

є максимальною уніпотентною підгрупою групи $GL(n, K)$.

Доведення. За теоремою 5.5 $UT(n, K/\text{rad } K)$ є максимальною уніпотентною підгрупою групи $GL(n, K/\text{rad } K)$. За лемою 5.2 $\varphi : X \rightarrow \widetilde{X}$ можна розглядати як епіморфізм груп $GL(n, K)$ на $GL(n, K/\text{rad } K)$. Ясно, що $P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$ є повний прообраз підгрупи $UT(n, K/\text{rad } K)$ групи $GL(n, K/\text{rad } K)$ при цьому епіморфізмі. За лемою 5.2 властивість 3) повний прообраз P максимальної уніпотентної підгрупи $UT(n, K/\text{rad } K)$ групи $GL(n, K/\text{rad } K)$ є максимальною уніпотентною підгрупою групи $GL(n, K)$. $\square$

Теорема 5.7. *Нехай K — комутативне кільце. Тоді*

$$P \cap SL(n, K), \text{ де } P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$$

є максимальною уніпотентною підгрупою групи $SL(n, K)$.

Доведення. За теоремою 5.6 P є максимальна уніпотентна підгрупа групи $GL(n, K)$. Зрозуміло, що $P_1 = P \cap SL(n, K)$ є уніпотентною підгрупою групи $SL(n, K)$. За лемою 5.2 $\varphi : X \rightarrow \widetilde{X}$ можна розглядати як епіморфізм груп $GL(n, K)$ в $GL(n, K/\text{rad } K)$. Крім того,

$$\varphi(P_1) \subset \varphi(P) = UT(n, K/\text{rad } K).$$

Нехай $\widetilde{X} \in UT(n, K/\text{rad } K)$, де $X \in M(n, K)$. За лемою 5.2 властивість 2) $X \in GL(n, K)$. Розглянемо матрицю $X_1 = X \cdot \text{diag}[\det X^{-1}, 1, \dots, 1] \in SL(n, K)$. Оскільки $\widetilde{X} \in UT(n, K/\text{rad } K)$, то $\det \widetilde{X} = 1$ і

$$\varphi(P_1) \ni \widetilde{X}_1 = X \cdot \text{diag}[\det X^{-1}, 1, \dots, 1] = \widetilde{X} \cdot \text{diag}[\det \widetilde{X}^{-1}, 1, \dots, 1] = \widetilde{X}.$$

Отже, $\varphi(P_1) \supset UT(n, K/\text{rad } K)$ і $\varphi(P_1) = UT(n, K/\text{rad } K)$. Якщо P_2 — уніпотентна підгрупа групи $SL(n, K)$, $P_1 \subset P_2$, то за лемою 5.2 властивість 3) $\varphi(P_2)$ є уніпотентна підгрупа групи $GL(n, K)$. Оскільки вона містить $\varphi(P_1) = UT(n, K/\text{rad } K)$, яка є максимальною уніпотентною підгрупою $GL(n, K/\text{rad } K)$, то $\varphi(P_2) = UT(n, K/\text{rad } K)$. А отже,

$$P_1 = P \cap SL(n, K) = \varphi^{-1}(UT(n/\text{rad } K)) \cap SL(n, K) \supset \\ \varphi^{-1}(\varphi(P_2)) \cap SL(n, K) \supset P_2.$$

Отже, P_1 є максимальна уніпотентна підгрупа групи $SL(n, K)$. □

Твердження 5.8. *Нехай K — комутативне кільце. Якщо максимальні уніпотентні підгрупа групи $GL(n, K)$ попарно спряжені, то будь-яка максимальна уніпотентна підгрупа групи $SL(n, K)$ спряжена до групи*

$$P \cap SL(n, K), \text{ де } P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

Доведення. Оскільки максимальні уніпотентні підгрупи групи $GL(n, K)$ попарно спряжені, то за теоремою 5.6 будь-яка максимальна уніпотентна підгрупа групи $GL(n, K)$ спряжена до $P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$. Нехай Q_1 — деяка максимальна уніпотентна підгрупа групи $SL(n, K)$. Вона також є уніпотентна підгрупа групи $GL(n, K)$. Користуючись стандартним застосуванням принципу максимуму для деякої максимальної уніпотентної підгрупи Q групи $GL(n, K)$, $Q \supset Q_1$. Оскільки група Q спряжена в групі $GL(n, K)$ до $P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$, то група Q_1 спряжена до деякої підгрупи Q_2 групи P . Тобто для деякої $C \in GL(n, K)$

$$C^{-1}Q_1C = Q_2 \subset P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

Тоді

$$\begin{aligned} & (C \operatorname{diag}[\det C^{-1}, 1, \dots, 1])^{-1} Q_1 C \operatorname{diag}[\det C^{-1}, 1, \dots, 1] \subset \\ & \operatorname{diag}[\det C, 1, \dots, 1] C^{-1} Q_1 C \operatorname{diag}[\det C^{-1}, 1, \dots, 1] \subset \\ & \operatorname{diag}[\det C, 1, \dots, 1] P \operatorname{diag}[\det C^{-1}, 1, \dots, 1]. \end{aligned}$$

Однак, якщо $X \in P$, то $\widetilde{X} \in UT(n, K/\operatorname{rad} K)$ і

$$\begin{aligned} & \operatorname{diag}[\det C, 1, \dots, 1] \cdot \widetilde{X} \cdot \operatorname{diag}[\det C^{-1}, 1, \dots, 1] = \\ & \operatorname{diag}[\det \widetilde{C}, 1, \dots, 1] \cdot \widetilde{X} \cdot \operatorname{diag}[\det \widetilde{C}^{-1}, 1, \dots, 1] \in \\ & \operatorname{diag}[\det \widetilde{C}, 1, \dots, 1] \cdot UT(n, K/\operatorname{rad} K) \cdot \operatorname{diag}[\det \widetilde{C}^{-1}, 1, \dots, 1] = \\ & UT(n, K/\operatorname{rad} K). \end{aligned}$$

Тобто $Q_3 = (C \operatorname{diag}[\det C^{-1}, 1, \dots, 1])^{-1} Q_1 C \operatorname{diag}[\det C^{-1}, 1, \dots, 1] \subset P$.

Оскільки

$$\det(C \cdot (\operatorname{diag}[\det C^{-1}, 1, \dots, 1])) = 1,$$

то Q_3 є підгрупа групи $P \cap SL(n, K)$, яка спряжена в $SL(n, K)$ з Q_1 . Враховуючи, що Q_1 , а отже, і Q_3 є максимальна уніпотентна підгрупа групи $SL(n, K)$, $P \cap SL(n, K)$ є уніпотентна підгрупа групи $SL(n, K)$, то $Q_3 = P \cap SL(n, K)$ а Q_1 спряжена в $SL(n, K)$ з $P \cap SL(n, K)$. $\square$

З доведеного твердження та теореми 5.4 відразу випливає:

Теорема 5.9. *Нехай K — комутативне кільце. Якщо $K/\operatorname{rad} K$ є скінченною прямою сумою кілець Безу, то будь-яка максимальна уніпотентна підгрупа групи $SL(n, K)$ спряжена до групи*

$$P_1 = P \cap SL(n, K), \text{ де } P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\operatorname{rad} K)\}.$$

5.4. Силівські p -підгрупи повної та спеціальної лінійної групи над кільцем характеристики p^s

Лема 5.10. *Нехай характеристика комутативного кільця K рівна p^s , де p — просте число, $s > 0$.*

- 1) *Будь-яка $n \times n$ -матриця A ($n > 0$) над кільцем K є p -елементом групи $GL(n, K)$ тоді і лише тоді, коли A буде уніпотентною матрицею;*
- 2) *будь-яка підгрупа P групи $GL(n, K)$ є p -група тоді і лише тоді, коли P буде уніпотентною підгрупою групи $GL(n, K)$;*
- 3) *будь-яка підгрупа P групи $GL(n, K)$ є силівською p -підгрупою групи $GL(n, K)$ тоді і лише тоді, коли P буде максимальною уніпотентною підгрупою групи $GL(n, K)$.*

Доведення. Ясно, що властивості 2) та 3) негайно слідують з властивості 1). Оскільки p^s характеристика кільця K , то в кільці K елемент p нільпотентний і $p \in \text{rad } K$. Тоді характеристика кільця $K/\text{rad } K$ ділить p . Так-як число p просте, то p — характеристика кільця $K/\text{rad } K$. Нехай далі A — $n \times n$ -матриця над кільцем K , E_n — одинична $n \times n$ -матриця над кільцем K , $A' = A - E_n$.

Якщо A є p -елементом групи $GL(n, K)$, то для достатньо великого m $A^{p^m} = E_n$ і в кільці $K/\text{rad } K$ $\widetilde{A}^{p^m} = \widetilde{E}_n$. Оскільки E_n та A' комутують, p — характеристика кільця $K/\text{rad } K$, то

$$\widetilde{E}_n = \widetilde{A}^{p^m} = (\widetilde{E}_n + \widetilde{A}')^{p^m} = \widetilde{E}_n + \widetilde{A}'^{p^m},$$

$\widetilde{A}'^{p^m} = 0$. Тобто матриця $\widetilde{A} = \widetilde{E}_n + \widetilde{A}'$ уніпотентна. Тоді за лемою 5.2 властивість 3) матриця A уніпотентна.

Якщо A — уніпотентна матриця групи $GL(n, K)$, то для достатньо великого M $A'^M = 0$. Але для достатньо великого m $p^m \geq M$ і $A'^{p^m} = 0$. Можна вважати, що $m \geq s$. Оскільки E_n та A' комутують, то

$$A^{p^{2m}} = E_n + \sum_{i=1}^{p^{2m}-1} C_{p^{2m}}^i A'^i + A'^{p^{2m}}. \quad (5.2)$$

Враховуючи, що $A'^{p^m} = 0$,

$$A^{p^{2m}} = E_n + \sum_{i=1}^{p^m-1} C_{p^{2m}}^i A'^i.$$

Крім того,

$$\begin{aligned} C_{p^{2m}}^i &= \frac{p^{2m}!}{i!(p^{2m}-i)!} = \frac{1 \cdot 2 \cdots p^{2m}}{1 \cdot 2 \cdots i \cdot 1 \cdot 2 \cdots (p^{2m}-i)} = \\ &= \frac{(p^{2m}-i+1) \cdots (p^{2m}-1) \cdot p^{2m}}{1 \cdot 2 \cdots i} = \\ &= \frac{(p^{2m}-(i-1)) \cdots (p^{2m}-2) \cdot (p^{2m}-1)}{1 \cdot 2 \cdots (i-1)} \cdot \frac{p^{2m}}{i} = \\ &= \frac{\prod_{j=1}^{i-1} (p^{2m}-j)}{\prod_{j=1}^{i-1} j} \cdot \frac{p^{2m}}{i} = \prod_{j=1}^{i-1} \frac{p^{2m}-j}{j} \cdot \frac{p^{2m}}{i} \quad (1 \leq i < p^m). \end{aligned}$$

Нехай $k \in \mathbb{N}$, $1 \leq j < i < p^m$, $p^k | j$. Тоді $p^k \leq j < p^m$, $p^k | p^m$, $p^k | (p^m - j)$. Але $p^m \nmid i$ і $p^m = p^{2m-m} | C_{p^{2m}}^i$. Отже, враховуючи, що $m \geq s$, у кільці K $C_{p^{2m}}^i = 0$ ($i = 1, \dots, p^m$). Згідно (5.2) тоді $A^{p^{2m}} = E_n$. Отже, A є p -елементом групи $GL(n, K)$. $\square$

Наслідок 5.11. *Нехай K — комутативне кільце характеристики p^s , де p — просте число, $s > 0$.*

$$P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}$$

є силовською p -підгрупою групи $GL(n, K)$.

Доведення. Доведення випливає з леми 5.10 та теореми 5.6. $\square$

Наслідок 5.12. *Нехай K — комутативне кільце характеристики p^s , де p — просте число, $s > 0$. Якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу, то будь-яка силовська p -підгрупа групи $GL(n, K)$ спряжена до групи*

$$P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

Доведення. Доведення випливає з леми 5.10 та теореми 5.4. $\square$

Наслідок 5.13. *Нехай K — комутативне кільце характеристики p^s , де p — просте число, $s > 0$, і*

$$P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

Тоді $P \cap SL(n, K)$ є силовською p -підгрупою групи $SL(n, K)$.

Доведення. Доведення випливає з леми 5.10 та теореми 5.7. $\square$

Наслідок 5.14. *Нехай K — комутативне кільце характеристики p^s , де p — просте число. Якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу, то будь-яка силовська p -підгрупа групи $SL(n, K)$ спряжена до групи*

$$P \cap SL(n, K), \text{ де } P = \{X \in M(n, K) | \widetilde{X} \in UT(n, K/\text{rad } K)\}.$$

Доведення. Доведення випливає з леми 5.10 та теореми 5.9. $\square$

5.5. Висновки до розділу

В розділі розглядаються уніпотентні підгрупи повної та спеціальної лінійної групи над комутативним кільцем K . В підрозділі 5.2 п'ятого

розділу показано, що всі максимальні уніпотентні підгрупи повної лінійної групи над кільцем K попарно спряжені, якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу. В підрозділі 5.3 п'ятого розділу показано, що всі максимальні уніпотентні підгрупи спеціальної лінійної групи над кільцем K попарно спряжені, якщо $K/\text{rad } K$ є скінченною прямою сумою кілець Безу.

В підрозділі 5.4 результати про максимальні уніпотентні підгрупи повної та спеціальної лінійної групи над комутативним кільцем застосовуються до вивчення силовських p -підгрупи повної та спеціальної лінійної групи над тим же кільцем характеристика якого p^s .

Результати цього розділу анонсовано в [217] та опубліковані в роботах [78, 219].

РОЗДІЛ 6.

ЕКВІВАЛЕНТНІСТЬ МАТРИЦЬ ЗА МОДУЛЕМ ІДЕАЛІВ

При розв'язанні класифікаційних задач теорії зображень та лінійної алгебри є природнім побудова певних канонічних форм. Канонічні форми Жордана і Фробеніуса (пов'язані з подібністю матриць) знаходять важливі застосування в усіх природничих науках. Добре відомі широкі застосування канонічної форми Кронекера – Вейерштрасса (для пучка матриць).

6.1. Еквівалентність пар матриць над полем

Задача про пучок матриць — це задача про зведення двох матриць A і B над полем k одного і того ж розміру $m \times n$ ($m, n \in \mathbb{N} \cup 0$) одночасними елементарними перетвореннями рядків та стовпців. Таким чином дві пари $m \times n$ -матриць (A, B) та (A', B') вважаються *еквівалентними*, якщо існують оборотні $m \times m$ -матриця X та $n \times n$ -матриця Y , що

$$XAY = A', \quad XBY = B'.$$

Для її розв'язання необхідно вказати канонічну форму відносно вказаного відношення еквівалентності. Аналогічно, як і у випадку про зведення однієї матриці перетвореннями подібності, це достатньо зробити для нерозкладної пари матриць, вказавши, при цьому, набір нерозкладних канонічних пар (тобто нерозкладних пар матриць найбільш простого вигляду, таких, що між собою вони нееквівалентні, а будь-яка інша нерозкладна пара матриць еквівалентна одній з виділених). Пара $m \times n$ -

матриць (A, B) називається нерозкладною, якщо вона не є еквівалентною прямій сумі деяких пар матриць (A_1, B_1) і (A_2, B_2) відповідно розмірів $m_1 \times n_1$ і $m_2 \times n_2$, де $(m_1, n_1), (m_2, n_2) \neq (0, 0)$, тобто парі вигляду $(A_1 \otimes A_2, B_1 \otimes B_2)$, де

$$A_1 \otimes A_2 = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \quad B_1 \otimes B_2 = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}.$$

Нерозкладні канонічні пари матриць, наприклад, над алгебраїчно замкнутим полем k в цьому випадку добре відомі (див., наприклад, [21]).

$$1) \quad A_1 = \begin{pmatrix} E_s & \bar{0} \end{pmatrix}, \quad B_1 = \begin{pmatrix} \bar{0} & E_s \end{pmatrix}, \quad \text{де } s \geq 0;$$

$$2) \quad A_2 = \begin{pmatrix} E_s \\ \tilde{0} \end{pmatrix}, \quad B_2 = \begin{pmatrix} \tilde{0} \\ E_s \end{pmatrix}, \quad \text{де } s \geq 0;$$

$$3) \quad A_3 = E_s, \quad B_3 = J_s(a), \quad \text{де } s > 0;$$

$$4) \quad A_4 = J_s(a), \quad B_4 = E_s, \quad \text{де } s > 0;$$

тут E_s означає одиничну $s \times s$ -матрицю $J_s(a)$ — жорданова $s \times s$ -клітка з діагональним елементом $a \in k$, а $\bar{0}$ і $\tilde{0}$ — нульовий стовпець і нульовий рядок, відповідно.

Аналогічно до еквівалентності пар матриць вводиться поняття подібності пар матриць. Дві пари $n \times n$ -матриць (A, B) та (A', B') вважаються *подібними*, якщо існують оборотна $n \times n$ -матриця X , що

$$X^{-1}AX = A', \quad X^{-1}BX = B'.$$

Задача про подібність пар матриць над деяким полем вважається класичною нерозв'язаною задачею лінійної алгебри. Зрозуміло будь-яка інша класифікаційна задача, яка включає задачу про подібність пар матриць над деяким полем, є також нерозв'язною. Такі задачі були названі [53] *дикими*.

6.2. Еквівалентність матриць та пар матриць над кільцем

Добре відомо, що задача про еквівалентність двох матриць над полем повністю зводиться до порівняння їх рангів. При переході від полів до довільних комутативних кілець ситуація ускладнюється. Вперше Г. Сміт [208] у 1861 р. встановив, що кожна матриця над кільцем цілих чисел $\mathbb{Z}$ еквівалентна до матриці діагональної форми, тобто існують такі матриці $X \in GL(m, \mathbb{Z})$ і $Y \in GL(n, \mathbb{Z})$, що

$$D^A = XAY = \text{diag}(\mu_1^A, \mu_2^A, \dots, \mu_r^A, 0, \dots, 0), \quad (6.1)$$

де $\mu_r^A \neq 0$ і $\mu_i^A | \mu_{i+1}^A$ ($i = 1, 2, \dots, r$): Матриця D^A прямокутна $m \times n$ -матриця над кільцем $\mathbb{Z}$; в якій всі елементи в позиціях $(i; j)$ для $i \neq j$ дорівнюють нулю. Матрицю D^A називають *канонічною діагональною формою* матриці A . У 1943 р. О. Хелмер [158] ввів поняття адекватних кілець, і показав, що кожна матриця над таким кільцем є еквівалентною до канонічної діагональної форми.

Кільце R називають адекватним, якщо R – область цілісності, в якій кожний скінченно породжений ідеал головний і для кожного ненульового елемента $a \in R$ і кожного елемента $b \in R$ існують такі елементи $c, d \in R$, що $a = cd$, причому c є взаємно простим із b , а кожний необоротний дільник d_i елемента d має необоротний спільний дільник із $b \in R$. Кільця, над якими кожна матриця еквівалентна до канонічної діагональної форми, стали пізніше називати *кільцями елементарних дільників* [128, 171].

З іншого боку, П. М. Гудивок [26] виділив класи кілець, над якими задача про еквівалентність матриць є дико (містить задачу про подібність пар матриць над деяким полем). Зрозуміло, що такі кільця не є

кільцями елементарних дільників.

Теорема 6.1 ([26]). *Нехай K — нетерове факторіальне кільце, що не є кільцем головних ідеалів. Задача описання з точністю до еквівалентності довільних квадратних матриць над кільцем K є дика.*

Теорема 6.2 ([26]). *Нехай K — локальне факторіальне кільце, що не є кільцем головних ідеалів. Задача описання з точністю до еквівалентності довільних квадратних матриць над кільцем K є дика.*

При вивченні матриць над кільцями, що є складнішою задачею ніж над полями, також активно досліджуються питання про описання пар матриць відносно деяких відношень еквівалентності. Дві пари матриць (A_1, A_2) та (B_1, B_2) , де A_i, B_i $m \times n_i$ -матриці ($i = 1, 2$), вважаються *узагальнено еквівалентними*, якщо існують оборотні $m \times m$ -матриця X та $n_i \times n_i$ -матриці Y_i ($i = 1, 2$), що

$$XA_1Y_1 = B_1, \quad XA_2Y_2 = B_2.$$

Зауважимо, що у випадку $n_1 = n_2$ і $Y_1 = Y_2$ це означення збігається із класичним означенням еквівалентності пар матриць. Системний виклад дослідження узагальненої еквівалентності пар матриць над адекватними кільцями можна знайти в [68].

При вивченні різних класифікаційних матричних задач над кільцями актуальним є з'ясування, коли розглядувана задача містить задачу про подібність пар матриць над деяким полем.

Нехай K комутативне кільце з одиницею і його ідеал $J \neq K$. Якщо для матриць однакового розміру T та U над кільцем K всі елементи $T - U$ належать деякому ідеалу J кільця K , то це, як і раніше, позначатимемо $T \equiv U \pmod{J}$. (В цьому випадку матриці T та U називають *конгруентними за модулем J* .)

Означення 6.3. Будемо говорити, що дві $t \times n$ -матриці T та U над кільцем K є еквівалентними за модулем J , якщо для деякої оборотної $n \times n$ -матриці X над кільцем K і оборотної $t \times t$ матриці Y над кільцем K

$$T \equiv XUY \pmod{J}.$$

Аналогічно, будемо говорити, що матриці $n \times n$ -матриці T та U над кільцем K є подібними за модулем J , якщо для деякої оборотної $n \times n$ -матриці X над кільцем K

$$T \equiv X^{-1}UX \pmod{J}.$$

Якщо $J = 0$, то ми отримаємо класичні означення еквівалентності і подібності матриць. Якщо T та U еквівалентні або подібні за класичні означення, то вони, очевидно, відповідно еквівалентні або подібні за модулем любого ідеалу.

Означення 6.4. Нехай I та J ідеали кільця K , $I \neq K$, J — максимальний ідеал кільця K , $K\langle X, Y \rangle$ — асоціативна вільна алгебра над кільцем K від двох невідомих X та Y . Якщо існує блокова матриця $M(T, U)$ над кільцем K , кожний блок якої є значенням деякого полінома від квадратних матриць T, U і для довільних квадратних матриць T, U, T' та U' однакового розміру з еквівалентності матриць $M(T, U) M(T', U')$ за модулем I випливає подібність пар матриць (Y, U) і (Y', U') за модулем J , тоді задача описання матриць над кільцем K за модулем I називається дикою за модулем J .

6.3. Еквівалентність матриць над факторіальним кільцем

Нехай K область цілісності. Ми використовуватимемо позначення $a|b$ для запису того, що елемент a кільця K *ділить* його елемент b , тобто $b = ak$ для деякого $k \in K$. Необоротний елемент c кільця K називається *простим* елементом, якщо з умови $c = ab$ для деяких $a, b \in K$ випливає, що $a \in K^*$ або $b \in K^*$. Елементи a і b кільця K називають *асоційованими*, якщо $a = b\varepsilon$ для деякого $\varepsilon \in K^*$ (K^* — мультиплікативна група кільця K). Елементи a і b кільця K називають *неасоційованими* в іншому випадку.

Область цілісності K називається *факторіальним кільцем*, якщо в K існує система простих елементів P таких, що кожен ненульовий елемент $x \in K$ допускає єдине представлення

$$x = \varepsilon \prod_{p \in P} p^{s_p}$$

де ε оборотний елемент кільця K , а показники $s \geq 0$ не нульові тільки для скінченної кількості елементів. Число $l(x) = \sum_{p \in P} s_p$ називається довжиною елемента x .

Нехай далі в межах підрозділу K факторіальне кільце. Для простого елемента p кільця K та довільних елементів $x, y \in K$, якщо $p|xy$, то $p|x$ або $p|y$. Дійсно перевірку потребує випадок $x, y \notin K^*$. Розклад xy на прості множники можна одержати з умови $p|xy$ тоді він міститиме простий множник асоційований з p . Натомість розклад xy на прості отриманий з відповідних розкладів x та y при умові, що $p \nmid x$ та $p \nmid y$ не міститиме простий множник асоційований з p . Таким чином фактор-кільце K/pK цілісне. Нам знадобиться наступні прості лема.

Лема 6.5. Нехай t_1 і t_2 — неасоційовані прості елементи. Якщо

$$t_1^2x + t_2^2y + t_1t_2z \equiv 0 \pmod{t_1t_2tK}$$

($t \in K$), то $x, y, z \in t_1K + t_2K + tK$.

Доведення. Дійсно, із

$$t_1^2x + t_2^2y + t_1t_2z = t_1t_2tw$$

для $w \in K$ випливає, що $t_1(t_1x + t_2z - t_2tw) = -t_2^2y$. Тоді $t_1|t_2^2y$ і $t_1|y$. Тобто $y = t_1y'$ для деякого $y' \in K$. Отже, $t_1^2x + t_1t_2^2y' + t_1t_2z = t_1t_2tw$ і, враховуючи, що $t_1 \neq 0$, одержимо

$$t_1x + t_2^2y' + t_2z = t_2tw.$$

Звідси $t_2(t_2y' + z - tw) = -t_1x$, $t_2|t_1^2x$ і $t_2|x$. Тобто $x = t_2x'$ для деякого $x' \in K$. Отже, $t_1t_2x' + t_2^2y' + t_2z = t_2tw$ і, враховуючи, що $t_2 \neq 0$, одержимо

$$t_1x' + t_2y' + z = tw.$$

Таким чином $x = t_2x', y = t_1y', z = tw - t_1x' - t_2y' \in t_1K + t_2K + tK$. $\square$

Лема 6.6. Нехай t_1 і t_2 — неасоційовані прості елементи. Якщо

$$t_1^2x + t_2^2y + t_1t_2z \equiv 0 \pmod{t_1^2tK}$$

($t \in K$), то $x, y, z \in t_1K + t_2K + tK$.

Доведення. Дійсно, із

$$t_1^2x + t_2^2y + t_1t_2z = t_1^2tw$$

для $w \in K$ випливає, що $t_1(t_1x + t_2z - t_1tw) = -t_2^2y$. Тоді $t_1|t_2^2y$ і $t_1|y$. Тобто $y = t_1y'$ для деякого $y' \in K$. Отже, $t_1^2x + t_1t_2^2y' + t_1t_2z = t_1^2tw$ і, враховуючи, що $t_1 \neq 0$, одержимо

$$t_1x + t_2^2y' + t_2z = t_1tw.$$

Звідси $t_2(t_2y' + z) = t_1(tw - x)$, $t_2|t_1(x - tw)$ і $t_2|x - tw$. Тобто $x = t_2x' + tw$ для деякого $x' \in K$. Отже, $t_1t_2x' + t_1tw + t_2^2y' + t_2z = t_1tw$ і, враховуючи, що $t_2 \neq 0$, одержимо $t_1x' + t_2y' + z = 0$. Таким чином $x = t_2x' + tw$, $y = t_1y'$, $z = -t_1x' - t_2y' \in t_1K + t_2K + tK$. $\square$

Теорема 6.7. *Нехай K — факторіальне кільце, а $J \neq K$ — його ідеал, що має щонайменше два неасоційовані прості елементи. Тоді для будь-якого елемента $v \in J$, принаймні три з множників розкладу, якого на прості множники належать J , задача класифікації матриць над K за модулем vK є дика за модулем J .*

Доведення. Оскільки принаймні три з множників розкладу v на прості множники належать J , тоді $v = t_1t_2t$, де t_1, t_2 прості, а t є необоротний елемент ідеалу J .

Нехай t_1 та t_2 неасоційовані

$$t_1^2x + t_2^2y + t_1t_2z \equiv 0 \pmod{t_1t_2tK}$$

($t \in K$), то за лемою 6.5 $x, y, z \in t_1K + t_2K + tK \subset J$. Нехай A, B, A', B' довільні $n \times n$ -матриці над кільцем K , $M(A, B) = t_1^2A + t_2^2B + t_1t_2E_n$, де E_n одинична $n \times n$ -матриця над кільцем K . З еквівалентності матриць $M(A, B)$, $M(A', B')$ над K за модулем t_1t_2tK одержимо, що для деяких оборотних $n \times n$ -матриць X та Y над кільцем K $M(A, B) = XM(A', B')Y$. Тобто $t_1^2A + t_2^2B + t_1t_2E_n \equiv t_1^2XA'Y + t_2^2XB'Y + t_1t_2XY \pmod{t_1t_2tK}$. Звідси

$$\begin{aligned} E_n &\equiv XY \pmod{J}, & \text{а отже,} & & X &\equiv y^{-1} \pmod{J}, \\ A &\equiv XA'Y \pmod{J}, & \text{а отже,} & & A &\equiv Y^{-1}A'Y \pmod{J}, \\ B &\equiv XB'Y \pmod{J}, & \text{а отже,} & & B &\equiv Y^{-1}B'Y \pmod{J}. \end{aligned}$$

Отже, задача класифікації матриць над K за модулем t_1t_2tK у випадку, коли t_1 та t_2 неасоційовні, є дика за модулем J .

Нехай t_1 та t_2 асоційовані. Не зменшуючи загальності, можна вважати $t_1 = t_2$, Тоді $v = t_1^2 t$. Ідеал J містить також деякий простий елемент t'_2 неасоційований з t_1 . Якщо

$$t_1^2 x + t_2'^2 y + t_1 t'_2 z \equiv 0 \pmod{t_1^2 t K}$$

($t \in K$), то за лемою 6.6 $x, y, z \in t_1 K + t_2' K + t K \subset J$. Нехай A, B, A', B' довільні $n \times n$ -матриці над кільцем K , $M(A, B) = t_1^2 A + t_2'^2 B + t_1 t'_2 E_n$, де E_n одинична $n \times n$ -матриця над кільцем K . З еквівалентності матриць $M(A, B)$, $M(A', B')$ над K за модулем $t_1^2 t K$ одержимо, що для деяких оборотних $n \times n$ -матриць X та Y над кільцем K $M(A, B) = X M(A', B') Y$. Тобто

$$t_1^2 A + t_2'^2 B + t_1 t'_2 E_n \equiv t_1^2 X A' Y + t_2'^2 X B' Y + t_1 t'_2 X Y \pmod{t_1^2 t K}.$$

Звідси

$$\begin{aligned} E_n &\equiv X Y \pmod{J}, & \text{а отже,} & & X &\equiv Y^{-1} \pmod{J}, \\ A &\equiv X A' Y \pmod{J}, & \text{а отже,} & & A &\equiv Y^{-1} A' Y \pmod{J}, \\ B &\equiv X B' Y \pmod{J}, & \text{а отже,} & & B &\equiv Y^{-1} B' Y \pmod{J}. \end{aligned}$$

Отже, задача класифікації матриць над K за модулем vK є дика за модулем J . $\square$

Наслідок 6.8. *Нехай K — локальне факторіальне кільце, що не є областю головних ідеалів. Тоді для будь-якого елемента v довжини $l(v) > 2$ задача класифікації матриць над K за модулем vK є дика за модулем радикала Джекобсона кільця K .*

Доведення. Для доведення зауважимо тільки, що локальне факторіальне кільце K , що не є областю головних ідеалів має щонайменше два неасоційовані прості елементи. Крім того, радикал Джекобсона кільця K містить всі необоротні чи тим більше прості елементи. І наслідок негайно слідує з теореми 6.7. $\square$

Прикладом локального факторіального кільця, що має щонайменше два неасоційовані прості елементи є кільце формальних степеневих рядів $F[[x, y]]$ від двох змінних x, y над полем F .

6.4. Висновки до розділу

В розділі розглядаються класифікаційні матричні задачі над кільцями. У підрозділі 6.1 описано розв'язок задачі про пучок матриць та вводиться поняття дикої класифікаційної задачі. У підрозділі 6.2 описано розв'язок задачі про еквівалентність матриць над деякими класами кілець а також описано класи кілець над яким ця задача дика. Описується відношення узагальненої еквівалентності для пар матриць, що робить можливість розв'язати класифікаційну задачу над деякими класами кілець.

У підрозділі 6.3 досліджено, зв'язок між дикістю матричної задачі, про описання матриць над факторіальними кільцями з точністю до еквівалентності за модулем ідеалу і властивостями множини простих елементів даного кільця. Доведено 1) дикість за модулем максимального ідеалу задачі про описання, з точністю до еквівалентності за модулем ідеалу, матриць над факторіальними кільцем у випадку наявності простих елементів з вказаними властивостями; 2) дикість за модулем радикалу Джекобсона задачі про описання, з точністю до еквівалентності за модулем головного ідеалу породженого будь-яким елементом довжини більше 2, матриць над локальним факторіальними кільцем, що не є областю головних ідеалів.

Результати цього розділу анонсовано в [210] та опубліковані в [108].

РОЗДІЛ 7.

ЗАСТОСУВАННЯ В ТЕОРІЇ ГРУПОВИХ КІЛЕЦЬ І ТЕОРІЇ КОДІВ

Теорія зображень над комутативними кільцями знайшла численні застосування при вивченні як груп і пов'язаних з ними групових кілець так і матричних об'єктів, наприклад, кодів над тими ж кільцями.

7.1. Одиниці скінченного порядку цілочислового групового кільця групи $PSL(3, 4)$

Нехай G — скінченна група. Як і раніше,

$$V(\mathbb{Z}G) = \{u \in U(\mathbb{Z}G) | \varepsilon(u) = 1\}.$$

позначає нормалізовану мультиплікативну групу групового кільця $\mathbb{Z}G$, де $\varepsilon : \mathbb{Z}G \rightarrow \mathbb{Z}$,

$$\varepsilon \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} \alpha_g \quad (\alpha_g \in \mathbb{Z}, g \in G),$$

— поповнююче відображення кільця $\mathbb{Z}G$. Під одиницями скінченного порядку завжди розумітимемо нетривіальні одиниці скінченного порядку групи $V(\mathbb{Z}G)$. Досліджуватиметься гіпотеза Цассенхауза 1.23 про раціональну спряженість одиниць скінченного порядку з $V(\mathbb{Z}G)$ з елементами групи G .

В підрозділі досліджуються одиниці скінченного порядку групи $V(\mathbb{Z}G)$ для простої групи $G = PSL(3, 4)$. Відомо (див. також обчислення в GAP у додатку Б), що група G володіє 10-ма класами спряжених елементів. Класи подано в таблиці, де перше число позначення класу вказує на порядок всіх елементів класу.

Позначення класу	Порядки елементів	Число елементів
$1a$	1	1
$2a$	2	315
$3a$	3	2240
$4a$	4	1260
$4b$	4	1260
$4c$	4	1260
$5a$	5	4032
$5b$	5	4032
$7a$	7	2880
$7b$	7	2880

Відомі також таблиця характерів групи G та таблиці характерів Брауера, які можна одержати наведеними обчислення в GAP у додатку Б. Зокрема, (див. таблиця Б.1) можна одержати так впорядковану таблицю характерів групи G :

	$1a$	$2a$	$3a$	$4a$	$4b$	$4c$	$5a$	$5b$	$7a$	$7b$
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	20	4	2	0	0	0	0	0	-1	-1
χ_3	35	3	-1	3	-1	-1	0	0	0	0
χ_4	35	3	-1	-1	3	-1	0	0	0	0
χ_5	35	3	-1	-1	-1	3	0	0	0	0
χ_6	45	-3	0	1	1	1	0	0	B	$\overline{B}$
χ_7	45	-3	0	1	1	1	0	0	$\overline{B}$	B
χ_8	63	-1	0	-1	-1	-1	A	A^*	0	0
χ_9	63	-1	0	-1	-1	-1	A^*	A	0	0
χ_{10}	64	0	1	0	0	0	-1	-1	1	1

Тут і в наступних двох таблицях $A = -\alpha - \alpha^4$, $B = \zeta + \zeta^2 + \zeta^4$, $\alpha = e^{\frac{2\pi i}{5}}$ і $\zeta = e^{\frac{2\pi i}{7}}$, $\bar{B} = \zeta^3 + \zeta^5 + \zeta^6$ — комплексно спряжений елемент до B , $A^* = -\alpha^2 - \alpha^3$.

Крім того, таблиця характерів Брауера групи G , що відповідає характеристиці $p = 2$ (див. таблиця Б.2) має вигляд:

	$1a$	$3a$	$5a$	$5b$	$7a$	$7b$
χ_1	1	1	1	1	1	1
χ_2	8	-1	A	A^*	1	1
χ_3	8	-1	A^*	A	1	1
χ_4	9	0	-1	-1	B	$\bar{B}$
χ_5	9	0	-1	-1	$\bar{B}$	B
χ_6	64	1	-1	-1	1	1

А таблиця характерів Брауера групи G , що відповідає характеристиці $p = 3$ (див. таблиця Б.3) має вигляд:

	$1a$	$2a$	$4a$	$4b$	$4c$	$5a$	$5b$	$7a$	$7b$
χ_1	1	1	1	1	1	1	1	1	1
χ_2	15	-1	3	-1	-1	0	0	1	1
χ_3	15	-1	-1	3	-1	0	0	1	1
χ_4	15	-1	-1	-1	3	0	0	1	1
χ_5	19	3	-1	-1	-1	-1	-1	-2	-2
χ_6	45	-3	1	1	1	0	0	B	$\bar{B}$
χ_7	45	-3	1	1	1	0	0	$\bar{B}$	B
χ_8	63	-1	-1	-1	-1	A	A^*	0	0
χ_9	63	-1	-1	-1	-1	A^*	A	0	0

Головний результат підрозділу є теорема:

Теорема 7.1. Нехай $G = PSL(3, 4)$ і $u = \sum_{g \in G} \alpha_g g$ — одиниця скін-

ченного порядку групи $V(\mathbb{Z}G)$, $\nu_C = \varepsilon_C(u) = \sum_{g \in C} \alpha_g$ — значення часткового поповнюючого відображення, що відповідає класу спряжених елементів C групи G на одиниці u .

1) Якщо $|u| \in \{2, 3\}$, то u раціонально спряжена з деяким $g \in G$.

2) У $V(\mathbb{Z}G)$ немає елементів порядку 10, 12, 14, 15, 21 або 35.

3) Якщо $|u| = 4$, тоді $\nu_{rx} = 0$ для будь-якого $rx \notin \{2a, 4a, 4b, 4c\}$ і

$$(\nu_{2a}, \nu_{4a}, \nu_{4b}, \nu_{4c}) \in \{(2, -1, -1, 1), (2, -1, 0, 0), (0, -1, 0, 2), \\ (2, -1, 1, -1), (0, -1, 1, 1), (0, -1, 2, 0), \\ (-2, -1, 2, 2), (2, 0, -1, 0), (0, 0, -1, 2), \\ (2, 0, 0, -1), (0, 0, 0, 1), (0, 0, 1, 0), (-2, 0, 1, 2), \\ (0, 0, 2, -1), (-2, 0, 2, 1), (2, 1, -1, -1), \\ (0, 1, -1, 1), (0, 1, 0, 0), (-2, 1, 0, 2), (0, 1, 1, -1), \\ (-2, 1, 1, 1), (-2, 1, 2, 0), (0, 2, -1, 0), (-2, 2, -1, 2), \\ (0, 2, 0, -1), (-2, 2, 0, 1), \\ (-2, 2, 1, 0), (-2, 2, 2, -1)\}.$$

4) Якщо $|u| = 5$, то $\nu_{rx} = 0$ $rx \notin \{5a, 5b\}$ і

$$(\nu_{5a}, \nu_{5b}) \in \{(2, -1), (1, 0), (0, 1), (-1, 2)\}.$$

5) Якщо $|u| = 7$, то $\nu_{rx} = 0$ $rx \notin \{7a, 7b\}$ і

$$(\nu_{7a}, \nu_{7b}) \in \{(2, -1), (1, 0), (0, 1), (-1, 2)\}.$$

6) Якщо $|u| = 6$, тоді $\nu_{rx} = 0$ $rx \notin \{2a, 3a\}$ і

$$(\nu_{2a}, \nu_{3a}) \in \{(4, -3), (-2, 3)\}.$$

Опишемо твердження, які застосовуються для доведення теореми, про одиниці скінченного порядку групи $V(\mathbb{Z}G)$ для довільної скінченної групи G . Нехай $u = \sum_{g \in G} \alpha_g g$ — одиниця скінченного порядку групи $V(\mathbb{Z}G)$,

$$G = C_1 \cup C_2 \cup \dots \cup C_l$$

— об'єднання неперетинаючихся класів спряжених елементів групи G записаних у деякому порядку, такому, що $C_1 = \{1\}$, l — число класів спряжених елементів групи G , $\nu_i = \varepsilon_{C_i}(u) = \sum_{g \in C_i} \alpha_g$ — значення i -вого часткового поповнюючого відображення на одиниці u . За лемою 1.25 $\nu_1 = 0$ і $\nu_j = 0$, якщо клас спряжених елементів C_j складається з центрального елемента. Тому $\nu_2 + \nu_3 + \dots + \nu_l = \sum_{i=1}^l \nu_i = \sum_{i=1}^l \sum_{g \in C_i} \alpha_g = \sum_{g \in \bigcup_{i=1}^l C_i} \alpha_g = \sum_{g \in G} \alpha_g = \varepsilon(u) = 1$, оскільки $u \in V(\mathbb{Z}G)$.

Твердження 7.2 ([133]). *Якщо u — одиниця скінченного порядку з $V(\mathbb{Z}G)$, то порядок u ділить показник групи G .*

Наступні твердження забезпечують взаємозв'язок між частковими поповнюючими відображеннями та порядком одиниць.

Твердження 7.3 ([182, теорема 2.7], [160, твердження 3.1]). *Нехай u — одиниця $V(\mathbb{Z}G)$ скінченного порядку, $x \in G$ і $\varepsilon_x(u) \neq 0$, то порядок x ділить порядок u .*

З твердження 7.3, зокрема, випливає, що для одиниці $u \in V(\mathbb{Z}G)$ скінченного порядку і $x \in G$, якщо існує простий дільник p порядку x , але не порядку u , то часткове поповнююче відображення $\varepsilon_x(u) = 0$. Крім того, одержуємо також твердження.

Твердження 7.4 ([161, твердження 2.2]). *Нехай u — одиниця $V(\mathbb{Z}G)$ скінченного порядку, $x \in G$. Якщо p -частина елемента x для деякого*

простого числа p має строго більший порядок ніж порядок p -частини u , то $\varepsilon_x(u) = 0$.

Очевидно, для будь-якого характеру χ групи G та будь-якої одиниці u скінченного порядку з $V(\mathbb{Z}G)$ $\chi(u) = \chi(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} \alpha_g \chi(g) = \sum_{g \in \cup_{i=1}^l C_i} \alpha_g \chi(g) = \sum_{i=1}^l \sum_{g \in C_i} \alpha_g \chi(g) = \sum_{i=1}^l \sum_{g \in C_i} \alpha_g \chi(h_i) = \sum_{i=2}^l \nu_i \chi(h_i)$, де h_i — представник класу спряжених елементів C_i .

Нехай h — натуральне число, z — первісний корінь h -ї степені з одиниці, $Gal(\mathbb{Q}(z)/\mathbb{Q})$ — група Галуа розширення $\mathbb{Q}(z)$ поля раціональних чисел $\mathbb{Q}$. Будемо позначати

$$\mathrm{Tr}_{\mathbb{Q}(z^d)/\mathbb{Q}}(x) = \sum_{\sigma \in Gal(\mathbb{Q}(z)/\mathbb{Q})} \sigma(x) \quad (x \in \mathbb{Q}(z)).$$

Очевидно, якщо $x \in \mathbb{Q}$, то $\sigma(x) = x$ і

$$\mathrm{Tr}_{\mathbb{Q}(z)/\mathbb{Q}}(x) = \sum_{\sigma \in Gal(\mathbb{Q}(z)/\mathbb{Q})} x = x \cdot \sum_{\sigma \in Gal(\mathbb{Q}(z)/\mathbb{Q})} 1 = x\varphi(h),$$

де φ — функція Ейлера.

Твердження 7.5 ([177, теорема 1], [161]). *Нехай p дорівнює нулю або є простий дільник $|G|$. Припустимо, що u — одиниця $V(\mathbb{Z}G)$ скінченного порядку k . Нехай z — первісний корінь k -ї степені з одиниці. Тоді для кожного цілого j і будь-якого характеру χ групи G (при $p = 0$) чи будь-якого характеру Брауера χ групи G , що відповідає характеристиці p (при $p > 0$), число*

$$\mu_j(u, \chi, p) = \frac{1}{k} \sum_{d|k} \mathrm{Tr}_{\mathbb{Q}(z^d)/\mathbb{Q}} \{ \chi(u^d) z^{-dj} \} \quad (7.1)$$

є невід'ємним цілим числом.

Ми будемо використовувати позначення $\mu_j(u, \chi, *)$ замість $\mu_j(u, \chi, p)$, коли $p = 0$.

Доведення теореми 7.1 Нехай $G = PSL(3, 4)$. Спочатку за лемою 1.25 для будь-якої одиниці $u \in V(\mathbb{Z}G)$ скінченного порядку ми маємо $\nu_{1a} = 0$. З формулою (7.1) маємо

$$\nu_{2a} + \nu_{3a} + \nu_{4a} + \nu_{4b} + \nu_{4c} + \nu_{5a} + \nu_{5b} + \nu_{7a} + \nu_{7b} = 1.$$

За рівністю (1.3) для відповідних харктерів $\chi_1, \chi_2, \dots, \chi_{10}$ групи G отримуємо

$$\begin{pmatrix} \chi_1(u) \\ \chi_2(u) \\ \vdots \\ \chi_{10}(u) \end{pmatrix} = X(G) \begin{pmatrix} \nu_{1a} \\ \nu_{2a} \\ \nu_{3a} \\ \nu_{4a} \\ \nu_{4b} \\ \nu_{4c} \\ \nu_{5a} \\ \nu_{5b} \\ \nu_{7a} \\ \nu_{7b} \end{pmatrix} = X(G) \begin{pmatrix} 0 \\ \nu_{2a} \\ \nu_{3a} \\ \nu_{4a} \\ \nu_{4b} \\ \nu_{4c} \\ \nu_{5a} \\ \nu_{5b} \\ \nu_{7a} \\ \nu_{7b} \end{pmatrix},$$

де $X(G) = (\chi_i(x_j))$ — таблиця характерів групи G . За таблицею Б.1

отримаємо в розгорнутому вигляді

$$\begin{pmatrix} \chi_1(u) \\ \chi_2(u) \\ \chi_3(u) \\ \chi_4(u) \\ \chi_5(u) \\ \chi_6(u) \\ \chi_7(u) \\ \chi_8(u) \\ \chi_9(u) \\ \chi_{10}(u) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 20 & 4 & 2 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ 35 & 3 & -1 & 3 & -1 & -1 & 0 & 0 & 0 & 0 \\ 35 & 3 & -1 & -1 & 3 & -1 & 0 & 0 & 0 & 0 \\ 35 & 3 & -1 & -1 & -1 & 3 & 0 & 0 & 0 & 0 \\ 45 & -3 & 0 & 1 & 1 & 1 & 0 & 0 & B & \bar{B} \\ 45 & -3 & 0 & 1 & 1 & 1 & 0 & 0 & \bar{B} & B \\ 63 & -1 & 0 & -1 & -1 & -1 & A & A^* & 0 & 0 \\ 63 & -1 & 0 & -1 & -1 & -1 & A^* & A & 0 & 0 \\ 64 & 0 & 1 & 0 & 0 & 0 & -1 & -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ \nu_{2a} \\ \nu_{3a} \\ \nu_{4a} \\ \nu_{4b} \\ \nu_{4c} \\ \nu_{5a} \\ \nu_{5b} \\ \nu_{7a} \\ \nu_{7b} \end{pmatrix}.$$

Або більш компактно

$$\begin{pmatrix} \chi_2(u) \\ \chi_3(u) \\ \chi_4(u) \\ \chi_5(u) \\ \chi_6(u) \\ \chi_7(u) \\ \chi_8(u) \\ \chi_9(u) \\ \chi_{10}(u) \end{pmatrix} = \begin{pmatrix} 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ 3 & -1 & 3 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 3 & -1 & -1 & 3 & -1 & 0 & 0 & 0 & 0 & 0 \\ 3 & -1 & -1 & -1 & 3 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 1 & 1 & 0 & 0 & B & \bar{B} \\ -3 & 0 & 1 & 1 & 1 & 0 & 0 & \bar{B} & B \\ -1 & 0 & -1 & -1 & -1 & A & A^* & 0 & 0 \\ -1 & 0 & -1 & -1 & -1 & A^* & A & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \nu_{2a} \\ \nu_{3a} \\ \nu_{4a} \\ \nu_{4b} \\ \nu_{4c} \\ \nu_{5a} \\ \nu_{5b} \\ \nu_{7a} \\ \nu_{7b} \end{pmatrix}. \quad (7.2)$$

Аналогічні формули за таблицею Б.2 для відповідних характерів Брауера $\chi_1, \chi_2, \chi_3, \dots, \chi_6$, що відповідають характеристиці $p = 2$, набудуть

вигляду

$$\begin{pmatrix} \chi_2(u) \\ \chi_3(u) \\ \chi_4(u) \\ \chi_5(u) \\ \chi_6(u) \end{pmatrix} = \begin{pmatrix} -1 & A & A^* & 1 & 1 \\ -1 & A^* & A & 1 & 1 \\ 0 & -1 & -1 & B & \bar{B} \\ 0 & -1 & -1 & \bar{B} & B \\ 1 & -1 & -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \nu_{3a} \\ \nu_{5a} \\ \nu_{5b} \\ \nu_{7a} \\ \nu_{7b} \end{pmatrix}. \quad (7.3)$$

Також за таблицею Б.3 отримаємо формули для відповідних характерів Брауера $\chi_1, \chi_2, \dots, \chi_9$, що відповідають характеристиці $p = 3$,

$$\begin{pmatrix} \chi_2(u) \\ \chi_3(u) \\ \chi_4(u) \\ \chi_5(u) \\ \chi_6(u) \\ \chi_7(u) \\ \chi_8(u) \\ \chi_9(u) \end{pmatrix} = \begin{pmatrix} -1 & 3 & -1 & -1 & 0 & 0 & 1 & 1 \\ -1 & -1 & 3 & -1 & 0 & 0 & 1 & 1 \\ -1 & -1 & -1 & 3 & 0 & 0 & 1 & 1 \\ 3 & -1 & -1 & -1 & -1 & -1 & -2 & -2 \\ -3 & 1 & 1 & 1 & 0 & 0 & B & \bar{B} \\ -3 & 1 & 1 & 1 & 0 & 0 & \bar{B} & B \\ -1 & -1 & -1 & -1 & A & A^* & 0 & 0 \\ -1 & -1 & -1 & -1 & A^* & A & 0 & 0 \end{pmatrix} \begin{pmatrix} \nu_{2a} \\ \nu_{4a} \\ \nu_{4b} \\ \nu_{4c} \\ \nu_{5a} \\ \nu_{5b} \\ \nu_{7a} \\ \nu_{7b} \end{pmatrix}. \quad (7.4)$$

Випадок (i). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 2. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{3a, 4a, 4b, 4c, 5a, 5b, 7a, 7b\}$. Тому u раціонально спряжена з деяким елементом $g \in G$ за твердженням 1.24.

Випадок (ii). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 3. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{2a, 4a, 4b, 4c, 5a, 5b, 7a, 7b\}$. Тому u раціонально спряжена з деяким елементом $g \in G$ за твердженням 1.24.

Випадок (iii). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 4. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{3a, 5a, 5b, 7a, 7b\}$. Отже, $1 = \varepsilon(u) = \nu_{2a} + \nu_{4a} + \nu_{4b} + \nu_{4c}$. Оскільки $u^2 \in V(\mathbb{Z}G)$ має порядок 2, то за випадком (i) елемент u^2 раціонально спряжений з елементом групи G порядку 2. А в групі G елементи порядку 2 вичерпуються елементами класу $2a$. Тоді

$\chi(u^2) = \chi(2a)$ для довільного характеру χ групи G . Нехай z — первісний корінь 4-го степеня з 1 ($z^2 = -1$).

Тоді, наприклад,

$$\begin{aligned} \mu_0(u, \chi_2, *) &= \frac{1}{4} \sum_{d|4} \text{Tr}_{\mathbb{Q}(z^d)/\mathbb{Q}} \{ \chi_2(u^d) z^0 \} = \\ &= \frac{1}{4} \left(\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}} \{ \chi_2(u) \} + \text{Tr}_{\mathbb{Q}(z^2)/\mathbb{Q}} \{ \chi_2(u^2) \} + \text{Tr}_{\mathbb{Q}(z^4)/\mathbb{Q}} \{ \chi_2(u^4) \} \right). \end{aligned}$$

Оскільки $\mathbb{Q}(z^2) = \mathbb{Q}(-1) = \mathbb{Q}(z^4) = \mathbb{Q}(1) = \mathbb{Q}$ а група Галуа $\text{Gal}(\mathbb{Q}(z)/\mathbb{Q})$ розширення $\mathbb{Q}(z)$ поля раціональних чисел $\mathbb{Q}$ складається з двох елементів $z \rightarrow z, z \rightarrow z^3 = z^{-1} = \bar{z}$, то

$$\begin{aligned} \mu_0(u, \chi_2, *) &= \frac{1}{4} \left(\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}} \{ \chi_2(u) \} + \chi_2(2a) + \chi_2(1) \right) = \\ &= \frac{1}{4} \left(\chi_2(u) + \overline{\chi_2(u)} + 4 + 20 \right) = \frac{1}{4} \left(\chi_2(u) + \overline{\chi_2(u)} + 24 \right). \end{aligned}$$

За формулою 7.2 $\chi_2(u) = 4\nu_{2a} \in \mathbb{Z}$ і

$$\mu_2(u, \chi_2, *) = \frac{1}{4} (4\nu_{2a} + \overline{4\nu_{2a}} + 24) = \frac{1}{4} (8\nu_{2a} + 24).$$

Крім того,

$$\begin{aligned} \mu_2(u, \chi_2, *) &= \frac{1}{4} \sum_{d|4} \text{Tr}_{\mathbb{Q}(z^d)/\mathbb{Q}} \{ \chi_2(u^d) z^{-d^2} \} = \\ &= \frac{1}{4} \left(\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}} \{ \chi_2(u) z^{-2} \} + \text{Tr}_{\mathbb{Q}(z^2)/\mathbb{Q}} \{ \chi_2(u^2) z^{-4} \} + \text{Tr}_{\mathbb{Q}(z^4)/\mathbb{Q}} \{ \chi_2(u^4) z^{-8} \} \right). \end{aligned}$$

Оскільки $\mathbb{Q}(z^2) = \mathbb{Q}(z^4) = \mathbb{Q}$ а група $\text{Gal}(\mathbb{Q}(z)/\mathbb{Q})$ складається з двох елементів $z \rightarrow z, z \rightarrow z^3 = z^{-1} = \bar{z}$, то

$$\begin{aligned} \mu_2(u, \chi_2, *) &= \frac{1}{4} \left(\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}} \{ -\chi_2(u) \} + \chi_2(2a) + \chi_2(1) \right) = \\ &= \frac{1}{4} \left(-\chi_2(u) - \overline{\chi_2(u)} + 4 + 20 \right) = \frac{1}{4} \left(-\chi_2(u) - \overline{\chi_2(u)} + 24 \right). \end{aligned}$$

За формулою 7.2 $\chi_2(u) = 4\nu_{2a} \in \mathbb{Z}$ і

$$\mu_2(u, \chi_2, *) = \frac{1}{4} (-4\nu_{2a} - \overline{4\nu_{2a}} + 24) = \frac{1}{4} (-8\nu_{2a} + 24).$$

Пакет LAGUNA [123] для система GAP [145] використовувався для багаторазового обчислення $\mu_j(u, \chi, p)$. Застосування формул (7.2) та (7.4) до твердження 7.5 дає таку систему нерівностей:

$$\begin{aligned}\mu_0(u, \chi_2, *) &= \frac{1}{4}(8\nu_{2a} + 24) \geq 0; & \mu_2(u, \chi_2, *) &= \frac{1}{4}(-8\nu_{2a} + 24) \geq 0; \\ \mu_0(u, \chi_3, *) &= \frac{1}{4}(2\gamma_1 + 38) \geq 0; & \mu_2(u, \chi_3, *) &= \frac{1}{4}(-2\gamma_1 + 38) \geq 0; \\ \mu_0(u, \chi_4, *) &= \frac{1}{4}(2\gamma_2 + 38) \geq 0; & \mu_2(u, \chi_4, *) &= \frac{1}{4}(-2\gamma_2 + 38) \geq 0; \\ \mu_0(u, \chi_2, 3) &= \frac{1}{4}(-\gamma_3 + 14) \geq 0; & \mu_2(u, \chi_2, 3) &= \frac{1}{4}(\gamma_3 + 14) \geq 0; \\ \mu_0(u, \chi_3, 3) &= \frac{1}{4}(-\gamma_4 + 14) \geq 0; & \mu_2(u, \chi_3, 3) &= \frac{1}{4}(\gamma_4 + 14) \geq 0; \\ \mu_0(u, \chi_4, 3) &= \frac{1}{4}(-\gamma_5 + 14) \geq 0; & \mu_2(u, \chi_4, 3) &= \frac{1}{4}(\gamma_5 + 14) \geq 0; \\ \mu_0(u, \chi_5, 3) &= \frac{1}{4}(-\gamma_6 + 22) \geq 0; & \mu_2(u, \chi_5, 3) &= \frac{1}{4}(\gamma_6 + 22) \geq 0,\end{aligned}$$

де

$$\begin{aligned}\gamma_1 &= 3\nu_{2a} + 3\nu_{4a} - \nu_{4b} - \nu_{4c}, & \gamma_2 &= 3\nu_{2a} - \nu_{4a} + 3\nu_{4b} - \nu_{4c}, \\ \gamma_3 &= 2\nu_{2a} - 6\nu_{4a} + 2\nu_{4b} + 2\nu_{4c}, & \gamma_4 &= 2\nu_{2a} + 2\nu_{4a} - 6\nu_{4b} + 2\nu_{4c}, \\ \gamma_5 &= 2\nu_{2a} + 2\nu_{4a} + 2\nu_{4b} - 6\nu_{4c} & \text{і} & \gamma_6 = 6\nu_{2a} - 2\nu_{4a} - 2\nu_{4b} - 2\nu_{4c}.\end{aligned}$$

Розв'язуючи систему нерівностей та враховуючи, що ліві їх частини є цілі числа, одержимо, що $\nu_{2a} \in \{i \mid -3 \leq i \leq 3\}$, $\gamma_1, \gamma_2 \in \{1 + 2i \mid -10 \leq i \leq 9\}$ і $\gamma_3, \gamma_4, \gamma_5 \in \{2 + 4i \mid -4 \leq i \leq 3\}$. Враховуючи, що $\nu_{2a} + \nu_{4a} + \nu_{4b} + \nu_{4c} = 1$, одержуємо, що єдині можливі розв'язки для $(\nu_{2a}, \nu_{4a}, \nu_{4b}, \nu_{4c})$ наведено в частині 3) теореми 7.1.

Випадок (iv). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 5. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{2a, 3a, 4a, 4b, 4c, 7a, 7b\}$. Отже, $1 = \varepsilon(u) = \nu_{5a} + \nu_{5b}$. Застосування формул (7.3) до твердження 7.5 дає таку систему нерівностей:

$$\mu_1(u, \chi_2, 2) = \frac{1}{5}(\gamma_1 + 8) \geq 0; \quad \mu_2(u, \chi_2, 2) = \frac{1}{5}(\gamma_2 + 8) \geq 0,$$

де $\gamma_1 = -3\nu_{5a} + 2\nu_{5b}$ і $\gamma_2 = 2\nu_{5a} - 3\nu_{5b}$. Звідси враховуючи, що $\nu_{5a} + \nu_{5b} = 1$ одержимо, що єдині можливі розв'язки для (ν_{5a}, ν_{5b}) наведено в частині 4) теореми 7.1.

Випадок (v). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 7. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{2a, 3a, 4a, 4b, 4c, 5a, 5b\}$. Отже, $1 = \varepsilon(u) = \nu_{7a} + \nu_{7b}$. Застосування формул (7.2) та (7.3) до твердження 7.5 дає таку систему нерівностей:

$$\begin{aligned}\mu_1(u, \chi_6, *) &= \frac{1}{7}(\gamma_1 + 45) \geq 0; & \mu_3(u, \chi_6, *) &= \frac{1}{7}(\gamma_2 + 45) \geq 0; \\ \mu_1(u, \chi_4, 2) &= \frac{1}{7}(\gamma_3 + 9) \geq 0; & \mu_3(u, \chi_4, 2) &= \frac{1}{7}(\gamma_4 + 9) \geq 0,\end{aligned}$$

де $\gamma_1 = 4\nu_{7a} - 3\nu_{7b}$, $\gamma_2 = -3\nu_{7a} + 4\nu_{7b}$, $\gamma_3 = 5\nu_{7a} - 2\nu_{7b}$ і $\gamma_4 = -2\nu_{7a} + 5\nu_{7b}$. Звідси враховуючи, що $\nu_{7a} + \nu_{7b} = 1$ одержуємо, що єдині можливі розв'язки для (ν_{7a}, ν_{7b}) наведено в частині 5) теореми 7.1.

Випадок (vi). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 6. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{4a, 4b, 4c, 5a, 5b, 7a, 7b\}$. Отже, $1 = \varepsilon(u) = \nu_{2a} + \nu_{3b}$. Застосування формул (7.2) до твердження 7.5 дає таку систему нерівностей:

$$\begin{aligned}\mu_0(u, \chi_2, *) &= \frac{1}{6}(4\gamma_1 + 28) \geq 0; & \mu_3(u, \chi_2, *) &= \frac{1}{6}(-4\gamma_1 + 20) \geq 0; \\ \mu_0(u, \chi_3, *) &= \frac{1}{6}(\gamma_2 + 36) \geq 0; & \mu_1(u, \chi_6, *) &= \frac{1}{6}(-3\nu_{2a} + 48) \geq 0,\end{aligned}$$

де $\gamma_1 = 2\nu_{2a} + \nu_{3a}$ і $\gamma_2 = 6\nu_{2a} - 2\nu_{3a}$. Ясно, що $2\gamma_1 + 14 \equiv -2\gamma_1 + 10 \equiv 0 \pmod{3}$. Тоді $\gamma_1 + 7 \equiv -\gamma_1 + 5 \equiv 0 \pmod{3}$ і $\gamma_1 \equiv 2 \pmod{3}$. Звідси $\gamma_1 \in \{-7, -4, -1, 2, 5\}$. Тому враховуючи, що $\nu_{2a} + \nu_{3b} = 1$, одержимо, що єдині можливі розв'язки для (ν_{2a}, ν_{3a}) наведено в частині 6) теореми 7.1.

Випадок (vii). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 10. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{3a, 4a, 4b, 4c, 7a, 7b\}$. Отже, $1 = \varepsilon(u) = \nu_{2a} + \nu_{5a} + \nu_{5b}$. Очевидно, $u^5, u^2 \in V(\mathbb{Z}G)$ — одиниці відповідно порядків 2 та 5. З доведених властивостей таких одиниць $\chi(u^5) = \chi(2a)$ і $\chi(u^2) = m_1\chi(5a) + m_2\chi(5b)$, де $(m_1, m_2) \in \{(1, 0), (0, 1), (2, -1), (-1, 2)\}$. Застосування формул (7.2) до твердження 7.5 дає таку систему нерівно-

стей:

$$\begin{aligned}\mu_0(u, \chi_2, *) &= \frac{1}{10}(16\nu_{2a} + 24) \geq 0; \quad \mu_5(u, \chi_2, *) = \frac{1}{10}(-16\nu_{2a} + 16) \geq 0. \\ \mu_1(u, \chi_3, *) &= \frac{1}{10}(3\nu_{2a} + 32) \geq 0.\end{aligned}$$

Зрозуміло, що $-1 \leq \nu_{2a} \leq 1$. Крім того, $8\nu_{2a} + 12 \equiv 0 \pmod{5}$, $2\nu_{2a} + 3 \equiv 0 \pmod{5}$, і $\nu_{2a} \equiv 1 \pmod{5}$. Тоді $\nu_{2a} = 1$. Але тоді $\mu_1(u, \chi_3, *) = \frac{35}{10} = \frac{7}{2}$ не є цілими, що неможливо.

Випадок (viii). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 12. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{5a, 5b, 7a, 7b\}$. Отже, $1 = \varepsilon(u) = \nu_{2a} + \nu_{3a} + \nu_{4a} + \nu_{4b} + \nu_{4c}$. Очевидно, $u^6, u^4, u^3, u^2 \in V(\mathbb{Z}G)$ — одиниці відповідно порядків 2, 3, 4 та 6. З доведених властивостей таких одиниць $\chi(u^6) = \chi(2a)$, $\chi(u^4) = \chi(3a)$, $\chi(u^3) = m_1\chi(2a) + m_2\chi(4a) + m_3\chi(4b) + m_4\chi(4c)$, де $(m_1, m_2, m_3, m_4) \in \{(2, -1, -1, 1), (2, -1, 0, 0), (0, -1, 0, 2), (2, -1, 1, -1), (0, -1, 1, 1), (0, -1, 2, 0), (-2, -1, 2, 2), (2, 0, -1, 0), (0, 0, -1, 2), (2, 0, 0, -1), (0, 0, 0, 1), (0, 0, 1, 0), (-2, 0, 1, 2), (0, 0, 2, -1), (-2, 0, 2, 1), (2, 1, -1, -1), (0, 1, -1, 1), (0, 1, 0, 0), (-2, 1, 0, 2), (0, 1, 1, -1), (-2, 1, 1, 1), (-2, 1, 2, 0), (0, 2, -1, 0), (-2, 2, -1, 2), (0, 2, 0, -1), (-2, 2, 0, 1), (-2, 2, 1, 0), (-2, 2, 2, -1)\}$ та $\chi(u^2) = m_5\chi(2a) + m_6\chi(3a)$, де $(m_5, m_6) \in \{(4, -3), (-2, 3)\}$. Нехай z — первісний корінь 12-го степеня з 1 ($z^6 = -1$).

Тоді, наприклад,

$$\begin{aligned}\mu_3(u, \chi_2, *) &= \frac{1}{12} \sum_{d|12} \text{Tr}_{\mathbb{Q}(z^d)/\mathbb{Q}} \{ \chi_2(u^d) z^{-3d} \} = \\ &= \frac{1}{12} (\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}} \{ \chi_2(u) z^{-3} \} + \text{Tr}_{\mathbb{Q}(z^2)/\mathbb{Q}} \{ \chi_2(u^2) z^{-6} \} + \text{Tr}_{\mathbb{Q}(z^3)/\mathbb{Q}} \{ \chi_2(u^3) z^{-9} \} + \\ &+ \text{Tr}_{\mathbb{Q}(z^4)/\mathbb{Q}} \{ \chi_2(u^4) z^{-12} \} + \text{Tr}_{\mathbb{Q}(z^6)/\mathbb{Q}} \{ \chi_2(u^6) z^{-18} \} + \text{Tr}_{\mathbb{Q}(z^{12})/\mathbb{Q}} \{ \chi_2(u^{12}) z^{-36} \}) = \\ &= \frac{1}{12} (\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}} \{ \chi_2(u) z^{-3} \} + \text{Tr}_{\mathbb{Q}(z^2)/\mathbb{Q}} \{ -\chi_2(u^2) \} + \text{Tr}_{\mathbb{Q}(z^3)/\mathbb{Q}} \{ \chi_2(u^3) z^3 \} + \\ &+ \text{Tr}_{\mathbb{Q}(z^4)/\mathbb{Q}} \{ \chi_2(u^4) \} + \text{Tr}_{\mathbb{Q}(z^6)/\mathbb{Q}} \{ -\chi_2(u^6) \} + \text{Tr}_{\mathbb{Q}(z^{12})/\mathbb{Q}} \{ \chi_2(u^{12}) \}) .\end{aligned}$$

Оскільки за формулою 7.2 $\chi_2(u) = 4\nu_{2a} + 2\nu_{3a}$, $\chi_2(u^2), \chi_2(u^3), \chi_2(u^4) \in \mathbb{Z}$ і $\mathbb{Q}(z^{12}) = \mathbb{Q}(z^6) = \mathbb{Q}$ а $|Gal(\mathbb{Q}(z^4)/\mathbb{Q})| = |Gal(\mathbb{Q}(z^3)/\mathbb{Q})| = |Gal(\mathbb{Q}(z^2)/\mathbb{Q})| = 2$, $|Gal(\mathbb{Q}(z)/\mathbb{Q})| = 4$, то

$$\mu_3(u, \chi_2, *) = \frac{1}{12} (\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}}\{\chi_2(u)z^{-3}\} - 4\chi_2(u^2) + \text{Tr}_{\mathbb{Q}(z^3)/\mathbb{Q}}\{\chi_2(u^3)z^3\} + 2 \cdot 2 - 4 + 20).$$

Очевидно, група $Gal(\mathbb{Q}(z)/\mathbb{Q})$ складається з гомоморфізмів $z \rightarrow z$, $z \rightarrow z^5$, $z \rightarrow z^7$, $z \rightarrow z^{11} = z^{-1} = \bar{z}$ а $Gal(\mathbb{Q}(z^3)/\mathbb{Q})$ складається з гомоморфізмів $z^3 \rightarrow z^3$, $z^3 \rightarrow z^{-3} = \bar{z}^3$ і

$$\text{Tr}_{\mathbb{Q}(z)/\mathbb{Q}}\{z^{-3}\} = z^{-3} + z^{-15} + z^{-21} + z^{-33} = z^{-3} + z^{-3} + z^3 + z^3 = 0,$$

$$\text{Tr}_{\mathbb{Q}(z^3)/\mathbb{Q}}\{z^3\} = z^3 + z^{-3} = 0.$$

Тоді

$$\begin{aligned} \mu_3(u, \chi_2, *) &= \frac{1}{12} (-4\chi_2(u^2) + 20) = \frac{1}{12} (-4(4m_5 + 2m_6) + 20) = \\ &= \frac{1}{3} (-(4m_5 + 2m_6) + 5), \end{aligned}$$

де $(m_5, m_6) \in \{(4, -3), (-2, 3)\}$.

За твердження 7.5 $\mu_3(u, \chi_2, *) \in \mathbb{Z}$ і, отже, $-(4m_5 + 2m_6) + 5 \equiv 0 \pmod{3}$. Але для $(m_5, m_6) = (4, -3)$ маємо $-(4m_5 + 2m_6) + 5 \equiv -10 + 5 \equiv 1 \pmod{3}$ а для $(m_5, m_6) = (-2, 3)$ теж маємо $-(4m_5 + 2m_6) + 5 \equiv 2 + 5 \equiv 1 \pmod{3}$, що неможливо.

Випадок (ix). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 14. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{3a, 4a, 4b, 4c, 5a, 5b\}$. Отже, $1 = \varepsilon(u) = \nu_{2a} + \nu_{7a} + \nu_{7b}$. Очевидно, $u^7, u^2 \in V(\mathbb{Z}G)$ — одиниці відповідно порядків 2 та 7. З доведених властивостей таких одиниць $\chi(u^7) = \chi(2a)$ і $\chi(u^2) = m_1\chi(7a) + m_2\chi(7b)$, де $(m_1, m_2) \in \{(1, 0), (0, 1), (2, -1), (-1, 2)\}$.

Застосування формул (7.2) до твердження 7.5 дає таку систему нерівностей:

$$\mu_0(u, \chi_2, *) = \frac{1}{14}(6\gamma_1 + 18) \geq 0; \quad \mu_7(u, \chi_2, *) = \frac{1}{14}(-6\gamma_1 + 10) \geq 0;$$

де $\gamma_1 = 4\nu_{2a} - \nu_{7a} - \nu_{7b}$. Ясно, що $-3 \leq \gamma_1 \leq 1$. За твердження 7.5 $\mu_0(u, \chi_2, *) \in \mathbb{Z}$ і, отже, $3\gamma_1 + 9 \equiv 0 \pmod{7}$. Тобто $\gamma_1 \equiv -3 \equiv 4 \pmod{7}$ і $\gamma_1 = -3$. Таким чином

$$\begin{cases} \nu_{2a} + \nu_{7a} + \nu_{7b} = 1 \\ 4\nu_{2a} - \nu_{7a} - \nu_{7b} = -3, \end{cases}$$

ліва частина суми $5\nu_{2a} = -2$ рівнянь системи ділиться на 5 при будь-якому цілому ν_{2a} а права — ні. Отже, шуканих цілих значень $\nu_{2a}, \nu_{7a}, \nu_{7b}$ не існує.

Випадок (ix). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 14. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{3a, 4a, 4b, 4c, 5a, 5b\}$. Отже, $1 = \varepsilon(u) = \nu_{2a} + \nu_{7a} + \nu_{7b}$. Очевидно, $u^7, u^2 \in V(\mathbb{Z}G)$ — одиниці відповідно порядків 2 та 7. З доведених властивостей таких одиниць $\chi(u^7) = \chi(2a)$ і $\chi(u^2) = m_1\chi(7a) + m_2\chi(7b)$, де $(m_1, m_2) \in \{(1, 0), (0, 1), (2, -1), (-1, 2)\}$. Застосування формул (7.2) до твердження 7.5 дає таку систему нерівностей:

$$\mu_0(u, \chi_2, *) = \frac{1}{14}(6\gamma_1 + 18) \geq 0; \quad \mu_7(u, \chi_2, *) = \frac{1}{14}(-6\gamma_1 + 10) \geq 0;$$

де $\gamma_1 = 4\nu_{2a} - \nu_{7a} - \nu_{7b}$. Ясно, що $-3 \leq \gamma_1 \leq 1$. Ми знаємо $\mu_0(u, \chi_2, *) \in \mathbb{Z}$ і, отже, $3\gamma_1 + 9 \equiv 0 \pmod{7}$. Тоді $\gamma_1 \equiv -3 \equiv 4 \pmod{7}$ і $\gamma_1 = -3$. Звідси

$$\begin{cases} \nu_{2a} + \nu_{7a} + \nu_{7b} = 1 \\ 4\nu_{2a} - \nu_{7a} - \nu_{7b} = -3, \end{cases}$$

ліва частина суми $5\nu_{2a} = -2$ рівнянь системи ділиться на 5 при будь-якому цілому ν_{2a} а права — ні. Отже, шуканих цілих значень $\nu_{2a}, \nu_{7a}, \nu_{7b}$ не існує.

Випадок (x). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 15. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{2a, 4a, 4b, 4c, 7a, 7b\}$. Отже, $1 = \varepsilon(u) = \nu_{3a} + \nu_{5a} + \nu_{5b}$. Очевидно, $u^5, u^3 \in V(\mathbb{Z}G)$ — одиниці відповідно порядків 3 та 5. З доведених властивостей таких одиниць $\chi(u^5) = \chi(3a)$ і $\chi(u^3) = m_1\chi(5a) + m_2\chi(5b)$, де $(m_1, m_2) \in \{(1, 0), (0, 1), (2, -1), (-1, 2)\}$. Застосування формул (7.2) до твердження 7.5 дає таку систему нерівностей:

$$\mu_0(u, \chi_2, *) = \frac{1}{15}(16\nu_{3a} + 24) \geq 0; \mu_5(u, \chi_2, *) = \frac{1}{15}(-8\nu_{3a} + 18) \geq 0.$$

За твердження 7.5 $\mu_0(u, \chi_2, *) \in \mathbb{Z}$ і, отже, $16\nu_{3a} + 24 \equiv 0 \pmod{15}$. Звідси $\nu_{3a} + 9 \equiv 0 \pmod{15}$ і $\nu_{3a} \equiv 6 \pmod{15}$. Крім того, з нерівностей одержимо $-1 \leq \nu_{3a} \leq 2$, що неможливе.

Випадок (xi). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 21. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{2a, 3a, 4a, 4b, 4c, 5a, 5b\}$. Отже, $1 = \varepsilon(u) = \nu_{3a} + \nu_{7a} + \nu_{7b}$. Очевидно, $u^7, u^3 \in V(\mathbb{Z}G)$ — одиниці відповідно порядків 3 та 7. З доведених властивостей таких одиниць $\chi(u^7) = \chi(3a)$ і $\chi(u^3) = m_1\chi(7a) + m_2\chi(7b)$ де $(m_1, m_2) \in \{(1, 0), (0, 1), (2, -1), (-1, 2)\}$. Застосування формул (7.2) до твердження 7.5 дає таку систему нерівностей:

$$\begin{aligned} \mu_0(u, \chi_2, *) &= \frac{1}{21}(12\gamma_1 + 18) \geq 0; \quad \mu_7(u, \chi_2, *) = \frac{1}{21}(-6\gamma_1 + 12) \geq 0; \\ \mu_1(u, \chi_3, *) &= \frac{1}{21}(-\nu_{3a} + 36) \geq 0, \end{aligned}$$

де $\gamma_1 = 2\nu_{3a} - \nu_{7a} - \nu_{7b}$. Ясно, що $-1 \leq \gamma_1 \leq 2$. За твердження 7.5 $\mu_7(u, \chi_2, *) \in \mathbb{Z}$ і, отже, $-2\gamma_1 + 4 \equiv 0 \pmod{7}$. Тобто $\gamma_1 \equiv 2 \pmod{7}$ і $\gamma_1 = 2$. Таким чином

$$\begin{cases} \nu_{3a} + \nu_{7a} + \nu_{7b} = 1, \\ 2\nu_{3a} - \nu_{7a} - \nu_{7b} = 2. \end{cases}$$

Звідки, додавши рівняння, одержимо $3\nu_{3a} = 3$ і $\nu_{3a} = 1$. Але тоді $\mu_1(u, \chi_3, *) = \frac{1}{21}(-1 + 36) = \frac{35}{21} = \frac{5}{3} \notin \mathbb{Z}$, що суперечить твердженню 7.5.

Випадок (xii). Нехай одиниця $u \in V(\mathbb{Z}G)$ має порядок 35. За твердженням 7.3 $\nu_{rx} = 0$ для всіх $rx \in \{2a, 3a, 4a, 4b, 4c\}$. Отже, $1 = \varepsilon(u) = \nu_{5a} + \nu_{5b} + \nu_{7a} + \nu_{7b}$. Очевидно, $u^7, u^5 \in V(\mathbb{Z}G)$ — одиниці відповідно порядків 5 та 7. З доведених властивостей таких одиниць $\chi(u^7) = m_1\chi(5a) + m_2\chi(5b)$ і $\chi(u^5) = m_3\chi(7a) + m_4\chi(7b)$ де $(m_1, m_2, m_3, m_4) \in \{(1, 0, 1, 0), (1, 0, 0, 1), (0, 1, 1, 0), (0, 1, 0, 1), (1, 0, 2, -1), (0, 1, 2, -1), (1, 0, -1, 2), (0, 1, -1, 2), (2, -1, 1, 0), (2, -1, 0, 1), (2, -1, 2, -1), (2, -1, -1, 2), (-1, 2, 1, 0), (-1, 2, 0, 1), (-1, 2, 2, -1), (-1, 2, -1, 2)\}$. Застосування формул (7.4) (7.2) до твердження 7.5 дає таку систему нерівностей:

$$\mu_0(u, \chi_2, 3) = \frac{1}{35}(24\gamma + 21) \geq 0; \quad \mu_0(u, \chi_2, *) = \frac{1}{35}(-24\gamma + 14) \geq 0,$$

де $\gamma = \nu_{7a} + \nu_{7b}$. Ясно, що $0 \leq \gamma \leq 0$, тобто $\gamma = 0$. Але тоді $\mu_0(u, \chi_2, *) = \frac{14}{35} = \frac{2}{5} \notin \mathbb{Z}$, що суперечить твердженню 7.5.

Теорема доведена.

Зауваження 7.6. Для групи $G = PSL(3, 4)$ в групі $V(\mathbb{Z}G)$ не існує одиниць $u = \sum_{g \in G} \alpha_g g$ інших скінченних порядків крім порядків розглянутих у теоремі 7.1.

Доведення. Засобами програмування в GAP див. додаток Б одержимо $|G| = 20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$ і $\exp(G) = 420 = 2^2 \cdot 3 \cdot 5 \cdot 7$. За твердженням 7.2 нам потрібно розглянути лише одиниці $u \in V(\mathbb{Z}G)$ порядку

$$2, 3, 5, 7;$$

$$4 = 2^2, 6 = 2 \cdot 3, 10 = 2 \cdot 5, 14 = 2 \cdot 7,$$

$$15 = 3 \cdot 5, 21 = 3 \cdot 7, 35 = 5 \cdot 7;$$

$$\begin{aligned}
12 &= 2^2 \cdot 3, \quad 20 = 2^2 \cdot 5, \quad 28 = 2^2 \cdot 7, \quad 30 = 2 \cdot 3 \cdot 5, \\
42 &= 2 \cdot 3 \cdot 7, \quad 70 = 2 \cdot 5 \cdot 7, \quad 105 = 3 \cdot 5 \cdot 7; \\
60 &= 2^2 \cdot 3 \cdot 5, \quad 84 = 2^2 \cdot 3 \cdot 7, \quad 140 = 2^2 \cdot 5 \cdot 7, \quad 210 = 2 \cdot 3 \cdot 5 \cdot 7; \\
420 &= 2^2 \cdot 3 \cdot 5 \cdot 7.
\end{aligned}$$

В теоремі 7.1 розглянуто одиниці групи $V(\mathbb{Z}G)$ порядків 2, 3, 4, 5, 7, 6, та показано відсутність одиниць порядків 10, 12, 14, 15, 21 або 35. Залишаються тільки такі можливі порядки:

$$20, 28, 30, 42, 70, 105, 60, 84, 140, 210, 420.$$

Відсутність у групі $V(\mathbb{Z}G)$ одиниць порядку 10 негайно означає відсутність одиниць порядку 20, 30, 70, 60, 140, 210, 420. Залишаються тільки такі можливі порядки:

$$28, 42, 105, 84.$$

Відсутність у групі $V(\mathbb{Z}G)$ одиниць порядку 14 означає відсутність одиниць порядку 28, 42, 84. Залишається тільки такий можливий порядок:

$$105.$$

Відсутність у групі $V(\mathbb{Z}G)$ одиниць порядку 21 означає відсутність одиниць порядку 105. $\square$

7.2. Побудова розширених бінарних кодів Голя за груповим кільцем скінченних груп порядку 24

Нехай $\mathbb{F}_2$ — поле з двох елементів, $G = \{g_1, \dots, g_{24}\}$ — скінченна група порядку $|G| = 24$. Розглянемо групове кільце $\mathbb{F}_2G$. Для довільного елемента $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_{24}}g_{24} \in \mathbb{F}_2G$ визначимо $C(v)$, як лінійний

код породжений рядками матриці

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

Відомо [185], що для

$$\left. \begin{array}{l} 1) \quad \sigma(v) = \sigma(v)^T, \\ 2) \quad \sigma(v)^2 = 0_{24 \times 24}, \\ 3) \quad \text{rank}(\sigma(v)) = 12 \end{array} \right\} \quad (7.5)$$

код $C(v)$ самодуальний. Крім того, він є розширений бінарним кодом Голя (тобто бінарним $[24, 12, 8]$ -кодом), якщо 8 є його мінімальна відстань. У [102] розширений бінарний код Голя було побудовано у вигляді $C(v)$ з групової алгебри $\mathbb{F}_2 S_4$, де S_4 — симетрична група порядку 24. У [185] аналогічний результат одержано для групи D_{24} дієдра порядку 24.

Зрозуміло, що є 15 групи порядку 24 з точністю до ізоморфізму. Їх можна одержати наведеними обчислення в GAP у додатку В.6. А саме:

$$\begin{array}{ccccccccc} C_3 \rtimes C_8, & C_{24}, & SL(2, 3), & C_3 \rtimes Q_8, & C_4 \times S_3, \\ D_{24}, & C_2 \times (C_3 \rtimes C_4), & (C_6 \times C_2) \rtimes C_2, & C_{12} \times C_2, & C_3 \times D_8, \\ C_3 \times Q_8, & S_4, & C_2 \times A_4, & C_2 \times C_2 \times S_3, & C_6 \times C_2 \times C_2, \end{array}$$

де C_n позначає циклічну групу порядку n , D_n — групу дієдра порядку n , S_n — симетричну групу степеня n , A_4 — знакозмінну групу степеня 4, Q_8 — групу кватерніонів порядку 8, $SL(2, 3)$ — спеціальну лінійну групу степеня 2 над полем з 3 елементів, $A \times B$ — прямий добуток груп A і B , $A \rtimes B$ — напівпрямий добуток груп A і B (A нормальна підгрупа в AB).

Природно виникає питання: для яких з цих груп G порядку 24, крім D_{24} , S_4 , ми можемо побудувати розширений бінарний код Голя у вигляді

$C(v)$, де $v \in \mathbb{F}_2G$, v задовольняє (7.5)? Легко бачити, що для любого $g \in G$ $\sigma(g)\sigma(v) = \sigma(gv)$ і $C(gv) = C(v)$. Тому сама група G є ізоморфна деякій підгрупі групи автоморфізмів коду $C(v)$ а для розширеного бінарного коду Голя група автоморфізмів є групою Матьє M_{24} [165]. Задати групу Матьє M_{24} та її порядок можна обчислити в GAP за кодом наведеними в додатку В.

$$|M_{24}| = 244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23.$$

Крім того, за кодом наведеними в додатку В існує 8 груп, з точністю до ізоморфізму, порядку 24, які ізоморфні деяким підгрупам групи Матьє M_{24} :

$$\begin{aligned} &SL(2, 3), \quad C_4 \times S_3, \quad D_{24}, \quad (C_6 \times C_2) \rtimes C_2, \\ &C_3 \times D_8, \quad S_4, \quad C_2 \times A_4, \quad C_2 \times C_2 \times S_3. \end{aligned}$$

Перераховані групи є групами `SmallGroup(n,i)` для $i \in \{3, 5, 6, 8, 10, 12, 13, 14\}$ прийнятої в системі GAP. Залишалося відкритим питання про можливість побудови розширених бінарних кодів Голя у вигляді $C(v)$ для відповідних елементів v з групової алгебри $\mathbb{F}_2G$ для таких груп G порядку 24:

$$SL(2, 3), \quad C_4 \times S_3, \quad (C_6 \times C_2) \rtimes C_2, \quad C_3 \times D_8, \quad C_2 \times A_4, \quad C_2 \times C_2 \times S_3.$$

7.2.1. Група $SL(2, 3)$. Групу $SL(2, 3)$ можна задати через твірні елементи та визначальні співвідношення так $SL(2, 3) = \langle x, y \mid x^3 = y^3 = (xy)^2 \rangle$ (Див. [134]), де

$$x = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}, \quad y = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

Можна перевірити таке задання наведеними обчислення в GAP у додатку В.1 а також встановлено однозначне представлення елементів групи

у вказаному вигляді

$$G = \{1, \quad x, \quad x^2, \quad x^3, \quad x^4, \quad x^5, \\ y, \quad xy, \quad x^2y, \quad x^3y, \quad x^4y, \quad x^5y, \\ y^2, \quad xy^2, \quad x^2y^2, \quad x^3y^2, \quad x^4y^2, \quad x^5y^2, \\ y^2x, \quad xy^2x, \quad x^2y^2x, \quad x^3y^2x, \quad x^4y^2x, \quad x^5y^2x\}$$

та визначено порядок їх розташування в групі.

Тепер ми доведемо, що не можна побудувати розширений бінарний код Голея вигляді $C(v)$, для жодного елементів v , що задовольняє умови (7.5) з $\mathbb{F}_2SL(2, 3)$. Нехай

$$\begin{aligned} \kappa = \kappa_1 = & \alpha_1 + \alpha_2x + \alpha_3x^2 + \alpha_4x^3 + \alpha_5x^4 + \alpha_6x^5, \\ & \alpha_7y + \alpha_8xy + \alpha_9x^2y + \alpha_{10}x^3y + \alpha_{11}x^4y + \alpha_{12}x^5y, \\ & \alpha_{13}y^2 + \alpha_{14}xy^2 + \alpha_{15}x^2y^2 + \alpha_{16}x^3y^2 + \alpha_{17}x^4y^2 + \alpha_{18}x^5y^2, \\ & \alpha_{19}y^2x + \alpha_{20}xy^2x + \alpha_{21}x^2y^2x + \alpha_{22}x^3y^2x + \\ & \alpha_{23}x^4y^2x + \alpha_{24}x^5y^2x \in \mathbb{F}_2SL(2, 3), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$. Було з'ясовано обчисленнями в GАР наведеними в додатку

В.1 вигляд матриці $\sigma(\kappa_1)$:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ \alpha_6 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_{12} & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{18} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{24} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_5 & \alpha_6 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_{11} & \alpha_{12} & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{17} & \alpha_{18} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{23} & \alpha_{24} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} \\ \alpha_4 & \alpha_5 & \alpha_6 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{19} & \alpha_{20} & \alpha_{21} \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_1 & \alpha_2 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_7 & \alpha_8 & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{13} & \alpha_{14} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{19} & \alpha_{20} \\ \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_1 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_7 & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{13} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{19} \\ \alpha_{16} & \alpha_{22} & \alpha_8 & \alpha_{13} & \alpha_{19} & \alpha_{11} & \alpha_1 & \alpha_{21} & \alpha_{14} & \alpha_4 & \alpha_{24} & \alpha_{17} & \alpha_7 & \alpha_{20} & \alpha_5 & \alpha_{10} & \alpha_{23} & \alpha_2 & \alpha_{18} & \alpha_{12} & \alpha_6 & \alpha_{15} & \alpha_9 & \alpha_3 \\ \alpha_{11} & \alpha_{16} & \alpha_{22} & \alpha_8 & \alpha_{13} & \alpha_{19} & \alpha_{17} & \alpha_1 & \alpha_{21} & \alpha_{14} & \alpha_4 & \alpha_{24} & \alpha_2 & \alpha_7 & \alpha_{20} & \alpha_5 & \alpha_{10} & \alpha_{23} & \alpha_3 & \alpha_{18} & \alpha_{12} & \alpha_6 & \alpha_{15} & \alpha_9 \\ \alpha_{19} & \alpha_{11} & \alpha_{16} & \alpha_{22} & \alpha_8 & \alpha_{13} & \alpha_{24} & \alpha_{17} & \alpha_1 & \alpha_{21} & \alpha_{14} & \alpha_4 & \alpha_{23} & \alpha_2 & \alpha_7 & \alpha_{20} & \alpha_5 & \alpha_{10} & \alpha_9 & \alpha_3 & \alpha_{18} & \alpha_{12} & \alpha_6 & \alpha_{15} \\ \alpha_{13} & \alpha_{19} & \alpha_{11} & \alpha_{16} & \alpha_{22} & \alpha_8 & \alpha_4 & \alpha_{24} & \alpha_{17} & \alpha_1 & \alpha_{21} & \alpha_{14} & \alpha_{10} & \alpha_{23} & \alpha_2 & \alpha_7 & \alpha_{20} & \alpha_5 & \alpha_{15} & \alpha_9 & \alpha_3 & \alpha_{18} & \alpha_{12} & \alpha_6 \\ \alpha_8 & \alpha_{13} & \alpha_{19} & \alpha_{11} & \alpha_{16} & \alpha_{22} & \alpha_{14} & \alpha_4 & \alpha_{24} & \alpha_{17} & \alpha_1 & \alpha_{21} & \alpha_5 & \alpha_{10} & \alpha_{23} & \alpha_2 & \alpha_7 & \alpha_{20} & \alpha_6 & \alpha_{15} & \alpha_9 & \alpha_3 & \alpha_{18} & \alpha_{12} \\ \alpha_{22} & \alpha_8 & \alpha_{13} & \alpha_{19} & \alpha_{11} & \alpha_{16} & \alpha_{21} & \alpha_{14} & \alpha_4 & \alpha_{24} & \alpha_{17} & \alpha_1 & \alpha_{20} & \alpha_5 & \alpha_{10} & \alpha_{23} & \alpha_2 & \alpha_7 & \alpha_{12} & \alpha_6 & \alpha_{15} & \alpha_9 & \alpha_3 & \alpha_{18} \\ \alpha_{10} & \alpha_{15} & \alpha_{21} & \alpha_7 & \alpha_{18} & \alpha_{24} & \alpha_{16} & \alpha_6 & \alpha_{20} & \alpha_{13} & \alpha_3 & \alpha_{23} & \alpha_1 & \alpha_{12} & \alpha_{19} & \alpha_4 & \alpha_9 & \alpha_{22} & \alpha_2 & \alpha_{17} & \alpha_{11} & \alpha_5 & \alpha_{14} & \alpha_8 \\ \alpha_{24} & \alpha_{10} & \alpha_{15} & \alpha_{21} & \alpha_7 & \alpha_{18} & \alpha_{23} & \alpha_{16} & \alpha_6 & \alpha_{20} & \alpha_{13} & \alpha_3 & \alpha_{22} & \alpha_1 & \alpha_{12} & \alpha_{19} & \alpha_4 & \alpha_9 & \alpha_8 & \alpha_2 & \alpha_{17} & \alpha_{11} & \alpha_5 & \alpha_{14} \\ \alpha_{18} & \alpha_{24} & \alpha_{10} & \alpha_{15} & \alpha_{21} & \alpha_7 & \alpha_3 & \alpha_{23} & \alpha_{16} & \alpha_6 & \alpha_{20} & \alpha_{13} & \alpha_9 & \alpha_{22} & \alpha_1 & \alpha_{12} & \alpha_{19} & \alpha_4 & \alpha_{14} & \alpha_8 & \alpha_2 & \alpha_{17} & \alpha_{11} & \alpha_5 \\ \alpha_7 & \alpha_{18} & \alpha_{24} & \alpha_{10} & \alpha_{15} & \alpha_{21} & \alpha_{13} & \alpha_3 & \alpha_{23} & \alpha_{16} & \alpha_6 & \alpha_{20} & \alpha_4 & \alpha_9 & \alpha_{22} & \alpha_1 & \alpha_{12} & \alpha_{19} & \alpha_5 & \alpha_{14} & \alpha_8 & \alpha_2 & \alpha_{17} & \alpha_{11} \\ \alpha_{21} & \alpha_7 & \alpha_{18} & \alpha_{24} & \alpha_{10} & \alpha_{15} & \alpha_{20} & \alpha_{13} & \alpha_3 & \alpha_{23} & \alpha_{16} & \alpha_6 & \alpha_{19} & \alpha_4 & \alpha_9 & \alpha_{22} & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_5 & \alpha_{14} & \alpha_8 & \alpha_2 & \alpha_{17} \\ \alpha_{15} & \alpha_{21} & \alpha_7 & \alpha_{18} & \alpha_{24} & \alpha_{10} & \alpha_6 & \alpha_{20} & \alpha_{13} & \alpha_3 & \alpha_{23} & \alpha_{16} & \alpha_{12} & \alpha_{19} & \alpha_4 & \alpha_9 & \alpha_{22} & \alpha_1 & \alpha_{17} & \alpha_{11} & \alpha_5 & \alpha_{14} & \alpha_8 & \alpha_2 \\ \alpha_9 & \alpha_{14} & \alpha_{20} & \alpha_{12} & \alpha_{17} & \alpha_{23} & \alpha_{15} & \alpha_5 & \alpha_{19} & \alpha_{18} & \alpha_2 & \alpha_{22} & \alpha_6 & \alpha_{11} & \alpha_{24} & \alpha_3 & \alpha_8 & \alpha_{21} & \alpha_1 & \alpha_{16} & \alpha_{10} & \alpha_4 & \alpha_{13} & \alpha_7 \\ \alpha_{23} & \alpha_9 & \alpha_{14} & \alpha_{20} & \alpha_{12} & \alpha_{17} & \alpha_{22} & \alpha_{15} & \alpha_5 & \alpha_{19} & \alpha_{18} & \alpha_2 & \alpha_{21} & \alpha_6 & \alpha_{11} & \alpha_{24} & \alpha_3 & \alpha_8 & \alpha_7 & \alpha_1 & \alpha_{16} & \alpha_{10} & \alpha_4 & \alpha_{13} \\ \alpha_{17} & \alpha_{23} & \alpha_9 & \alpha_{14} & \alpha_{20} & \alpha_{12} & \alpha_2 & \alpha_{22} & \alpha_{15} & \alpha_5 & \alpha_{19} & \alpha_{18} & \alpha_8 & \alpha_{21} & \alpha_6 & \alpha_{11} & \alpha_{24} & \alpha_3 & \alpha_{13} & \alpha_7 & \alpha_1 & \alpha_{16} & \alpha_{10} & \alpha_4 \\ \alpha_{12} & \alpha_{17} & \alpha_{23} & \alpha_9 & \alpha_{14} & \alpha_{20} & \alpha_{18} & \alpha_2 & \alpha_{22} & \alpha_{15} & \alpha_5 & \alpha_{19} & \alpha_3 & \alpha_8 & \alpha_{21} & \alpha_6 & \alpha_{11} & \alpha_{24} & \alpha_4 & \alpha_{13} & \alpha_7 & \alpha_1 & \alpha_{16} & \alpha_{10} \\ \alpha_{20} & \alpha_{12} & \alpha_{17} & \alpha_{23} & \alpha_9 & \alpha_{14} & \alpha_{19} & \alpha_{18} & \alpha_2 & \alpha_{22} & \alpha_{15} & \alpha_5 & \alpha_{24} & \alpha_3 & \alpha_8 & \alpha_{21} & \alpha_6 & \alpha_{11} & \alpha_{10} & \alpha_4 & \alpha_{13} & \alpha_7 & \alpha_1 & \alpha_{16} \\ \alpha_{14} & \alpha_{20} & \alpha_{12} & \alpha_{17} & \alpha_{23} & \alpha_9 & \alpha_5 & \alpha_{19} & \alpha_{18} & \alpha_2 & \alpha_{22} & \alpha_{15} & \alpha_{11} & \alpha_{24} & \alpha_3 & \alpha_8 & \alpha_{21} & \alpha_6 & \alpha_{16} & \alpha_{10} & \alpha_4 & \alpha_{13} & \alpha_7 & \alpha_1 \end{pmatrix}.$$

Тоді

$$\sigma(\kappa_1) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 & A_8 \\ A_9 & A_{10} & A_{11} & A_{12} \\ A_{13} & A_{14} & A_{15} & A_{16} \end{pmatrix},$$

де $A_1 = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)$, $A_2 = circ(\alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12})$,
 $A_3 = circ(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}, \alpha_{17}, \alpha_{18})$, $A_4 = circ(\alpha_{19}, \alpha_{20}, \alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24})$,
 $A_5 = circ(\alpha_{16}, \alpha_{22}, \alpha_8, \alpha_{13}, \alpha_{19}, \alpha_{11})$, $A_6 = circ(\alpha_1, \alpha_{21}, \alpha_{14}, \alpha_4, \alpha_{24}, \alpha_{17})$,
 $A_7 = circ(\alpha_7, \alpha_{20}, \alpha_5, \alpha_{10}, \alpha_{23}, \alpha_2)$, $A_8 = circ(\alpha_{18}, \alpha_{12}, \alpha_6, \alpha_{15}, \alpha_9, \alpha_3)$,
 $A_9 = circ(\alpha_{10}, \alpha_{15}, \alpha_{21}, \alpha_7, \alpha_{18}, \alpha_{24})$, $A_{10} = circ(\alpha_{16}, \alpha_6, \alpha_{20}, \alpha_{13}, \alpha_3, \alpha_{23})$,
 $A_{11} = circ(\alpha_1, \alpha_{12}, \alpha_{19}, \alpha_4, \alpha_9, \alpha_{22})$, $A_{12} = circ(\alpha_2, \alpha_{17}, \alpha_{11}, \alpha_5, \alpha_{14}, \alpha_8)$,
 $A_{13} = circ(\alpha_9, \alpha_{14}, \alpha_{20}, \alpha_{12}, \alpha_{17}, \alpha_{23})$, $A_{14} = circ(\alpha_{15}, \alpha_5, \alpha_{19}, \alpha_{18}, \alpha_2, \alpha_{22})$,
 $A_{15} = circ(\alpha_6, \alpha_{11}, \alpha_{24}, \alpha_3, \alpha_8, \alpha_{21})$, $A_{16} = circ(\alpha_1, \alpha_{16}, \alpha_{10}, \alpha_4, \alpha_{13}, \alpha_7)$.

Тут для довільних елементів $x_1, x_2, \dots, x_{n-1}, x_n$ через

$$circ(x_1, x_2, \dots, x_{n-1}, x_n) = \begin{pmatrix} x_1 & x_2 & \dots & x_{n-1} & x_n \\ x_n & x_1 & \dots & x_{n-2} & x_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_3 & x_4 & \dots & x_1 & x_2 \\ x_2 & x_3 & \dots & x_n & x_1 \end{pmatrix}$$

позначаємо так звану *головну циркулярну матрицю*. Ми шукаємо розширені бінарні коди Голея з умов:

- 1) $\sigma(\alpha) = \sigma(\alpha)^T$,
- 2) $\sigma(\alpha)^2 = 0_{24 \times 24}$,
- 3) $Rank(\sigma(\alpha)) = 12$,

для деяких дільників нуля α з $\mathbb{F}_2SL(2, 3)$. З умови $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, отримуємо, що $\alpha_5 = \alpha_3$, $\alpha_6 = \alpha_2$, $\alpha_{11} = \alpha_8$, $\alpha_{13} = \alpha_{10}$, $\alpha_{16} = \alpha_7$, $\alpha_{18} = \alpha_{15}$,

$\alpha_{19} = \alpha_9$, $\alpha_{21} = \alpha_{17}$, $\alpha_{22} = \alpha_{12}$, $\alpha_{23} = \alpha_{20}$ і $\alpha_{24} = \alpha_{14}$. Умови підтверджуються також обчисленнями в GАР наведеними в додатку В.1. Тепер нехай

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(x + x^5) + \alpha_3(x^2 + x^4) + \alpha_4x^3 + \alpha_7(y + x^3y^2) + \alpha_8(xy + x^4y) + \\ & \alpha_9(x^2y + y^2x) + \alpha_{10}(x^3y + y^2) + \alpha_{12}(x^5y + x^3y^2x) + \alpha_{14}(xy^2 + x^5y^2x) + \\ & \alpha_{15}(x^2y^2 + x^5y^2) + \alpha_{17}(x^4y^2 + x^2y^2x) + \alpha_{20}(xy^2z + x^4y^2x) \in \mathbb{F}_2SL(2, 3), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$. Тоді

$$\sigma(\kappa_2)^2 = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 \\ B_5 & B_6 & B_7 & B_8 \\ B_9 & B_{10} & B_{11} & B_{12} \\ B_{13} & B_{14} & B_{15} & B_{16} \end{pmatrix},$$

де $B_1 = circ(\gamma_1, \gamma_{12}, \gamma_{11}, 0, \gamma_{11}, \gamma_{12})$, $B_2 = circ(\gamma_{10}, \gamma_4, \gamma_7, \gamma_9, \gamma_4, \gamma_6)$,
 $B_3 = circ(\gamma_9, \gamma_8, \gamma_3, \gamma_{10}, \gamma_5, \gamma_3)$, $B_4 = circ(\gamma_7, \gamma_2, \gamma_5, \gamma_6, \gamma_2, \gamma_8)$,
 $B_5 = circ(\gamma_{10}, \gamma_6, \gamma_4, \gamma_9, \gamma_7, \gamma_4)$, $B_6 = circ(\gamma_1, \gamma_5, \gamma_8, 0, \gamma_8, \gamma_5, \gamma_{10})$,
 $B_7 = circ(\gamma_2, \gamma_{11}, \gamma_9, \gamma_2, \gamma_{12}, \gamma_3)$, $B_8 = circ(\gamma_6, \gamma_{12}, \gamma_3, \gamma_7, \gamma_{11})$,
 $B_9 = circ(\gamma_9, \gamma_3, \gamma_5, \gamma_{10}, \gamma_3, \gamma_8)$, $B_{10} = circ(\gamma_{10}, \gamma_{12}, \gamma_2, \gamma_9, \gamma_{11}, \gamma_2)$,
 $B_{11} = circ(\gamma_1, \gamma_6, \gamma_7, 0, \gamma_7, \gamma_6)$, $B_{12} = circ(\gamma_{12}, \gamma_5, \gamma_4, \gamma_{11}, \gamma_8, \gamma_4)$,
 $B_{13} = circ(\gamma_7, \gamma_8, \gamma_2, \gamma_6, \gamma_5, \gamma_2)$, $B_{14} = circ(\gamma_3, \gamma_{11}, \gamma_7, \gamma_3, \gamma_{12}, \gamma_6)$,
 $B_{15} = circ(\gamma_{12}, \gamma_4, \gamma_8, \gamma_{11}, \gamma_4, \gamma_5)$, $B_{16} = circ(\gamma_1, \gamma_{10}, \gamma_9, 0, \gamma_9, \gamma_{10})$, де $\gamma_1 = \alpha_1^2 + \alpha_4^2$, $\gamma_2 = (\alpha_2 + \alpha_3 + \alpha_7 + \alpha_{10})(\alpha_9 + \alpha_{12} + \alpha_{14} + \alpha_{17})$,
 $\gamma_3 = (\alpha_2 + \alpha_3 + \alpha_9 + \alpha_{12})(\alpha_7 + \alpha_{10} + \alpha_{14} + \alpha_{17})$,
 $\gamma_4 = (\alpha_7 + \alpha_9 + \alpha_{10} + \alpha_{12})(\alpha_2 + \alpha_3 + \alpha_{14} + \alpha_{17})$,
 $\gamma_5 = \alpha_2\alpha_7 + \alpha_7\alpha_8 + \alpha_3\alpha_9 + \alpha_8\alpha_9 + \alpha_3\alpha_{10} + \alpha_8\alpha_{10} + \alpha_9\alpha_{10} + \alpha_2\alpha_{12} + \alpha_7\alpha_{12} +$
 $\alpha_8\alpha_{12} + \alpha_2\alpha_{15} + \alpha_3\alpha_{15} + \alpha_9\alpha_{15} + \alpha_{12}\alpha_{15} + \alpha_2\alpha_{20} + \alpha_3\alpha_{20} + \alpha_7\alpha_{20} + \alpha_{10}\alpha_{20}$,
 $\gamma_6 = \alpha_2\alpha_7 + \alpha_2\alpha_8 + \alpha_3\alpha_8 + \alpha_3\alpha_{10} + \alpha_3\alpha_{14} + \alpha_8\alpha_{14} + \alpha_{10}\alpha_{14} + \alpha_7\alpha_{15} + \alpha_{10}\alpha_{15} +$
 $\alpha_{14}\alpha_{15} + \alpha_2\alpha_{17} + \alpha_7\alpha_{17} + \alpha_8\alpha_{17} + \alpha_{15}\alpha_{17} + \alpha_2\alpha_{20} + \alpha_3\alpha_{20} + \alpha_7\alpha_{20} + \alpha_{10}\alpha_{20}$, $\gamma_7 =$
 $\alpha_3\alpha_7 + \alpha_2\alpha_8 + \alpha_3\alpha_8 + \alpha_9^2 + \alpha_2\alpha_{10} + \alpha_{12}^2 + \alpha_2\alpha_{14} + \alpha_7\alpha_{14} + \alpha_8\alpha_{14} + \alpha_7\alpha_{15} + \alpha_{10}\alpha_{15} +$

$$\begin{aligned}
& \alpha_{14}\alpha_{15} + \alpha_3\alpha_{17} + \alpha_8\alpha_{17} + \alpha_{10}\alpha_{17} + \alpha_{15}\alpha_{17} + \alpha_2\alpha_{20} + \alpha_3\alpha_{20} + \alpha_7\alpha_{20} + \alpha_{10}\alpha_{20}, \gamma_8 = \\
& \alpha_3\alpha_7 + \alpha_7\alpha_8 + \alpha_2\alpha_9 + \alpha_7\alpha_9 + \alpha_8\alpha_9 + \alpha_2\alpha_{10} + \alpha_8\alpha_{10} + \alpha_3\alpha_{12} + \alpha_8\alpha_{12} + \alpha_{10}\alpha_{12} + \\
& \alpha_{14}^2 + \alpha_2\alpha_{15} + \alpha_3\alpha_{15} + \alpha_9\alpha_{15} + \alpha_{12}\alpha_{15} + \alpha_{17}^2 + \alpha_2\alpha_{20} + \alpha_3\alpha_{20} + \alpha_7\alpha_{20} + \alpha_{10}\alpha_{20}, \gamma_9 = \\
& \alpha_7^2 + \alpha_2\alpha_8 + \alpha_3\alpha_8 + \alpha_2\alpha_9 + \alpha_{10}^2 + \alpha_3\alpha_{12} + \alpha_2\alpha_{14} + \alpha_8\alpha_{14} + \alpha_{12}\alpha_{14} + \alpha_2\alpha_{15} + \alpha_3\alpha_{15} + \\
& \alpha_9\alpha_{15} + \alpha_{12}\alpha_{15} + \alpha_3\alpha_{17} + \alpha_8\alpha_{17} + \alpha_9\alpha_{17} + \alpha_9\alpha_{20} + \alpha_{12}\alpha_{20} + \alpha_{14}\alpha_{20} + \alpha_{17}\alpha_{20}, \gamma_{10} = \\
& \alpha_2\alpha_8 + \alpha_3\alpha_8 + \alpha_3\alpha_9 + \alpha_2\alpha_{12} + \alpha_3\alpha_{14} + \alpha_8\alpha_{14} + \alpha_9\alpha_{14} + \alpha_2\alpha_{15} + \alpha_3\alpha_{15} + \alpha_9\alpha_{15} + \\
& \alpha_{12}\alpha_{15} + \alpha_2\alpha_{17} + \alpha_8\alpha_{17} + \alpha_{12}\alpha_{17} + \alpha_9\alpha_{20} + \alpha_{12}\alpha_{20} + \alpha_{14}\alpha_{20} + \alpha_{17}\alpha_{20}, \gamma_{11} = \\
& \alpha_2^2 + \alpha_3^2 + \alpha_7\alpha_8 + \alpha_7\alpha_9 + \alpha_8\alpha_9 + \alpha_8\alpha_{10} + \alpha_8\alpha_{12} + \alpha_{10}\alpha_{12} + \alpha_7\alpha_{14} + \alpha_{12}\alpha_{14} + \alpha_7\alpha_{15} + \\
& \alpha_{10}\alpha_{15} + \alpha_{14}\alpha_{15} + \alpha_9\alpha_{17} + \alpha_{10}\alpha_{17} + \alpha_{15}\alpha_{17} + \alpha_9\alpha_{20} + \alpha_{12}\alpha_{20} + \alpha_{14}\alpha_{20} + \alpha_{17}\alpha_{20}, \\
& \gamma_{12} = \alpha_7\alpha_8 + \alpha_8\alpha_9 + \alpha_8\alpha_{10} + \alpha_9\alpha_{10} + \alpha_7\alpha_{12} + \alpha_8\alpha_{12} + \alpha_9\alpha_{14} + \alpha_{10}\alpha_{14} + \alpha_7\alpha_{15} + \\
& \alpha_{10}\alpha_{15} + \alpha_{14}\alpha_{15} + \alpha_7\alpha_{17} + \alpha_{12}\alpha_{17} + \alpha_{15}\alpha_{17} + \alpha_9\alpha_{20} + \alpha_{12}\alpha_{20} + \alpha_{14}\alpha_{20} + \alpha_{17}\alpha_{20}.
\end{aligned}$$

З умови $\sigma(\kappa_2)^2 = 0_{24 \times 24}$ одержимо $\alpha_1 = \alpha_4$ і

$$\begin{cases} (\alpha_2 + \alpha_3 + \alpha_7 + \alpha_{10})(\alpha_9 + \alpha_{12} + \alpha_{14} + \alpha_{17}) = 0, \\ (\alpha_2 + \alpha_3 + \alpha_9 + \alpha_{12})(\alpha_7 + \alpha_{10} + \alpha_{14} + \alpha_{17}) = 0, \\ (\alpha_7 + \alpha_9 + \alpha_{10} + \alpha_{12})(\alpha_2 + \alpha_3 + \alpha_{14} + \alpha_{17}) = 0. \end{cases}$$

Або

$$\left[\begin{cases} \alpha_2 + \alpha_3 = \alpha_7 + \alpha_{10}, \\ (\alpha_2 + \alpha_3 + \alpha_9 + \alpha_{12})(\alpha_2 + \alpha_3 + \alpha_{14} + \alpha_{17}) = 0, \\ (\alpha_2 + \alpha_3 + \alpha_9 + \alpha_{12})(\alpha_2 + \alpha_3 + \alpha_{14} + \alpha_{17}) = 0, \\ \alpha_9 + \alpha_{12} = \alpha_{14} + \alpha_{17}, \\ (\alpha_2 + \alpha_3 + \alpha_9 + \alpha_{12})(\alpha_7 + \alpha_{10} + \alpha_9 + \alpha_{12}) = 0, \\ (\alpha_7 + \alpha_{10} + \alpha_9 + \alpha_{12})(\alpha_2 + \alpha_3 + \alpha_9 + \alpha_{12}) = 0, \end{cases} \right.$$

Таким чином

$$\left[\left\{ \begin{array}{l} \alpha_2 + \alpha_3 = \alpha_7 + \alpha_{10}, \\ \left[\begin{array}{l} \alpha_2 + \alpha_3 = \alpha_9 + \alpha_{12}, \\ \alpha_2 + \alpha_3 = \alpha_{14} + \alpha_{17}, \end{array} \right. \\ \alpha_9 + \alpha_{12} = \alpha_{14} + \alpha_{17}, \\ \left\{ \begin{array}{l} \alpha_2 + \alpha_3 = \alpha_9 + \alpha_{12}, \\ \alpha_7 + \alpha_{10} = \alpha_9 + \alpha_{12}. \end{array} \right. \end{array} \right.$$

Отже, при всіх випадках принаймні 3 елементи серед $\alpha_2 + \alpha_3$, $\alpha_7 + \alpha_{10}$, $\alpha_9 + \alpha_{12}$, $\alpha_{14} + \alpha_{17}$ рівні. Оскільки $0 = \gamma_7 + \gamma_8 + \gamma_9 + \gamma_{11} = \alpha_2^2 + \alpha_3^2 + \alpha_7^2 + \alpha_9^2 + \alpha_{10}^2 + \alpha_{12}^2 + \alpha_{14}^2 + \alpha_{17}^2$, то всі з вказаних елементів рівні і $\alpha_2 + \alpha_3 = \alpha_7 + \alpha_{10} = \alpha_9 + \alpha_{12} = \alpha_{14} + \alpha_{17}$.

Припустимо спочатку, що $\alpha_2 + \alpha_3 = 1$. Тоді $\alpha_2 + 1 = \alpha_3$, $\alpha_7 + 1 = \alpha_{10}$, $\alpha_9 + 1 = \alpha_{12}$, $\alpha_{14} + 1 = \alpha_{17}$ і $\gamma_5 = \alpha_2\alpha_7 + \alpha_7\alpha_8 + (\alpha_2 + 1)\alpha_9 + \alpha_8\alpha_9 + (\alpha_2 + 1)(\alpha_7 + 1) + \alpha_8(\alpha_7 + 1) + \alpha_9(\alpha_7 + 1) + \alpha_2(\alpha_9 + 1) + \alpha_7(\alpha_9 + 1) + \alpha_8(\alpha_9 + 1) + \alpha_2\alpha_{15} + (\alpha_2 + 1)\alpha_{15} + \alpha_9\alpha_{15} + (\alpha_9 + 1)\alpha_{15} + \alpha_2\alpha_{20} + (\alpha_2 + 1)\alpha_{20} + \alpha_7\alpha_{20} + (\alpha_7 + 1)\alpha_{20} = \alpha_2\alpha_7 + \alpha_7\alpha_8 + \alpha_2\alpha_9 + \alpha_9 + \alpha_8\alpha_9 + \alpha_7\alpha_2 + \alpha_7 + \alpha_2 + 1 + \alpha_8\alpha_7 + \alpha_8 + \alpha_9\alpha_7 + \alpha_9 + \alpha_2\alpha_9 + \alpha_2 + \alpha_7\alpha_9 + \alpha_7 + \alpha_8\alpha_9 + \alpha_8 + \alpha_2\alpha_{15} + \alpha_2\alpha_{15} + \alpha_{15} + \alpha_9\alpha_{15} + \alpha_9\alpha_{15} + \alpha_{15} + \alpha_2\alpha_{20} + \alpha_2\alpha_{20} + \alpha_{20} + \alpha_7\alpha_{20} + \alpha_7\alpha_{20} + \alpha_{20} = 1$. Що неможливо.

Припустимо нарешті, що $\alpha_2 + \alpha_3 = 0$. Тоді $\alpha_2 = \alpha_3$, $\alpha_7 = \alpha_{10}$, $\alpha_9 = \alpha_{12}$, $\alpha_{14} = \alpha_{17}$. Тепер нехай

$$\begin{aligned} \kappa_3 = & \alpha_1(1 + x^3) + \alpha_2(x + x^2 + x^4 + x^5) + \alpha_7(y + x^3y + y^2 + x^3y^2) + \\ & \alpha_8(xy + x^4y) + \alpha_9(x^2y + x^5y + y^2x + x^3y^2x) + \\ & \alpha_{14}(xy^2 + x^4y^2 + x^2y^2z + x^5y^2z) + \alpha_{15}(x^2y^2 + x^5y^2) + \\ & \alpha_{20}(xy^2x + x^4y^2x) \in \mathbb{F}_2SL(2, 3). \end{aligned}$$

Тоді

$$\sigma(\kappa_3) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 & A_8 \\ A_9 & A_{10} & A_{11} & A_{12} \\ A_{13} & A_{14} & A_{15} & A_{16} \end{pmatrix},$$

де $A_1 = \text{circ}(\alpha_1, \alpha_2, \alpha_2, \alpha_1, \alpha_2, \alpha_2)$, $A_2 = \text{circ}(\alpha_7, \alpha_8, \alpha_9, \alpha_7, \alpha_8, \alpha_9)$,
 $A_3 = \text{circ}(\alpha_7, \alpha_{14}, \alpha_{15}, \alpha_7, \alpha_{14}, \alpha_{15})$, $A_4 = \text{circ}(\alpha_9, \alpha_{20}, \alpha_{14}, \alpha_9, \alpha_{20}, \alpha_{14})$,
 $A_5 = \text{circ}(\alpha_7, \alpha_9, \alpha_8, \alpha_7, \alpha_9, \alpha_8)$, $A_6 = \text{circ}(\alpha_1, \alpha_{14}, \alpha_{14}, \alpha_1, \alpha_{14}, \alpha_{14})$,
 $A_7 = \text{circ}(\alpha_7, \alpha_{20}, \alpha_2, \alpha_7, \alpha_{20}, \alpha_2)$, $A_8 = \text{circ}(\alpha_{15}, \alpha_9, \alpha_2, \alpha_{15}, \alpha_9, \alpha_2)$,
 $A_9 = \text{circ}(\alpha_7, \alpha_{15}, \alpha_{14}, \alpha_7, \alpha_{15}, \alpha_{14})$, $A_{10} = \text{circ}(\alpha_7, \alpha_2, \alpha_{20}, \alpha_7, \alpha_2, \alpha_{20})$,
 $A_{11} = \text{circ}(\alpha_1, \alpha_9, \alpha_9, \alpha_1, \alpha_9, \alpha_9)$, $A_{12} = \text{circ}(\alpha_2, \alpha_{14}, \alpha_8, \alpha_2, \alpha_{14}, \alpha_8)$,
 $A_{13} = \text{circ}(\alpha_9, \alpha_{14}, \alpha_{20}, \alpha_9, \alpha_{14}, \alpha_{20})$, $A_{14} = \text{circ}(\alpha_{15}, \alpha_2, \alpha_9, \alpha_{15}, \alpha_2, \alpha_9)$,
 $A_{15} = \text{circ}(\alpha_2, \alpha_8, \alpha_{14}, \alpha_2, \alpha_8, \alpha_{14})$, $A_{16} = \text{circ}(\alpha_1, \alpha_7, \alpha_7, \alpha_1, \alpha_7, \alpha_7)$.

За властивостями кодових слів розширеного бінарного коду Голя відстань Хемінга $w(r)$ від нульової послідовності до будь-якого ряду r , який буде зрозуміло ненульовим, матриці $\sigma(\kappa_3)$ кратна 4 тоді відстань Хемінга від нульової послідовності до будь-якого з перших 6-х рядків рівна

$$2w(\alpha_1, \alpha_2, \alpha_2, \alpha_7, \alpha_8, \alpha_9, \alpha_7, \alpha_{14}, \alpha_{15}, \alpha_9, \alpha_{20}, \alpha_{14}) \equiv 0 \pmod{4}.$$

Звідси $\alpha_1 + \alpha_8 + \alpha_{15} + \alpha_{20} = 0$. Рядки $\sigma(\kappa_3)$ з номерами $1 + 6i$, $2 + 6i$, $3 + 6i$ дорівнюють відповідно рядкам $\sigma(\kappa_3)$ з номерами $4 + 6i$, $5 + 6i$, $6 + 6i$ ($i = 0, 1, 2, 3$). Аналогічне справедливе для стовпців. Тоді $12 = \text{rank}(\sigma(\kappa_3)) = \text{rank } A$, де

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{pmatrix},$$

де $a_1 = \text{circ}(\alpha_1, \alpha_2, \alpha_2)$, $a_2 = \text{circ}(\alpha_7, \alpha_8, \alpha_9)$, $a_3 = \text{circ}(\alpha_7, \alpha_{14}, \alpha_{15})$,
 $a_4 = \text{circ}(\alpha_9, \alpha_{20}, \alpha_{14})$, $a_5 = \text{circ}(\alpha_7, \alpha_9, \alpha_8)$, $a_6 = \text{circ}(\alpha_1, \alpha_{14}, \alpha_{14})$,
 $a_7 = \text{circ}(\alpha_7, \alpha_{20}, \alpha_2)$, $a_8 = \text{circ}(\alpha_{15}, \alpha_9, \alpha_2)$, $a_9 = \text{circ}(\alpha_7, \alpha_{15}, \alpha_{14})$,
 $a_{10} = \text{circ}(\alpha_7, \alpha_2, \alpha_{20})$, $a_{11} = \text{circ}(\alpha_1, \alpha_9, \alpha_9)$, $a_{12} = \text{circ}(\alpha_2, \alpha_{14}, \alpha_8)$,
 $a_{13} = \text{circ}(\alpha_9, \alpha_{14}, \alpha_{20})$, $a_{14} = \text{circ}(\alpha_{15}, \alpha_2, \alpha_9)$, $a_{15} = \text{circ}(\alpha_2, \alpha_8, \alpha_{14})$,
 $a_{16} = \text{circ}(\alpha_1, \alpha_7, \alpha_7)$. Отже, A оборотна матриця, яка однак має власний
вектор $v = (1, \dots, 1)$ з власним значенням $\alpha_1 + \alpha_8 + \alpha_{15} + \alpha_{20} = 0$. Що
неможливо.

Перевіримо одержаний результат безпосереднім підрахунком. Обчисленнями в GAP у додатку B.1 з'ясовано, що є 64 елементи

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(x + x^5) + \alpha_3(x^2 + x^4) + \alpha_4x^3 + \alpha_7(y + x^3y^2) + \alpha_8(xy + x^4y) + \\ & \alpha_9(x^2y + y^2x) + \alpha_{10}(x^3y + y^2) + \alpha_{12}(x^5y + x^3y^2x) + \alpha_{14}(xy^2 + x^5y^2x) + \\ & \alpha_{15}(x^2y^2 + x^5y^2) + \alpha_{17}(x^4y^2 + x^2y^2x) + \alpha_{20}(xy^2z + x^4y^2x) \in \mathbb{F}_2SL(2, 3), \end{aligned}$$

що $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\kappa_2)) = 12$. З них всім 64 відповідають $[24, 12, 2]$ -коди і нема жодного якому відповідає $[24, 12, 8]$ -код. Також одержуємо неможливість побудови розширених кодів Голя з $\mathbb{F}_2SL(2, 3)$ описаним способом.

7.2.2. Група $C_4 \times S_3$. Групу можна задати через твірні елементи та визначальні співвідношення так $G = C_4 \times S_3 = \langle x, y, z \mid x^4 = y^3 = z^2 = 1, yx = xy, zx = xz, zyz y = 1 \rangle$.

Позначимо $a = xy$, тоді $za = zxy = xy^{-1}z = a^9a^{-4}z = a^5z$. Тоді також $C_4 \times S_3 = \langle a, z \mid a^{12} = z^2 = 1, za = a^5z \rangle$. Можна перевірити таке задання наведеними обчислення в GAP у додатку B.2 а також встановлено однозначне представлення елементів групи у вказаному вигляді

$$\begin{aligned} G = \{ & 1, \quad a, \quad a^2, \quad a^3, \quad a^4, \quad a^5, \quad a^6, \quad a^7, \quad a^8, \quad a^9, \quad a^{10}, \quad a^{11}, \\ & z, \quad az, \quad a^2z, \quad a^3z, \quad a^4z, \quad a^5z, \quad a^6z, \quad a^7z, \quad a^8z, \quad a^9z, \quad a^{10}z, \quad a^{11}z \} \end{aligned}$$

$$1) \sigma(\alpha) = \sigma(\alpha)^T,$$

$$2) \sigma(\alpha)^2 = 0_{24 \times 24},$$

$$3) \text{Rank}(\sigma(\alpha)) = 12,$$

для деяких дільників нуля α з $\mathbb{F}_2(C_4 \times S_3)$. З умови $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, отримаємо, що $\alpha_8 = \alpha_6$, $\alpha_9 = \alpha_5$, $\alpha_{10} = \alpha_4$, $\alpha_{11} = \alpha_3$, $\alpha_{12} = \alpha_2$, $\alpha_{20} = \alpha_{14}$, $\alpha_{22} = \alpha_{16}$ і $\alpha_{24} = \alpha_{18}$. Умови підтверджуються також обчисленнями в GAP наведеними в додатку В.2. Тепер нехай

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(a + a^{11}) + \alpha_3(a^2 + a^{10}) + \alpha_4(a^3 + a^9) + \alpha_5(a^4 + a^8) + \\ & \alpha_6(a^5 + a^7) + \alpha_7a^6 + \alpha_{13}z + \alpha_{14}(az + a^7z) + \alpha_{15}a^2z + \alpha_{16}(a^3z + a^9z) + \\ & \alpha_{17}a^4z + \alpha_{18}(a^5z + a^{11}z) + \alpha_{19}a^6z + \alpha_{21}a^8z + \alpha_{23}a^{10}z \in \mathbb{F}_2(C_4 \times S_3), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$. Тоді

$$\sigma(\kappa_2)^2 = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix},$$

де

$$B_1 = \text{circ}(\gamma_7, \gamma_4, \gamma_6, 0, \gamma_5, \gamma_4, 0, \gamma_4, \gamma_5, 0, \gamma_6, \gamma_4),$$

$$B_2 = \text{circ}(0, \gamma_1, 0, \gamma_3, 0, \gamma_2, 0, \gamma_1, 0, \gamma_3, 0, \gamma_2),$$

$$B_3 = \text{circ}(0, \gamma_2, 0, \gamma_3, 0, \gamma_1, 0, \gamma_2, 0, \gamma_3, 0, \gamma_1),$$

$$B_4 = \text{circ}(\gamma_7, \gamma_4, \gamma_6, 0, \gamma_5, \gamma_4, 0, \gamma_4, \gamma_5, 0, \gamma_6, \gamma_4);$$

$$\gamma_1 = (\alpha_2 + \alpha_6)(\alpha_{13} + \alpha_{15} + \alpha_{19} + \alpha_{21}),$$

$$\gamma_2 = (\alpha_2 + \alpha_6)(\alpha_{13} + \alpha_{17} + \alpha_{19} + \alpha_{23}),$$

$$\gamma_3 = (\alpha_2 + \alpha_6)(\alpha_{15} + \alpha_{17} + \alpha_{21} + \alpha_{23}),$$

$$\begin{aligned} \gamma_4 = & \alpha_{13}\alpha_{14} + \alpha_{14}\alpha_{15} + \alpha_{15}\alpha_{16} + \alpha_{16}\alpha_{17} + \alpha_{13}\alpha_{18} + \alpha_{17}\alpha_{18} + \alpha_{14}\alpha_{19} + \\ & \alpha_{18}\alpha_{19} + \alpha_{14}\alpha_{21} + \alpha_{16}\alpha_{21} + \alpha_{16}\alpha_{23} + \alpha_{18}\alpha_{23}, \end{aligned}$$

$$\gamma_5 = \alpha_3^2 + \alpha_5^2 + \alpha_{13}\alpha_{17} + \alpha_{15}\alpha_{19} + \alpha_{13}\alpha_{21} + \alpha_{17}\alpha_{21} + \alpha_{15}\alpha_{23} + \alpha_{19}\alpha_{23},$$

$$\gamma_6 = \alpha_2^2 + \alpha_6^2 + \alpha_{13}\alpha_{15} + \alpha_{15}\alpha_{17} + \alpha_{17}\alpha_{19} + \alpha_{19}\alpha_{21} + \alpha_{13}\alpha_{23} + \alpha_{21}\alpha_{23},$$

$$\gamma_7 = \alpha_1^2 + \alpha_7^2 + \alpha_{13}^2 + \alpha_{15}^2 + \alpha_{17}^2 + \alpha_{19}^2 + \alpha_{21}^2 + \alpha_{23}^2.$$

$\sigma(\kappa_2)^2 = 0_{24 \times 24}$ лише якщо $\gamma_i = 0$. Припустимо спочатку, що $\alpha_2 + \alpha_6 = 1$. Тоді $\alpha_2 + 1 = \alpha_6$. З умов $\gamma_1 = \gamma_2 = 0$ одержимо $\alpha_{21} = \alpha_{13} + \alpha_{15} + \alpha_{19}$, $\alpha_{23} = \alpha_{13} + \alpha_{17} + \alpha_{19}$. Крім того, $\gamma_6 = \alpha_2^2 + \alpha_6^2 + \alpha_{13}\alpha_{15} + \alpha_{15}\alpha_{17} + \alpha_{17}\alpha_{19} + \alpha_{19}\alpha_{21} + \alpha_{13}\alpha_{23} + \alpha_{21}\alpha_{23} = \alpha_2^2 + (\alpha_2 + 1)^2 + \alpha_{13}\alpha_{15} + \alpha_{15}\alpha_{17} + \alpha_{17}\alpha_{19} + \alpha_{19}(\alpha_{13} + \alpha_{15} + \alpha_{19}) + \alpha_{13}(\alpha_{13} + \alpha_{17} + \alpha_{19}) + (\alpha_{13} + \alpha_{15} + \alpha_{19})(\alpha_{13} + \alpha_{17} + \alpha_{19}) = 1 + \alpha_{13}\alpha_{15} + \alpha_{15}\alpha_{17} + \alpha_{17}\alpha_{19} + \alpha_{13}\alpha_{19} + \alpha_{15}\alpha_{19} + \alpha_{19}^2 + \alpha_{13}^2 + \alpha_{13}\alpha_{17} + \alpha_{13}\alpha_{19} + \alpha_{13}^2 + \alpha_{13}\alpha_{17} + \alpha_{13}\alpha_{19} + \alpha_{13}\alpha_{15} + \alpha_{15}\alpha_{17} + \alpha_{15}\alpha_{19} + \alpha_{13}\alpha_{19} + \alpha_{17}\alpha_{19} + \alpha_{19}^2 = 1$., що неможливо.

Припустимо тепер, що ми маємо $\alpha_2 + \alpha_6 = 0$. Тоді $\alpha_6 = \alpha_2$ і

$$\left\{ \begin{array}{l} \alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21} + \alpha_{23} = 0, \\ \alpha_{13}\alpha_{15} + \alpha_{15}\alpha_{17} + \alpha_{17}\alpha_{19} + \alpha_{19}\alpha_{21} + \alpha_{13}\alpha_{23} + \alpha_{21}\alpha_{23} = 0, \\ \alpha_3^2 + \alpha_5^2 + \alpha_{13}\alpha_{17} + \alpha_{15}\alpha_{19} + \alpha_{13}\alpha_{21} + \alpha_{17}\alpha_{21} + \alpha_{15}\alpha_{23} + \alpha_{19}\alpha_{23} = 0, \\ \alpha_{13}\alpha_{14} + \alpha_{14}\alpha_{15} + \alpha_{15}\alpha_{16} + \alpha_{16}\alpha_{17} + \alpha_{13}\alpha_{18} + \alpha_{17}\alpha_{18} + \alpha_{14}\alpha_{19} + \alpha_{18}\alpha_{19} + \\ \alpha_{14}\alpha_{21} + \alpha_{16}\alpha_{21} + \alpha_{16}\alpha_{23} + \alpha_{18}\alpha_{23} = 0. \end{array} \right.$$

Тоді

$$\left\{ \begin{array}{l} \alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21} + \alpha_{23} = 0, \\ \alpha_{13}\alpha_{15} + \alpha_{15}\alpha_{17} + \alpha_{17}\alpha_{19} + \alpha_{19}\alpha_{21} + \alpha_{13}\alpha_{23} + \alpha_{21}\alpha_{23} = 0, \\ \alpha_3^2 + \alpha_5^2 + \alpha_{13}\alpha_{17} + \alpha_{15}\alpha_{19} + \alpha_{13}\alpha_{21} + \alpha_{17}\alpha_{21} + \alpha_{15}\alpha_{23} + \alpha_{19}\alpha_{23} = 0, \\ (\alpha_{13} + \alpha_{19})(\alpha_{14} + \alpha_{18}) + (\alpha_{15} + \alpha_{21})(\alpha_{14} + \alpha_{16}) + (\alpha_{17} + \alpha_{23})(\alpha_{16} + \alpha_{18}) = 0. \end{array} \right.$$

Звідси $\alpha_{23} = \alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21}$ і

$$\left\{ \begin{array}{l} \alpha_{13}\alpha_{14} + \alpha_{14}\alpha_{15} + \alpha_1\alpha_{16} + \alpha_7\alpha_{16} + \alpha_{13}\alpha_{16} + \alpha_1\alpha_{18} + \alpha_7\alpha_{18} + \alpha_{15}\alpha_{18} + \\ \alpha_{14}\alpha_{19} + \alpha_{16}\alpha_{19} + \alpha_{14}\alpha_{21} + \alpha_{18}\alpha_{21} = 0, \\ \alpha_3^2 + \alpha_5^2 + \alpha_1\alpha_{15} + \alpha_7\alpha_{15} + \alpha_{13}\alpha_{15} + \alpha_{15}^2 + \alpha_{13}\alpha_{17} + \alpha_{15}\alpha_{17} + \alpha_1\alpha_{19} + \alpha_7\alpha_{19} + \\ \alpha_{13}\alpha_{19} + \alpha_{15}\alpha_{19} + \alpha_{17}\alpha_{19} + \alpha_{19}^2 + \alpha_{13}\alpha_{21} + \alpha_{15}\alpha_{21} + \alpha_{17}\alpha_{21} + \alpha_{19}\alpha_{21} = 0, \\ (\alpha_{13} + \alpha_{19})(\alpha_{14} + \alpha_{18}) + (\alpha_{15} + \alpha_{21})(\alpha_{14} + \alpha_{16}) + \\ (\alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{19} + \alpha_{21})(\alpha_{16} + \alpha_{18}) = 0. \end{array} \right.$$

Тоді

$$\left\{ \begin{array}{l} (\alpha_1 + \alpha_7)(\alpha_{16} + \alpha_{18}) + (\alpha_{13} + \alpha_{19})(\alpha_{14} + \alpha_{16}) + (\alpha_{15} + \alpha_{21})(\alpha_{14} + \alpha_{18}) = 0, \\ \alpha_3^2 + \alpha_5^2 + \alpha_{19}^2 + \alpha_{15}^2 + (\alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{17} + \alpha_{21})(\alpha_{15} + \alpha_{19}) + \alpha_{15}\alpha_{19} + \\ \alpha_{13}\alpha_{17} + \alpha_{13}\alpha_{21} + \alpha_{17}\alpha_{21} = 0, \\ (\alpha_{13} + \alpha_{19})(\alpha_{14} + \alpha_{18}) + (\alpha_{15} + \alpha_{21})(\alpha_{14} + \alpha_{16}) + \\ (\alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{19} + \alpha_{21})(\alpha_{16} + \alpha_{18}) = 0. \end{array} \right. \quad (7.6)$$

Обчисленнями в GAP у додатку В.2 з'ясовано, що є 1920 елементів

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(a + a^{11}) + \alpha_3(a^2 + a^{10}) + \alpha_4(a^3 + a^9) + \alpha_5(a^4 + a^8) + \\ & \alpha_6(a^5 + a^7) + \alpha_7a^6 + \alpha_{13}z + \alpha_{14}(az + a^7z) + \alpha_{15}a^2z + \alpha_{16}(a^3z + a^9z) + \\ & \alpha_{17}a^4z + \alpha_{18}(a^5z + a^{11}z) + \alpha_{19}a^6z + \alpha_{21}a^8z + \alpha_{23}a^{10}z \in \mathbb{F}_2(C_4 \times S_3), \end{aligned}$$

що задовольняють систему разом з введеними обмеженнями:

$$\begin{aligned} \alpha_6 &= \alpha_2, \\ \alpha_{23} &= \alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21} \end{aligned}$$

та $\text{Rank}(\sigma(\kappa_2)) = 12$. З них 352 відповідають $[24, 12, 2]$ -коди, 1568 — відповідають $[24, 12, 4]$ -коди і немає жодного якому відповідає $[24, 12, 8]$ -код. Отже, не можна побудувати розширений код Голя з $\mathbb{F}_2SL(2, 3)$ описаним способом.

7.2.3. Група $(C_6 \times C_2) \rtimes C_2$. Групу можна задати через твірні елементи та визначальні співвідношення так $(C_6 \times C_2) \rtimes C_2 = \langle x, y, z \mid x^3 = 1, y^4 = 1, z^2 = 1, yz = zy^3, xy = yx^2, xz = zx \rangle$. Таке задання перевірене обчисленнями в GAP наведеному в додатку В.3 а також встановлено

однозначне представлення елементів групи у вказаному вигляді

$$G = \{1, \quad y, \quad y^2, \quad y^3, \\ x, \quad xy, \quad xy^2, \quad xy^3, \\ x^2, \quad x^2y, \quad x^2y^2, \quad x^2y^3, \\ z, \quad yz, \quad y^2z, \quad y^3z, \\ xz, \quad xyz, \quad xy^2z, \quad xy^3z, \\ x^2z, \quad x^2yz, \quad x^2y^2z, \quad x^2y^3z\}$$

та визначено порядок їх розташування в групі.

Тепер ми доведемо, що можна побудувати розширений код Голя з $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$. Розглянемо код C_κ для

$$\begin{aligned} \kappa = \kappa_1 = & \alpha_1 + \alpha_2 y + \alpha_3 y^2 + \alpha_4 y^3 + \\ & \alpha_5 x + \alpha_6 xy + \alpha_7 xy^2 + \alpha_8 xy^3 + \\ & \alpha_9 x^2 + \alpha_{10} x^2 y + \alpha_{11} x^2 y^2 + \alpha_{12} x^2 y^3 + \\ & \alpha_{13} z + \alpha_{14} yz + \alpha_{15} y^2 z + \alpha_{16} y^3 z + \\ & \alpha_{17} xz + \alpha_{18} xyz + \alpha_{19} xy^2 z + \alpha_{20} xy^3 z + \\ & \alpha_{21} x^2 z + \alpha_{22} x^2 yz + \alpha_{23} x^2 y^2 z + \alpha_{24} x^2 y^3 z \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$. Було з'ясовано обчисленнями в GАР наведеними в додатку

В.3 вигляд матриці $\sigma(\kappa_1)$:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{19} \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{22} \\ \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{17} \\ \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} \\ \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{18} \\ \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{21} \\ \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} \\ \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{16} & \alpha_{13} & \alpha_{14} & \alpha_{15} \\ \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_{10} & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{18} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{22} & \alpha_{15} & \alpha_{16} & \alpha_{13} & \alpha_{14} \\ \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_9 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_{22} & \alpha_{23} & \alpha_{24} & \alpha_{21} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{17} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{13} \\ \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_{10} \\ \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 \\ \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_{12} \\ \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 \\ \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 \\ \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_{11} \\ \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 \\ \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 \\ \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 \\ \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{23} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{19} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_{11} & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 \\ \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{20} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{24} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_{12} & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 \\ \alpha_{24} & \alpha_{23} & \alpha_{22} & \alpha_{21} & \alpha_{20} & \alpha_{19} & \alpha_{18} & \alpha_{17} & \alpha_{16} & \alpha_{15} & \alpha_{14} & \alpha_{13} & \alpha_{12} & \alpha_{11} & \alpha_{10} & \alpha_9 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 \end{pmatrix}.$$

Для умови $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, достатньо, щоб $\alpha_4 = \alpha_2$, $\alpha_8 = \alpha_6$, $\alpha_9 = \alpha_5$, $\alpha_{11} = \alpha_7$, $\alpha_{12} = \alpha_{10}$, $\alpha_{21} = \alpha_{17}$ і $\alpha_{23} = \alpha_{19}$. Умови підтверджуються також обчисленнями в GAP наведеними в додатку В.3. Таким чином $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, якщо елемент $\kappa_1 \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$ приймає форму:

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(y + y^3) + \alpha_3y^2 + \alpha_5(x + x^2) + \alpha_6(xy + xy^3) + \\ & \alpha_7(xy^2 + x^2y^2) + \alpha_{10}(x^2y + x^2y^3) + \alpha_{13}z + \alpha_{14}yz + \alpha_{15}y^2z + \\ & \alpha_{16}y^3z + \alpha_{17}(xz + x^2z) + \alpha_{18}xyz + \alpha_{19}(xy^2z + x^2y^2z) + \\ & \alpha_{20}xy^3z + \alpha_{22}x^2yz + \alpha_{24}x^2y^3z = \\ & \alpha_1 + \alpha_3y^2 + (\alpha_2 + \alpha_6x + \alpha_{10}x^2)(y + y^3) + \\ & (x + x^2)(\alpha_5 + \alpha_7y^2 + \alpha_{17}z + \alpha_{19}y^2z) + \\ & \alpha_{13}z + \alpha_{14}yz + \alpha_{15}y^2z + \alpha_{16}y^3z + \\ & \alpha_{18}xyz + \alpha_{20}xy^3z + \alpha_{22}x^2yz + \alpha_{24}x^2y^3z \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2) \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$.

Далі матриця $\sigma(\kappa_2)^2$ набуде вигляду:

$$\begin{pmatrix} \gamma_7 & \gamma_5 & 0 & \gamma_5 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_2 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 \\ \gamma_5 & \gamma_7 & \gamma_5 & 0 & \gamma_2 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 \\ 0 & \gamma_5 & \gamma_7 & \gamma_5 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_2 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 \\ \gamma_5 & 0 & \gamma_5 & \gamma_7 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 \\ \gamma_6 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_7 & \gamma_5 & 0 & \gamma_5 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 \\ \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_5 & \gamma_7 & \gamma_5 & 0 & \gamma_2 & \gamma_6 & \gamma_2 & \gamma_3 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 \\ \gamma_3 & \gamma_2 & \gamma_6 & \gamma_2 & 0 & \gamma_5 & \gamma_7 & \gamma_5 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 \\ \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_5 & 0 & \gamma_5 & \gamma_7 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_6 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 \\ \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_7 & \gamma_5 & 0 & \gamma_5 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 \\ \gamma_2 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_5 & \gamma_7 & \gamma_5 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 \\ \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_2 & 0 & \gamma_5 & \gamma_7 & \gamma_5 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 \\ \gamma_2 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_5 & 0 & \gamma_5 & \gamma_7 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_7 & \gamma_5 & 0 & \gamma_5 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_2 \\ 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & \gamma_5 & \gamma_7 & \gamma_5 & 0 & \gamma_2 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 \\ 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & \gamma_5 & \gamma_7 & \gamma_5 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_2 \\ 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & \gamma_5 & 0 & \gamma_5 & \gamma_7 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 \\ 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_7 & \gamma_5 & 0 & \gamma_2 & \gamma_6 & \gamma_2 & \gamma_3 \\ \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_2 & 0 & \gamma_5 & \gamma_7 & \gamma_5 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 \\ 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_2 & 0 & \gamma_5 & \gamma_7 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_6 \\ \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_7 & \gamma_5 & 0 & \gamma_5 \\ 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_2 & \gamma_6 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_5 & \gamma_7 & \gamma_5 & 0 \\ \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_2 & 0 & \gamma_5 & \gamma_7 & \gamma_5 \\ 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & \gamma_1 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_2 & \gamma_3 & \gamma_2 & \gamma_6 & \gamma_4 & \gamma_3 & \gamma_4 & \gamma_6 & \gamma_5 & 0 & \gamma_5 & \gamma_7 \end{pmatrix},$$

де $\gamma_1 = \alpha_6\alpha_{14} + \alpha_{10}\alpha_{14} + \alpha_6\alpha_{16} + \alpha_{10}\alpha_{16} + \alpha_2\alpha_{18} + \alpha_{10}\alpha_{18} + \alpha_2\alpha_{20} + \alpha_{10}\alpha_{20} + \alpha_2\alpha_{22} + \alpha_6\alpha_{22} + \alpha_2\alpha_{24} + \alpha_6\alpha_{24}$,

$$\gamma_2 = \alpha_{14}\alpha_{17} + \alpha_{16}\alpha_{17} + \alpha_{17}\alpha_{18} + \alpha_{14}\alpha_{19} + \alpha_{16}\alpha_{19} + \alpha_{18}\alpha_{19} + \alpha_{17}\alpha_{20} + \alpha_{19}\alpha_{20} + \alpha_{13}\alpha_{22} + \alpha_{15}\alpha_{22} + \alpha_{13}\alpha_{24} + \alpha_{15}\alpha_{24},$$

$$\gamma_3 = \alpha_{16}\alpha_{18} + \alpha_{14}\alpha_{20} + \alpha_{16}\alpha_{22} + \alpha_{20}\alpha_{22} + \alpha_{14}\alpha_{24} + \alpha_{18}\alpha_{24},$$

$$\gamma_4 = \alpha_{14}\alpha_{17} + \alpha_{16}\alpha_{17} + \alpha_{13}\alpha_{18} + \alpha_{15}\alpha_{18} + \alpha_{14}\alpha_{19} + \alpha_{16}\alpha_{19} + \alpha_{13}\alpha_{20} + \alpha_{15}\alpha_{20} + \alpha_{17}\alpha_{22} + \alpha_{19}\alpha_{22} + \alpha_{17}\alpha_{24} + \alpha_{19}\alpha_{24},$$

$$\gamma_5 = \alpha_{13}\alpha_{14} + \alpha_{14}\alpha_{15} + \alpha_{13}\alpha_{16} + \alpha_{15}\alpha_{16} + \alpha_{17}\alpha_{18} + \alpha_{18}\alpha_{19} + \alpha_{17}\alpha_{20} + \alpha_{19}\alpha_{20} + \alpha_{17}\alpha_{22} + \alpha_{19}\alpha_{22} + \alpha_{17}\alpha_{24} + \alpha_{19}\alpha_{24},$$

$$\gamma_6 = \alpha_5^2 + \alpha_7^2 + \alpha_{17}^2 + \alpha_{14}\alpha_{18} + \alpha_{19}^2 + \alpha_{16}\alpha_{20} + \alpha_{14}\alpha_{22} + \alpha_{18}\alpha_{22} + \alpha_{16}\alpha_{24} + \alpha_{20}\alpha_{24},$$

$$\gamma_7 = \alpha_1^2 + \alpha_3^2 + \alpha_{13}^2 + \alpha_{14}^2 + \alpha_{15}^2 + \alpha_{16}^2 + \alpha_{18}^2 + \alpha_{20}^2 + \alpha_{22}^2 + \alpha_{24}^2. \text{ З умови } \sigma(\kappa_2)^2 = 0_{24 \times 24}, \text{ зокрема, одержимо:}$$

$$\begin{cases} \alpha_{19} = \alpha_5 + \alpha_7 + \alpha_{17} + \alpha_{14}\alpha_{18} + \alpha_{16}\alpha_{20} + \alpha_{14}\alpha_{22} + \alpha_{18}\alpha_{22} + \alpha_{16}\alpha_{24} + \alpha_{20}\alpha_{24}, \\ \alpha_{24} = \alpha_1 + \alpha_3 + \alpha_{13} + \alpha_{14} + \alpha_{15} + \alpha_{16} + \alpha_{18} + \alpha_{20} + \alpha_{22}. \end{cases} \quad (7.7)$$

Нехай $\kappa_3 = y^2 + x^2(y + y^3) + (x + x^2)y^2z + \hat{x}y^3z \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$, де $\hat{x} = 1 + x + x^2$. Зрозуміло $\sigma(\kappa_3) = \sigma(\kappa_3)^T$. Крім того,

- $y^2x^2(y + y^3) = x^2y^2(y + y^3) = x^2(y + y^3)y^2,$
- $y^2(x + x^2)y^2z = (x + x^2)z = (x + x^2)y^2zy^2,$
- $y^2\hat{x}y^3z = \hat{x}yz = \hat{x}y^3zy^2$
- $x^2(y + y^3)(x + x^2)y^2z = (x + x^2)y^2zx^2(y + y^3),$
- $x^2(y + y^3)\hat{x}y^3z = x^2\hat{x}y^3(y + y^3)z = \hat{x}xy^3z(y + y^3) = \hat{x}y^3x^2z(y + y^3) = \hat{x}y^3zx^2(y + y^3) \text{ і}$
- $(x + x^2)y^2z\hat{x}y^3z = (x + x^2)\hat{x}y^2zyy^3z = (\hat{x} = \hat{x})y^2zyy^3z = 0 = \hat{x}y^3z(x + x^2)y^2z.$

Тому

$$\begin{aligned}
 \kappa_3^2 &= (y^2)^2 + (x^2(y + y^3))^2 + ((x + x^2)y^2z)^2 + (\hat{x}y^3z)^2 \\
 &= 1 + (y + y^3)^2 + (x + x^2)^2 + (\hat{x})^2y^2zy^3z \\
 &= 1 + x + x^2 + \hat{x} \\
 &= 2\hat{x} = 0.
 \end{aligned}$$

З вигляду κ_3 одержимо, що

$$\sigma(\kappa_3) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Обчисленнями в GAP у додатку В.3 з'ясовано, що розмірність простору його кодових слів 12 а мінімальна відстань 8. Крім того, було показано, що є 5760 елементів

$$\begin{aligned}
 \kappa_2 = & \alpha_1 + \alpha_2 (y + y^3) + \alpha_3 y^2 + \alpha_5 (x + x^2) + \alpha_6 (xy + xy^3) + \\
 & \alpha_7 (xy^2 + x^2 y^2) + \alpha_{10} (x^2 y + x^2 y^3) + \alpha_{13} z + \alpha_{14} yz + \alpha_{15} y^2 z + \\
 & \alpha_{16} y^3 z + \alpha_{17} (xz + x^2 z) + \alpha_{18} xyz + \alpha_{19} (xy^2 z + x^2 y^2 z) + \\
 & \alpha_{20} xy^3 z + \alpha_{22} x^2 yz + \alpha_{24} x^2 y^3 z \mathbb{F}_2((C_6 \times C_2) \rtimes C_2),
 \end{aligned}$$

що задовольняють умови $\sigma(\alpha)^2 = 0_{24 \times 24}$, $Rank(\sigma(\alpha)) = 12$. З них 416 відповідають $[24, 12, 2]$ -коди, 4192 — відповідають $[24, 12, 4]$ -коди, 576 — відповідають $[24, 12, 6]$ -коди і 576 — відповідають $[24, 12, 8]$ -коди.

7.2.4. Група $C_3 \times D_8$. Групу можна задати через твірні елементи та визначальні співвідношення так $C_3 \times D_8 = \langle x, y, z \mid x^3 = y^4 = z^2 = 1, xy = yx, xz = zx, yzyz = 1 \rangle$. Таке задання перевірене обчисленнями в GАР наведеними в додатку В.4 а також встановлено однозначне представлення елементів групи у вказаному вигляді

$$G = \{1, \quad y, \quad y^2, \quad y^3, \\ x, \quad yx, \quad y^2x, \quad y^3x, \\ x^2, \quad yx^2, \quad y^2x^2, \quad y^3x^2, \\ z, \quad zy, \quad zy^2, \quad zy^3, \\ zx, \quad zyx, \quad zy^2x, \quad zy^3x, \\ zx^2, \quad zyx^2, \quad zy^2x^2, \quad zy^3x^2\}$$

та визначено порядок їх розташування в групі.

Тепер ми доведемо, що можна побудувати розширений код Голея з $\mathbb{F}_2(C_3 \times D_8)$. Розглянемо код C_κ для

$$\begin{aligned} \kappa = \kappa_1 = & \alpha_1 + \alpha_2 y + \alpha_3 y^2 + \alpha_4 y^3 + \\ & \alpha_5 x + \alpha_6 yx + \alpha_7 y^2 x + \alpha_8 y^3 x + \\ & \alpha_9 x^2 + \alpha_{10} yx^2 + \alpha_{11} y^2 x^2 + \alpha_{12} y^3 x^2 + \\ & \alpha_{13} z + \alpha_{14} zy + \alpha_{15} zy^2 + \alpha_{16} zy^3 + \\ & \alpha_{17} zx + \alpha_{18} zyx + \alpha_{19} zy^2 x + \alpha_{20} zy^3 x + \\ & \alpha_{21} zx^2 + \alpha_{22} zyx^2 + \alpha_{23} zy^2 x^2 + \alpha_{24} zy^3 x^2 \in \mathbb{F}_2(C_3 \times D_8), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2(C_3 \times D_8)$. Було з'ясовано обчисленнями в GАР наведеними в

$\alpha_{12} = \alpha_6$, $\alpha_{21} = \alpha_{17}$, $\alpha_{22} = \alpha_{18}$, $\alpha_{23} = \alpha_{19}$, $\alpha_{24} = \alpha_{20}$. Умови підтверджуються також обчисленнями в GАР наведеними в додатку В.4. Таким чином $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, якщо елемент $\kappa_1 \in \mathbb{F}_2(C_3 \times D_8)$ приймає форму:

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(y + y^3) + \alpha_3y^2 + \alpha_5(x + x^2) + \alpha_6(yx + y^3x^2) + \\ & \alpha_7(y^2x + y^2x^2) + \alpha_8(yx^2 + y^3x) + \alpha_{13}z + \alpha_{14}zy + \alpha_{15}zy^2 + \alpha_{16}zy^3 + \\ & \alpha_{17}(zx + zx^2) + \alpha_{18}(zyx + zyx^2) + \alpha_{19}(zy^2x + zy^2x^2) + \alpha_{20}(zy^3x + zy^3x^2), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$. Тоді

$$\sigma(\kappa_2)^2 = \begin{pmatrix} C_1 & C_2 & C_2 & 0 & D & D \\ C_2 & C_1 & C_2 & D & 0 & D \\ C_2 & C_2 & C_1 & D & D & 0 \\ 0 & D & D & C_1 & C_2 & C_2 \\ D & 0 & D & C_2 & C_1 & C_2 \\ D & D & 0 & C_2 & C_2 & C_1 \end{pmatrix},$$

де $C_1 = \text{circ}(\gamma_3, \gamma_2, 0, \gamma_2)$, $C_2 = \text{circ}(\gamma_7, \gamma_6, \gamma_1, \gamma_6)$,

$D = \text{rcirc}(\gamma_5, \gamma_4, \gamma_5, \gamma_4)$, де

$$\gamma_1 = \alpha_6^2 + \alpha_8^2,$$

$$\gamma_2 = (\alpha_{13} + \alpha_{15})(\alpha_{14} + \alpha_{16}),$$

$$\gamma_3 = \alpha_1^2 + \alpha_3^2 + \alpha_{13}^2 + \alpha_{14}^2 + \alpha_{15}^2 + \alpha_{16}^2,$$

$$\gamma_4 = (\alpha_6 + \alpha_8)(\alpha_{13} + \alpha_{15} + \alpha_{17} + \alpha_{19}),$$

$$\gamma_5 = (\alpha_6 + \alpha_8)(\alpha_{14} + \alpha_{16} + \alpha_{18} + \alpha_{20}),$$

$$\begin{aligned} \gamma_6 = & \alpha_{14}\alpha_{17} + \alpha_{16}\alpha_{17} + \alpha_{13}\alpha_{18} + \alpha_{15}\alpha_{18} + \alpha_{17}\alpha_{18} + \alpha_{14}\alpha_{19} + \alpha_{16}\alpha_{19} + \\ & \alpha_{18}\alpha_{19} + \alpha_{13}\alpha_{20} + \alpha_{15}\alpha_{20} + \alpha_{17}\alpha_{20} + \alpha_{19}\alpha_{20}, \end{aligned}$$

$$\gamma_7 = \alpha_5^2 + \alpha_7^2 + \alpha_{17}^2 + \alpha_{18}^2 + \alpha_{19}^2 + \alpha_{20}^2.$$

З умови $\sigma(\kappa_2)^2 = 0_{24 \times 24}$, зокрема, одержимо:

$$\begin{cases} \alpha_8 &= \alpha_6, \\ \alpha_{16} &= \alpha_1 + \alpha_3 + \alpha_{13} + \alpha_{14} + \alpha_{15}, \\ \alpha_{20} &= \alpha_5 + \alpha_7 + \alpha_{17} + \alpha_{18} + \alpha_{19}. \end{cases} \quad (7.8)$$

Нехай

$$\begin{aligned} \kappa_3 &= 1 + zy + zy^2 + zy^3 + (zx + zx^2) + (zyx + zyx^2) = \\ &= 1 + z(y + y^2 + y^3 + x + x^2 + yx + yx^2) = \\ &= 1 + z(1 + 1 + y + y^2 + y^3 + (1 + y)(x + x^2)) = \\ &= 1 + z((1 + \hat{y}) + (1 + y)(1 + 1 + x + x^2)) = \\ &= 1 + z((1 + \hat{y}) + (1 + y)(1 + \hat{x})) \in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2), \end{aligned}$$

де $\hat{y} = 1 + y + y^2 + y^3$, $\hat{x} = 1 + x + x^2$. Зрозуміло $\sigma(\kappa_3) = \sigma(\kappa_3)^T$. Крім того,

$$\begin{aligned} \kappa_3^2 &= 1 + [z((1 + \hat{y}) + (1 + y)(1 + \hat{x}))]^2 = \\ &= 1 + z((1 + \hat{y}) + (1 + y)(1 + \hat{x})) z((1 + \hat{y}) + (1 + y)(1 + \hat{x})). \end{aligned}$$

Оскільки

- $y\hat{y} = y(1 + y + y^2 + y^3) = \hat{y} = (1 + y + y^2 + y^3)y = \hat{y}y$,
- $z\hat{y} = z + zy + zy^2 + zy^3 = z + y^3z + zy^2 + yz = \hat{y}z$,

елемент x центральний, $x^3 = y^4 = z^2 = 1$, $zyz = y^3$, то

$$\begin{aligned} \kappa_3^2 &= 1 + ((1 + \hat{y}) + (1 + y^3)(1 + \hat{x}))((1 + \hat{y}) + (1 + y)(1 + \hat{x})) = \\ &= 1 + (1 + \hat{y})^2 + ((1 + \hat{y})(1 + y) + (1 + y^3)(1 + \hat{y}))(1 + \hat{x}) + (1 + y^3)(1 + y)(1 + \hat{x})^2 = \\ &= 1 + (y + y^2 + y^3)^2 + (1 + y + 1 + y^3)(1 + \hat{y})(1 + \hat{x}) + (1 + y + y^3 + 1)(1 + \hat{x})^2 = \\ &= 1 + y^2 + 1 + y^2 + (y + y^3)(1 + \hat{y})(1 + \hat{x}) + (y + y^3)(x + x^2)^2 = \end{aligned}$$

$$(y+y^3)(1+\hat{y})(1+\hat{x})+(y+y^3)(x^2+x) = (y+y^3)(1+\hat{y})(1+\hat{x})+(y+y^3)(1+\hat{x}) =$$

$$(y+y^3)(1+\hat{y}+1)(1+\hat{x}) = (y+y^3)\hat{y}(1+\hat{x}) = 2\hat{y}(1+\hat{x}) = 0.$$

З вигляду κ_3 одержимо, що

$$\sigma(\kappa_3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Обчисленнями в GAP у додатку В.4 з'ясовано, що розмірність простору його кодових слів 12 а мінімальна відстань 8. Крім того, було показано, що є 1600 елементів

$$\kappa_2 = \alpha_1 + \alpha_2(y + y^3) + \alpha_3y^2 + \alpha_5(x + x^2) + \alpha_6(yx + y^3x^2) +$$

$$\alpha_7(y^2x + y^2x^2) + \alpha_8(yx^2 + y^3x) + \alpha_{13}z + \alpha_{14}zy + \alpha_{15}zy^2 + \alpha_{16}zy^3 +$$

$$\alpha_{17}(zx + zx^2) + \alpha_{18}(zyx + zy^2x) + \alpha_{19}(zy^2x + zy^2x^2) + \alpha_{20}(zy^3x + zy^3x^2),$$

що задовольняють умови $\sigma(\alpha)^2 = 0_{24 \times 24}$, $Rank(\sigma(\alpha)) = 12$. З них 128 відповідають $[24, 12, 2]$ -коди, 1216 — відповідають $[24, 12, 4]$ -коди, 128 — відповідають $[24, 12, 6]$ -коди і 128 — відповідають $[24, 12, 8]$ -коди.

7.2.5. Група $C_2 \times A_4$. Групу можна задати через твірні елементи та визначальні співвідношення так $C_2 \times A_4 = \langle x, y, z, w \mid x^2 = y^2 = z^2 = w^3 = 1, xy = yx, xz = zx, xw = wx, yz = zy, yw = wyz, zw = wy \rangle$. Таке задання перевірене обчисленнями в GAP наведеними в додатку

Тоді

$$\sigma(\kappa_1) = \begin{pmatrix} A_1 & A_2 & A_3 & B_1 & B_2 & B_3 \\ A_4 & A_5 & A_6 & B_4 & B_5 & B_6 \\ A_7 & A_8 & A_9 & B_7 & B_8 & B_9 \\ B_1 & B_2 & B_3 & A_1 & A_2 & A_3 \\ B_4 & B_5 & B_6 & A_4 & A_5 & A_6 \\ B_7 & B_8 & B_9 & A_7 & A_8 & A_9 \end{pmatrix},$$

де $A_1 = bc(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $A_2 = bc(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$, $A_3 = bc(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12})$,
 $A_4 = bc(\alpha_9, \alpha_{12}, \alpha_{10}, \alpha_{11})$, $A_5 = bc(\alpha_1, \alpha_4, \alpha_2, \alpha_3)$, $A_6 = bc(\alpha_5, \alpha_8, \alpha_6, \alpha_7)$,
 $A_7 = bc(\alpha_5, \alpha_7, \alpha_8, \alpha_6)$, $A_8 = bc(\alpha_9, \alpha_{11}, \alpha_{12}, \alpha_{10})$, $A_9 = bc(\alpha_1, \alpha_3, \alpha_4, \alpha_2)$,
 $B_1 = bc(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16})$, $B_2 = bc(\alpha_{17}, \alpha_{18}, \alpha_{19}, \alpha_{20})$, $B_3 = bc(\alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24})$,
 $B_4 = bc(\alpha_{21}, \alpha_{24}, \alpha_{22}, \alpha_{23})$, $B_5 = bc(\alpha_{13}, \alpha_{16}, \alpha_{14}, \alpha_{15})$, $B_6 = bc(\alpha_{17}, \alpha_{20}, \alpha_{18}, \alpha_{19})$,
 $B_7 = bc(\alpha_{17}, \alpha_{19}, \alpha_{20}, \alpha_{18})$, $B_8 = bc(\alpha_{21}, \alpha_{23}, \alpha_{24}, \alpha_{22})$, $B_9 = bc(\alpha_{13}, \alpha_{15}, \alpha_{16}, \alpha_{14})$,

Тут для довільних елементів a, b, c, d використовуємо позначення

$$cb(a, b, c, d) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}.$$

Для умови $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, достатньо, щоб $\alpha_9 = \alpha_5$, $\alpha_{10} = \alpha_7$, $\alpha_{11} = \alpha_8$,
 $\alpha_{12} = \alpha_6$, $\alpha_{21} = \alpha_{17}$, $\alpha_{22} = \alpha_{19}$, $\alpha_{23} = \alpha_{20}$, $\alpha_{24} = \alpha_{18}$. Умови підтверджуються також обчисленнями в GAP наведеними в додатку В.5. Таким чином $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, якщо елемент $\kappa_1 \in \mathbb{F}_2(C_2 \times A_4)$ приймає форму:

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2 y + \alpha_3 z + \alpha_4 yz + \alpha_5 (w + w^2) + \alpha_6 (yw + yzw^2) + \\ & \alpha_7 (yw^2 + zw) + \alpha_8 (zw^2 + yzw) + \alpha_{13} x + \alpha_{14} xy + \alpha_{15} xz + \alpha_{16} xyz + \\ & \alpha_{17} (xw + xw^2) + \alpha_{18} (xyw + xyzw^2) + \alpha_{19} (xyw^2 + xzw) + \\ & \alpha_{20} (xzw^2 + xyzw) \in \mathbb{F}_2(C_2 \times A_4), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$. Тоді

$$\sigma(\kappa_2)^2 = \begin{pmatrix} C_1 & C_2 & C_3 & 0 & D_1 & D_2 \\ C_2 & C_1 & C_4 & D_1 & 0 & D_3 \\ C_3 & C_4 & C_1 & D_2 & D_3 & 0 \\ 0 & D_1 & D_2 & C_1 & C_2 & C_3 \\ D_1 & 0 & D_3 & C_2 & C_1 & C_4 \\ D_2 & D_3 & 0 & C_3 & C_4 & C_1 \end{pmatrix},$$

де $C_1 = bc(\gamma_1, 0, 0, 0)$,

$$C_2 = bc(\gamma_8, \gamma_7, \gamma_6, \gamma_9), C_3 = bc(\gamma_8, \gamma_6, \gamma_9, \gamma_7), C_4 = bc(\gamma_8, \gamma_9, \gamma_7, \gamma_6),$$

$$D_1 = bc(\gamma_5, \gamma_4, \gamma_3, \gamma_2), D_2 = bc(\gamma_5, \gamma_3, \gamma_2, \gamma_4), D_3 = bc(\gamma_5, \gamma_2, \gamma_4, \gamma_3), \quad \text{де}$$

$$\gamma_1 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + \alpha_{13}^2 + \alpha_{14}^2 + \alpha_{15}^2 + \alpha_{16}^2,$$

$$\gamma_2 = \alpha_6\alpha_{14} + \alpha_7\alpha_{14} + \alpha_5\alpha_{15} + \alpha_6\alpha_{15} + \alpha_5\alpha_{16} + \alpha_7\alpha_{16} + \alpha_3\alpha_{17} + \alpha_4\alpha_{17} + \alpha_6\alpha_{17} + \alpha_7\alpha_{17} + \alpha_2\alpha_{18} + \alpha_3\alpha_{18} + \alpha_5\alpha_{18} + \alpha_7\alpha_{18} + \alpha_2\alpha_{19} + \alpha_4\alpha_{19} + \alpha_5\alpha_{19} + \alpha_6\alpha_{19},$$

$$\gamma_3 = \alpha_5\alpha_{14} + \alpha_8\alpha_{14} + \alpha_5\alpha_{15} + \alpha_6\alpha_{15} + \alpha_6\alpha_{16} + \alpha_8\alpha_{16} + \alpha_2\alpha_{17} + \alpha_3\alpha_{17} + \alpha_6\alpha_{17} + \alpha_8\alpha_{17} + \alpha_3\alpha_{18} + \alpha_4\alpha_{18} + \alpha_5\alpha_{18} + \alpha_8\alpha_{18} + \alpha_2\alpha_{20} + \alpha_4\alpha_{20} + \alpha_5\alpha_{20} + \alpha_6\alpha_{20},$$

$$\gamma_4 = \alpha_5\alpha_{14} + \alpha_8\alpha_{14} + \alpha_7\alpha_{15} + \alpha_8\alpha_{15} + \alpha_5\alpha_{16} + \alpha_7\alpha_{16} + \alpha_2\alpha_{17} + \alpha_4\alpha_{17} + \alpha_7\alpha_{17} + \alpha_8\alpha_{17} + \alpha_3\alpha_{19} + \alpha_4\alpha_{19} + \alpha_5\alpha_{19} + \alpha_8\alpha_{19} + \alpha_2\alpha_{20} + \alpha_3\alpha_{20} + \alpha_5\alpha_{20} + \alpha_7\alpha_{20},$$

$$\gamma_5 = \alpha_6\alpha_{14} + \alpha_7\alpha_{14} + \alpha_7\alpha_{15} + \alpha_8\alpha_{15} + \alpha_6\alpha_{16} + \alpha_8\alpha_{16} + \alpha_2\alpha_{18} + \alpha_4\alpha_{18} + \alpha_7\alpha_{18} + \alpha_8\alpha_{18} + \alpha_2\alpha_{19} + \alpha_3\alpha_{19} + \alpha_6\alpha_{19} + \alpha_8\alpha_{19} + \alpha_3\alpha_{20} + \alpha_4\alpha_{20} + \alpha_6\alpha_{20} + \alpha_7\alpha_{20},$$

$$\gamma_6 = \alpha_2\alpha_5 + \alpha_3\alpha_5 + \alpha_3\alpha_6 + \alpha_4\alpha_6 + \alpha_5\alpha_6 + \alpha_7^2 + \alpha_2\alpha_8 + \alpha_4\alpha_8 + \alpha_5\alpha_8 + \alpha_6\alpha_8 + \alpha_{14}\alpha_{17} + \alpha_{15}\alpha_{17} + \alpha_{15}\alpha_{18} + \alpha_{16}\alpha_{18} + \alpha_{17}\alpha_{18} + \alpha_{19}^2 + \alpha_{14}\alpha_{20} + \alpha_{16}\alpha_{20} + \alpha_{17}\alpha_{20} + \alpha_{18}\alpha_{20},$$

$$\gamma_7 = \alpha_2\alpha_5 + \alpha_4\alpha_5 + \alpha_6^2 + \alpha_3\alpha_7 + \alpha_4\alpha_7 + \alpha_5\alpha_7 + \alpha_2\alpha_8 + \alpha_3\alpha_8 + \alpha_5\alpha_8 + \alpha_7\alpha_8 + \alpha_{14}\alpha_{17} + \alpha_{16}\alpha_{17} + \alpha_{18}^2 + \alpha_{15}\alpha_{19} + \alpha_{16}\alpha_{19} + \alpha_{17}\alpha_{19} + \alpha_{14}\alpha_{20} + \alpha_{15}\alpha_{20} + \alpha_{17}\alpha_{20} + \alpha_{19}\alpha_{20},$$

$$\gamma_8 = \alpha_5^2 + \alpha_2\alpha_6 + \alpha_4\alpha_6 + \alpha_2\alpha_7 + \alpha_3\alpha_7 + \alpha_6\alpha_7 + \alpha_3\alpha_8 + \alpha_4\alpha_8 + \alpha_6\alpha_8 + \alpha_7\alpha_8 + \alpha_{17}^2 + \alpha_{14}\alpha_{18} + \alpha_{16}\alpha_{18} + \alpha_{14}\alpha_{19} + \alpha_{15}\alpha_{19} + \alpha_{18}\alpha_{19} + \alpha_{15}\alpha_{20} + \alpha_{16}\alpha_{20} +$$

$$\alpha_{18}\alpha_{20} + \alpha_{19}\alpha_{20},$$

$$\begin{aligned} \gamma_9 = & \alpha_3\alpha_5 + \alpha_4\alpha_5 + \alpha_2\alpha_6 + \alpha_3\alpha_6 + \alpha_5\alpha_6 + \alpha_2\alpha_7 + \alpha_4\alpha_7 + \alpha_5\alpha_7 + \alpha_6\alpha_7 + \\ & \alpha_8^2 + \alpha_{15}\alpha_{17} + \alpha_{16}\alpha_{17} + \alpha_{14}\alpha_{18} + \alpha_{15}\alpha_{18} + \alpha_{17}\alpha_{18} + \alpha_{14}\alpha_{19} + \alpha_{16}\alpha_{19} + \alpha_{17}\alpha_{19} + \\ & \alpha_{18}\alpha_{19} + \alpha_{20}^2. \end{aligned}$$

Крім того, $\gamma_6 + \gamma_7 + \gamma_8 + \gamma_9 = \alpha_5^2 + \alpha_6^2 + \alpha_7^2 + \alpha_8^2 + \alpha_{17}^2 + \alpha_{18}^2 + \alpha_{19}^2 + \alpha_{20}^2$.

З умови $\sigma(\kappa_2)^2 = 0_{24 \times 24}$, зокрема, одержимо:

$$\begin{cases} \alpha_{16} = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_{13} + \alpha_{14} + \alpha_{15}, \\ \alpha_{20} = \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8 + \alpha_{17} + \alpha_{18} + \alpha_{19}. \end{cases} \quad (7.9)$$

Нехай

$$\begin{aligned} \kappa_3 = & 1 + x + xz + xyz + (xyzw^2 + xyw) + (xzw^2 + xyzw) = \\ & 1 + x + xz + xyz + xyw + xyzw + xzw^2 + xyzw^2 = \\ & 1 + x + xz + xzy + xyw + xyzw + xzw^2 + xzyw^2 = \\ & 1 + x(1 + z + zy + yw + yzw + zw^2 + zyw^2) \in \mathbb{F}_2(C_2 \times A_4). \end{aligned}$$

Зрозуміло $\sigma(\kappa_3) = \sigma(\kappa_3)^T$. Оскільки x центральний елемент групового кільця, $x^2 = 0$, то

$$\begin{aligned} \kappa_3^2 = & 1 + x^2(1 + z + zy + yw + yzw + zw^2 + zyw^2)^2 = \\ & 1 + ((1 + y + z + zy) + y + yw + yzw + zw^2 + zyw^2)^2. \end{aligned}$$

Крім того,

- $yzw = ywy = wzy = wz$,
- $(1 + y + z + zy)w = w(1 + yz + y + z) = w(1 + y + z + yz)$.

Оскільки $1 + y + z + yz$ центральний елемент групового кільця, $y^2 = z^2 =$

$(yz)^2 = 1$, то

$$\begin{aligned}\kappa_3^2 &= 1 + (1 + y + z + zy)^2 + (y + yw + yzw + zw^2 + zyw^2)^2 = \\ &= y^2 + z^2 + (zy)^2 + (y + yw + yzw + zw^2 + zyw^2)^2 = \\ &= 1 + (y + yw + yzw + zw^2 + zyw^2)^2.\end{aligned}$$

Для групи $A_4 = \langle y, z, w \mid y^2 = z^2 = w^3 = 1, yz = zy, yw = wyz, zw = wy \rangle = \{1, y, z, yz, w, yw, zw, yzw, w^2, yw^2, zw^2, yzw^2\}$ випишемо таблицю Келі.

	1	y	z	yz	w	yw	zw	yzw	w ²	yw ²	zw ²	yzw ²
1	1	y	z	yz	w	yw	zw	yzw	w ²	yw ²	zw ²	yzw ²
y	y	1	yz	z	yw	w	yzw	zw	yw ²	w ²	yzw ²	zw ²
z	z	yz	1	y	zw	yzw	w	yw	zw ²	yzw ²	w ²	yw ²
yz	yz	z	y	1	yzw	zw	yw	w	yzw ²	zw ²	yw ²	w ²
w	w	zw	yzw	yw	w ²	zw ²	yzw ²	yw ²	1	z	yz	y
yw	yw	yzw	zw	w	yw ²	yzw ²	zw ²	w ²	y	yz	z	1
zw	zw	w	yw	yzw	zw ²	w ²	yw ²	yzw ²	z	1	y	yz
yzw	yzw	yw	w	zw	yzw ²	yw ²	w ²	zw ²	yz	y	1	z
w ²	w ²	yzw ²	yw ²	zw ²	1	yz	y	z	w	yzw	yw	zw
yw ²	yw ²	zw ²	w ²	yzw ²	y	z	1	yz	yw	zw	w	yzw
zw ²	zw ²	yw ²	yzw ²	w ²	z	y	yz	1	zw	yw	yzw	w
yzw ²	yzw ²	w ²	zw ²	yw ²	yz	1	z	y	yzw	w	zw	yw

Тоді

$$\begin{aligned}\kappa_3^2 &= 1 + 1 + w + zw + yzw^2 + zw^2 + \\ &+ yzw + yzw^2 + w^2 + z + 1 + \\ &+ yw + yw^2 + zw^2 + 1 + z + \\ &+ yw^2 + y + 1 + yzw + w + \\ &+ w^2 + 1 + y + zw + yw = 0.\end{aligned}$$

Обчисленнями в GAP у додатку В.5 з'ясовано, що розмірність простору його кодових слів 12 а мінімальна відстань 8. Крім того, було показано, що є 2560 елементів

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2 y + \alpha_3 z + \alpha_4 yz + \alpha_5 (w + w^2) + \alpha_6 (yw + yzw^2) + \\ & \alpha_7 (yw^2 + zw) + \alpha_8 (zw^2 + yzw) + \alpha_{13} x + \alpha_{14} xy + \alpha_{15} xz + \alpha_{16} xyz + \\ & \alpha_{17} (xw + xw^2) + \alpha_{18} (xyw + xyzw^2) + \alpha_{19} (xyw^2 + xzw) + \\ & \alpha_{20} (xzw^2 + xyzw), \end{aligned}$$

що задовольняють умови $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$. З них 256 відповідають $[24, 12, 2]$ -коди, 1536 — відповідають $[24, 12, 4]$ -коди, 384 — відповідають $[24, 12, 6]$ -коди і 384 — відповідають $[24, 12, 8]$ -коди.

7.2.6. Група $C_2 \times C_2 \times S_3$. Групу можна задати через твірні елементи та визначальні співвідношення так $G = C_2 \times C_2 \times S_3 = \langle x, y, z, w \mid x^2 = y^2 = z^2 = w^3 = 1, xy = yx, xz = zx, xw = wx, yz = zy, yw = wy, zwz = 1 \rangle$. Можна перевірити таке задання наведеними обчислення в GAP у додатку В.6 а також встановлено однозначне представлення елементів групи у вказаному вигляді

$$\begin{aligned} G = \{ & 1, & z, & z^2, \\ & x, & xz, & xz^2, \\ & y, & yz, & yz^2, \\ & xy, & xyz, & xyz^2, \\ & w, & wz, & wz^2, \\ & wx, & wxz, & wxz^2, \\ & wy, & wyz, & wyz^2, \\ & wxy, & wxyz, & wxyz^2 \} \end{aligned}$$

та визначено порядок їх розташування в групі.

Тоді

$$\sigma(\kappa_1) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & B_1 & B_2 & B_3 & B_4 \\ A_2 & A_1 & A_4 & A_3 & B_2 & B_1 & B_4 & B_3 \\ A_3 & A_4 & A_1 & A_2 & B_3 & B_4 & B_1 & B_2 \\ A_4 & A_3 & A_2 & A_1 & B_4 & B_3 & B_2 & B_1 \\ B_1 & B_2 & B_3 & B_4 & A_1 & A_2 & A_3 & A_4 \\ B_2 & B_1 & B_4 & B_3 & A_2 & A_1 & A_4 & A_3 \\ B_3 & B_4 & B_1 & B_2 & A_3 & A_4 & A_1 & A_2 \\ B_4 & B_3 & B_2 & B_1 & A_4 & A_3 & A_2 & A_1 \end{pmatrix},$$

де $A_1 = circ(\alpha_1, \alpha_2, \alpha_3)$, $A_2 = circ(\alpha_4, \alpha_5, \alpha_6)$, $A_3 = circ(\alpha_7, \alpha_8, \alpha_9)$,

$A_4 = circ(\alpha_{10}, \alpha_{11}, \alpha_{12})$, $B_1 = rcirc(\alpha_{13}, \alpha_{14}, \alpha_{15})$, $B_2 = rcirc(\alpha_{16}, \alpha_{17}, \alpha_{18})$,

$B_3 = rcirc(\alpha_{19}, \alpha_{20}, \alpha_{21})$, $B_4 = rcirc(\alpha_{22}, \alpha_{23}, \alpha_{24})$. Ми шукаємо

розширені бінарні коди Голя з умов:

$$1) \sigma(\alpha) = \sigma(\alpha)^T,$$

$$2) \sigma(\alpha)^2 = 0_{24 \times 24},$$

$$3) Rank(\sigma(\alpha)) = 12,$$

для деяких дільників нуля $\alpha \in \mathbb{F}_2(C_2 \times C_2 \times S_3)$. З умови $\sigma(\kappa_1) = \sigma(\kappa_1)^T$, отримаємо, що $\alpha_3 = \alpha_2$, $\alpha_6 = \alpha_5$, $\alpha_9 = \alpha_8$, $\alpha_{12} = \alpha_{11}$. Умови підтверджуються також обчисленнями в GAP наведеними в додатку В.6. Тепер нехай

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(y + z) + \alpha_4yz + \alpha_5(w + wy) + \alpha_7wz + \alpha_8(w^2 + wyz) + \\ & \alpha_{10}w^2y + \alpha_{11}(w^2z + w^2yz) + \alpha_{13}x + \alpha_{14}xy + \alpha_{15}xz + \alpha_{16}xyz + \\ & \alpha_{17}wx + \alpha_{18}wxy + \alpha_{19}wxz + \alpha_{20}wxyz + \alpha_{21}w^2x + \alpha_{22}w^2xy + \\ & \alpha_{23}w^2xz + \alpha_{24}w^2xyz \in \mathbb{F}_2(C_2 \times C_2 \times S_3), \end{aligned}$$

де $\alpha_i \in \mathbb{F}_2$. Тоді

$$\sigma(\kappa_2)^2 = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & 0 & 0 & 0 & 0 \\ C_2 & C_1 & C_4 & C_3 & 0 & 0 & 0 & 0 \\ C_3 & C_4 & C_1 & C_2 & 0 & 0 & 0 & 0 \\ C_4 & C_3 & C_2 & C_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & C_1 & C_2 & C_3 & C_4 \\ 0 & 0 & 0 & 0 & C_2 & C_1 & C_4 & C_3 \\ 0 & 0 & 0 & 0 & C_3 & C_4 & C_1 & C_2 \\ 0 & 0 & 0 & 0 & C_4 & C_3 & C_2 & C_1 \end{pmatrix},$$

де $C_1 = \text{circ}(\gamma_5, \gamma_4, \gamma_4)$, $C_2 = \text{circ}(0, \gamma_3, \gamma_3)$,

$C_3 = \text{circ}(0, \gamma_2, \gamma_2)$, $C_4 = \text{circ}(0, \gamma_1, \gamma_1)$;

$$\gamma_1 = \alpha_{17}\alpha_{19} + \alpha_{18}\alpha_{19} + \alpha_{16}\alpha_{20} + \alpha_{18}\alpha_{20} + \alpha_{16}\alpha_{21} + \alpha_{17}\alpha_{21} + \alpha_{14}\alpha_{22} + \alpha_{15}\alpha_{22} + \alpha_{13}\alpha_{23} + \alpha_{15}\alpha_{23} + \alpha_{13}\alpha_{24} + \alpha_{14}\alpha_{24},$$

$$\gamma_2 = \alpha_{14}\alpha_{19} + \alpha_{15}\alpha_{19} + \alpha_{13}\alpha_{20} + \alpha_{15}\alpha_{20} + \alpha_{13}\alpha_{21} + \alpha_{14}\alpha_{21} + \alpha_{17}\alpha_{22} + \alpha_{18}\alpha_{22} + \alpha_{16}\alpha_{23} + \alpha_{18}\alpha_{23} + \alpha_{16}\alpha_{24} + \alpha_{17}\alpha_{24},$$

$$\gamma_3 = \alpha_{14}\alpha_{16} + \alpha_{15}\alpha_{16} + \alpha_{13}\alpha_{17} + \alpha_{15}\alpha_{17} + \alpha_{13}\alpha_{18} + \alpha_{14}\alpha_{18} + \alpha_{20}\alpha_{22} + \alpha_{21}\alpha_{22} + \alpha_{19}\alpha_{23} + \alpha_{21}\alpha_{23} + \alpha_{19}\alpha_{24} + \alpha_{20}\alpha_{24},$$

$$\gamma_4 = \alpha_2^2 + \alpha_5^2 + \alpha_8^2 + \alpha_{11}^2 + \alpha_{13}\alpha_{14} + \alpha_{13}\alpha_{15} + \alpha_{14}\alpha_{15} + \alpha_{16}\alpha_{17} + \alpha_{16}\alpha_{18} + \alpha_{17}\alpha_{18} + \alpha_{19}\alpha_{20} + \alpha_{19}\alpha_{21} + \alpha_{20}\alpha_{21} + \alpha_{22}\alpha_{23} + \alpha_{22}\alpha_{24} + \alpha_{23}\alpha_{24},$$

$$\gamma_5 = \alpha_1^2 + \alpha_4^2 + \alpha_7^2 + \alpha_{10}^2 + \alpha_{13}^2 + \alpha_{14}^2 + \alpha_{15}^2 + \alpha_{16}^2 + \alpha_{17}^2 + \alpha_{18}^2 + \alpha_{19}^2 + \alpha_{20}^2 + \alpha_{21}^2 + \alpha_{22}^2 + \alpha_{23}^2 + \alpha_{24}^2.$$

З умови $\sigma(\alpha)^2 = 0_{24 \times 24}$ одержуємо, зокрема, $\gamma_5 = \gamma_4 = 0$. Отже,

$$\begin{aligned} \alpha_{24} &= \alpha_1 + \alpha_4 + \alpha_7 + \alpha_{10} + \alpha_{13} + \alpha_{14} + \alpha_{15} + \alpha_{16} + \alpha_{17} + \alpha_{18} + \\ &\quad \alpha_{19} + \alpha_{20} + \alpha_{21} + \alpha_{22} + \alpha_{23}, \\ \alpha_{11} &= \alpha_2 + \alpha_5 + \alpha_8 + \alpha_{13}\alpha_{14} + \alpha_{13}\alpha_{15} + \alpha_{14}\alpha_{15} + \alpha_{16}\alpha_{17} + \alpha_{16}\alpha_{18} + \\ &\quad \alpha_{17}\alpha_{18} + \alpha_{19}\alpha_{20} + \alpha_{19}\alpha_{21} + \alpha_{20}\alpha_{21} + \alpha_{22}\alpha_{23} + \alpha_{22}\alpha_{24} + \alpha_{23}\alpha_{24} \end{aligned} \quad (7.10)$$

Обчисленнями в GAP у додатку B.6 з'ясовано, що є 48384 елементів

$$\begin{aligned} \kappa_2 = & \alpha_1 + \alpha_2(y + z) + \alpha_4yz + \alpha_5(w + wy) + \alpha_7wz + \alpha_8(w^2 + wyz) + \\ & \alpha_{10}w^2y + \alpha_{11}(w^2z + w^2yz) + \alpha_{13}x + \alpha_{14}xy + \alpha_{15}xz + \alpha_{16}xyz + \\ & \alpha_{17}wx + \alpha_{18}wxy + \alpha_{19}wxz + \alpha_{20}wxyz + \alpha_{21}w^2x + \alpha_{22}w^2xy + \\ & \alpha_{23}w^2xz + \alpha_{24}w^2xyz, \end{aligned}$$

що задовольняють введеним обмеженням (7.10) а також умову $\sigma(\alpha)^2 = 0_{24 \times 24}$ разом з $\text{Rank}(\sigma(\kappa_2)) = 12$. З них 1536 відповідають $[24, 12, 2]$ -коди, 46848 — відповідають $[24, 12, 4]$ -коди і нема жодного якому відповідає $[24, 12, 8]$ -код. Отже, не можна побудувати розширений код Голея з $\mathbb{F}_2(C_2 \times C_2 \times S_3)$ описаним способом.

7.3. Одна конструкція самодуальних кодів

Нехай $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_n}g_n \in RG$. Як і раніше, визначаємо матрицю $\sigma(v) \in M_n(R)$, як

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \quad (7.11)$$

Зауважимо, що елементи $g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}$ є елементами групи G задані в певному порядку. Як і раніше, розглядаємо канонічну інволюцію $*$: $RG \rightarrow RG$, визначену за правилом

$$\left(\sum_{g \in G} a_g g \right)^* = \sum_{g \in G} a_g g^{-1}.$$

Одиниця $v \in V(KG)$, що задовольняє $vv^* = 1$ називається *унітарною*.

Почнемо з технічної леми.

Лема 7.7. Якщо $v = \sum_{i=1}^n \alpha_{g_i} g_i \in$ унітарна одиниця групового кільця RG і $\mu = \sum_{i=1}^n \alpha_{g_i}$, то $\mu^2 = 1$.

Доведення. Як і раніше, розглядаємо поповнююче відображення групового кільця $\varepsilon : RG \rightarrow R$, задане за правилом $\varepsilon(\sum_{i=1}^n \alpha_{g_i} g_i) = \sum_{i=1}^n \alpha_{g_i}$. Нехай $v = \sum_{i=1}^n \alpha_{g_i} g_i$ і $v^* = \sum_{i=1}^n \alpha_{g_i} g_i^{-1}$, тоді $\varepsilon(v) = \varepsilon(v^*) = \sum_{i=1}^n \alpha_{g_i} = \mu$. Тому $\varepsilon(vv^*) = \varepsilon(v)\varepsilon(v^*) = \mu^2 = 1$. $\square$

Нехай $v \in RG$, де R — скінченне фробеніусове кільце характеристики 2, а G — скінченна група порядку n . Визначаємо таку матрицю:

$$M(v) = \left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 & \alpha_2 & \cdots & \alpha_2 \\ \hline \alpha_1 & & & & \alpha_2 & & & \\ \vdots & & E_n & & \vdots & & \sigma(v) & \\ \alpha_1 & & & & \alpha_2 & & & \end{array} \right), \quad (7.12)$$

де $\sigma(v)$ матриця, що відповідає елементу v групового кільця, наведена в (7.11). Для довільного елемента $v \in RG$ визначимо $C(v)$, як лінійний код породжений рядками матриці $M(v)$ над кільцем R . Ми знайдемо достатні умови того, щоб $M(\sigma)$ породжував самодуальний код. Зауважмо, що не всі самодуальні коди будуються таким чином. Оскільки ми не можемо використати властивості рангу матриці над полем для кодів над кільцями, то будемо використовувати одне з понять рангу над кільцем, яке опишемо тут.

Зазвичай ранг вільного скінченно породженого модуля (тут розглядаємо тільки ліві модулі) над довільним кільцем з одиницею R визначається [109, Chapt. II], як мінімальна кількість елементів породжуючої множини. Якщо кільце R скінченне, то довільний вільний модуль над кільцем R рангу n складається з $|R|^n$ елементів. Вільний ранг l системи векторів $v_1, \dots, v_k$ з вільного модуля $R^n = \{(r_1, \dots, r_n) | r_i \in R\}$ рангу n

визначається у випадку, якщо R -модуль породжений $v_1, \dots, v_k$ вільний модуль рангу l , який виділяється прямим доданком у R^n .

Вільний ранг матриці визначається, як вільний ранг системи векторів рядків (чи векторів стовпців). Для матриць над комутативним кільцем R з одиницею ці два поняття рангів збігаються. Зрозуміло, що вільний ранг матриці над комутативним кільцем з одиницею не міняється, якщо над її рядками (те ж стосується стовпців) проводити елементарні перетворення 3 типів:

- 1) заміна двох рядків місцями,
- 2) додавання до деякого рядка іншого рядка домноженого на елемент кільця R ,
- 3) домноження деякого рядка на оборотній елемент кільця R .

Вільний ранг матриці також не зміниться при домноження зліва (те ж стосується домноження зправа) на оборотну матрицю відповідного розміру над кільцем R . Обчислення рангу дозволяє з'ясувати, коли самоортогональний код C_v є самодуальним.

Теорема 7.8. *Нехай R скінченне комутативне фробеніусове кільце характеристики 2 і $G = \{g_1, g_2, \dots, g_n\}$ скінченна група порядку n , $(\gamma_1 + \gamma_2)^2 + n(\alpha_1 + \alpha_2)^2 = 0$, $vv^* = 1 + (\alpha_1 + \alpha_2)^2 \hat{g}$ і $(\gamma_1 + 1)\alpha_1 + (\gamma_2 + \mu)\alpha_2 = 0$, де $\hat{g} = \sum_{i=1}^n g_i$ і $\mu = \sum_{i=1}^n \alpha_{g_i}$, то Код $C(v)$ породжений рядками матриці 7.12 є самодуальним кодом довжини $2n + 2$ тоді і тільки тоді, коли $(\gamma_1 + n\alpha_1^2, \gamma_2 + n\alpha_2^2, \mu\alpha_1 + \alpha_2)$ має вільний ранг 1.*

Доведення. Оскільки $(\gamma_1 + \gamma_2)^2 + n(\alpha_1 + \alpha_2)^2 = 0$, $vv^* = 1 + (\alpha_1 + \alpha_2)^2 \hat{g}$, $(\gamma_1 + 1)\alpha_1 + (\gamma_2 + \mu)\alpha_2 = 0$, то за теоремою 1.31 код C_v є самоортогональним.

Зрозуміло $\mu = \sum_{i=1}^n \alpha_{g_i^{-1}g_k} = \sum_{j=1}^n \alpha_{g_k^{-1}g_j}$ для довільного $k \in \{1, \dots, n\}$.

Крім того,

$$\text{rank}(M(\sigma)) = \text{rank} \left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 & \alpha_2 & \cdots & \alpha_2 \\ \hline \alpha_1 & & & & \alpha_2 & & & \\ \vdots & & & & \vdots & & & \\ \alpha_1 & & & & \alpha_2 & & & \end{array} \right) =$$

$$\text{rank} \left(\begin{array}{c|ccc|c|ccc} \gamma_1 + n\alpha_1^2 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 + n\alpha_2^2 & \alpha_2 & \cdots & \alpha_2 \\ \hline 0 & & & & 0 & & & \\ \vdots & & & & \vdots & & & \\ 0 & & & & 0 & & & \end{array} \right) =$$

$$\text{rank} \left[\left(\begin{array}{c|ccc|c|ccc} \gamma_1 + n\alpha_1^2 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 + n\alpha_2^2 & \alpha_2 & \cdots & \alpha_2 \\ \hline 0 & & & & 0 & & & \\ \vdots & & & & \vdots & & & \\ 0 & & & & 0 & & & \end{array} \right) \times \begin{pmatrix} E_n & 0 & 0 & 0 \\ 0 & E_n & 0 & \sigma(v) \\ 0 & 0 & E_n & 0 \\ 0 & 0 & 0 & E_n \end{pmatrix} \right] =$$

$$\text{rank} \left(\begin{array}{c|ccc|c|ccc} \gamma_1 + n\alpha_1^2 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 + n\alpha_2^2 & \mu\alpha_1 + \alpha_2 & \cdots & \mu\alpha_1 + \alpha_2 \\ \hline 0 & & & & 0 & & & \\ \vdots & & & & \vdots & & & \\ 0 & & & & 0 & & & \end{array} \right) =$$

$$\text{rank} \left(\begin{array}{c|ccc|c|ccc} \gamma_1 + n\alpha_1^2 & 0 & \cdots & 0 & \gamma_2 + n\alpha_2^2 & \mu\alpha_1 + \alpha_2 & \cdots & \mu\alpha_1 + \alpha_2 \\ \hline 0 & & & & 0 & & & \\ \vdots & & E_n & & \vdots & & 0 & \\ \hline 0 & & & & 0 & & & \end{array} \right).$$

Зрозуміло код C_v буде самодуальним тоді і тільки тоді, коли $|C_v| = |R|^n - 1$, тобто $M(v)$ матиме вільний ранг $n+1$ або $(\gamma_1 + n\alpha_1^2, \gamma_2 + n\alpha_2^2, \mu\alpha_1 + \alpha_2)$ має вільний ранг 1. $\square$

Наслідок 7.9. Нехай R — скінченне комутативне фробеніусове кільце характеристики 2 і G — скінченна група порядку n . Нехай v — унітарна одиниця групового кільця RG , $(\alpha_1 + \alpha_2)^2 = 0$, $(\gamma_1 + \gamma_2)^2 = 0$ і $(\gamma_1 + 1)\alpha_1 + (\gamma_2 + \mu)\alpha_2 = 0$, де $\mu = \sum_{i=1}^n \alpha_{g_i}$. Тоді код $C(v)$ самоортогональний код довжини $2n + 2$. Код $C(v)$ є самодуальним тоді і тільки тоді, коли $\gamma_1 + n\alpha_1^2 \in R^*$.

Доведення. Для доведення покажемо, що задовольняються умови теореми 7.8. Оскільки $(\alpha_1 + \alpha_2)^2 = 0$ і $(\gamma_1 + \gamma_2)^2 = 0$, то $(\gamma_1 + \gamma_2)^2 + n(\alpha_1 + \alpha_2)^2 = 0 + n \cdot 0 = 0$. Оскільки v унітарна одиниця, то $vv^* = 1$ і $vv^* = 1 = 1 + 0\hat{g} = 1 + (\alpha_1 + \alpha_2)^2\hat{g}$. Отже, умови теореми 7.8 виконуються і код $C(v)$ самоортогональний код довжини $2n + 2$. За теоремою 7.8 Код $C(v)$ є самодуальним тоді і тільки тоді, коли $(\gamma_1 + n\alpha_1^2, \gamma_2 + n\alpha_2^2, \mu\alpha_1 + \alpha_2)$ має вільний ранг 1. Тобто, коли

$$R = (\gamma_1 + n\alpha_1^2)R + (\gamma_2 + n\alpha_2^2)R + (\mu\alpha_1 + \alpha_2)R.$$

Або, що одне і те ж,

$$1 \in (\gamma_1 + n\alpha_1^2)R + (\gamma_2 + n\alpha_2^2)R + (\mu\alpha_1 + \alpha_2)R$$

чи

$$1 \in (\gamma_1 + n\alpha_1^2)^2 R + (\gamma_2 + n\alpha_2^2)^2 R + (\mu\alpha_1 + \alpha_2)^2 R$$

або

$$1 \in (\gamma_1^2 + n^2\alpha_1^4)R + (\gamma_2^2 + n\alpha_2^2)R + (\mu^2\alpha_1^2 + \alpha_2^2)R.$$

За лемою 7.7 маємо $\mu^2 = 1$. Крім того, $\alpha_1^2 = \alpha_2^2$ і $\gamma_1^2 = \gamma_2^2$. Тому код $C(v)$ є самодуальним тоді і тільки тоді, коли

$$1 \in (\gamma_1^2 + n^2\alpha_1^4)R + (\gamma_1^2 + n\alpha_1^2)R + (\alpha_1^2 + \alpha_1^2)R,$$

чи

$$1 \in (\gamma_1^2 + n^2\alpha_1^4)R$$

або

$$\gamma_1^2 + n^2\alpha_1^4 \in R^*.$$

Отже, код $C(v)$ є самодуальним тоді і тільки тоді, коли $\gamma_1 + n\alpha_1^2 \in R^*$. $\square$

Розроблена конструкція коду була використана [142] для побудови самодуальних кодів над полем $\mathbb{F}_2$ з двох елементів та комутативним локальним кільцем $\mathbb{F}_2 + u\mathbb{F}_2$ довжини 2 ($u^2 = 0$) з чотирьох елементів для груп порядків 9, 15, 21, 25, 27, 33 та 35. Було знайдено екстремальні бінарні самодуальні коди довжини 20, 32, 40, 44, 52, 56, 64, 68, 88 і добре відомі бінарні самодуальні коди довжини 72.

7.4. Висновки до розділу

У цьому розділі засобами теорії зображень розглядаються властивості одиниць скінченного порядку, унітарних одиниці та деякі дільників нуля групових кілець скінченних груп. Ці ж елементи застосовуються для побудови сумодуальних кодів над комутативними фробеніусовими кільцями. Було побудовано низку бінарних самодуальних кодів, багато з яких є екстремальними.

В підрозділі 7.1 методом Лутара — Пасі встановлено, що в цілочисловому груповому кільці скінченної групи $PSL(3, 4)$ показника 420, який має 23 нетривіальні дільники, можуть бути тільки нетривіальні одиниці порядку: 2, 3, 4, 5, 7 і 6 (відомо, що порядок розглядуваних одиниць завжди ділить показника 420), а для елементів порядку 2 та 3 виконується гіпотеза Цассенхауза.

В підрозділі 7.2 та 7.3 будуються самодуальні коди з використанням групових кілець. Зокрема, у підрозділі 7.2 розглянуто один метод побудови розширених бінарних кодів Галея за груповим алгебрами групи 24-го порядку. Встановлено, що з 15 відомих неізоморфних груп 24-го порядку, крім груп D_{24} , S_4 , для яких коди будувались раніше, таким способом можна побудувати код тільки для груп $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$. В підрозділі 7.3 відома конструкція коду, що використовувала дію регулярного зображення на певних елементах групового кільця, як частини матриці, рядки якої породжують лінійний код, була поширена для побудови нових самодуальних кодів над полем з двох елементів та над деякими скінченними комутативними фробеніусовими кільцями.

Результати цього розділу опубліковані в роботах [140, 142, 143, 149].

ВИСНОВКИ

Дисертаційна робота присвячена продовженню деяких природних напрямків досліджень зображень скінченних груп над комутативними кільцями та супутнім питанням. Тематика, представлена в роботі, має дуже довгу та багату історію, яка налічує вже понад 130 років і знайшла численні застосування, як у алгебрі, так далеко за її межами. У роботі, розширюються відомі властивості зображень скінченних груп над комутативними кільцями, що пов'язані в першу чергу з їх звідністю та розкладністю. Основними новими науковими результатами дисертації є наступні:

- Встановлено критерій скінченності множина нееквівалентних незвідних матричних зображень наперед заданого степеня скінченної p -групи над комутативним нетеровим локальним кільцем характеристики p^s ($s > 0$), яке не є напівпервісним, з нескінченним полем лишків.
- Показано нескінченність числа всіх нееквівалентних незвідних матричних зображень наперед заданого степеня $n > 1$ скінченної p -групи G порядку $|G| > 2$ над комутативним нетеровим локальним напівпервісним нецілісним кільцем характеристики p , з нескінченним полем лишків.
- Описано всі, з точністю до еквівалентності, матричні зображення 2-го степеня групи діедра порядку $2p$ (p — непарне просте число) над комутативними локальними кільцями довжини 2 характеристики 2, та з'ясовано критерій їх незвідності.
- Встановлено достатні умови спадкової звідності t -циклічних та бімономіальних матриць над комутативним кільцем.

- Побудовано серії нерозкладних та спадково незвідних унімономіальних зображень циклічної p -групи над скінченним комутативним локальним кільцем скінченної довжини характеристики p , та оцінене число побудованих зображень заданого степеня з певною точністю для кожної групи та кільця окремо.
- Показано, що всі максимальні уніпотентні підгрупи повної лінійної групи та спеціальної лінійної групи над кільцем K попарно спряжені, якщо фактор-кільце кільця K за первісним радикалом є скінченною прямою сумою кілець Безу.
- Показано дикийсть за модулем радикалу Джекобсона задачі про описання, з точністю до еквівалентності за модулем головного ідеалу породженого будь-яким елементом довжини більше 2, матриць над локальним факторіальним кільцем, що не є областю головних ідеалів.
- Встановлено, що в цілочисловому груповому кільці скінченної групи $PSL(3, 4)$ виконується гіпотеза Цассенхауза для елементів порядку 2 та 3.
- Вперше побудовано розширені бінарні коди Галея за груповим кільцем груп $(C_6 \times C_2) \rtimes C_2$, $C_3 \times D_8$, $C_2 \times A_4$ порядку 24 над полем з двох елементів, та підраховано їх кількість.

Дисертаційна робота має переважно теоретичний характер, що є внеском у актуальну задачу класифікації зображень скінченних груп над комутативними кільцями з точністю до еквівалентності. Розроблені методи застосовувалися в прилеглих теоріях лінійних груп, матриць, групових кілець та кодів над комутативними кільцями. Зокрема, застосування в останній сфері носить практичну спрямованість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Артамонов В. А., Бовди А. А. Целочисленные групповые кольца: Группа обратимых элементов и классическая K -теория. *Итоги науки и техники. Алгебра. Топология. Геометрия*. 1989. Т. 27. С. 3–43.
2. Башев В. А. Представления группы $Z_2 \times Z_2$ в поле характеристики 2. *Докл. АН СССР*. 1961. Т. 141, № 5. С. 1015–1018.
3. Берман С. Д., Гудивок П. М. Неразложимые представления конечных групп над кольцом целых p -адических чисел. *Изв. АН СССР. Серия математика* 1964. Т. 28, № 4. С. 875–910.
4. Берман С. Д., Гудивок П. М. О целочисленных представлениях конечных групп. *Докл. и сообщ. Ужгород. ун-та. Серия физ.-мат. наук* 1962. № 5. С. 74–76.
5. Берман С. Д., Гудивок П. М. Целочисленные представления конечных групп. *Докл. АН СССР*. 1962. Т. 145, № 6. С. 1199–1201
6. Берман С. Д. К теории групповых кодов. *Кибернетика*. 1967. № 1. С. 31–39.
7. Берман С. Д. Об уравнении $x^m = 1$ в целочисленном групповом кольце. *Укр. мат. журн.* 1955. Т. 7, № 3. С. 257–261.
8. Берман С. Д. Представления конечных групп над произвольным полем и над кольцом целых чисел. *Изв. АН СССР. Серия математика* 1966. Т. 30, № 1. С. 69–132.
9. Берман С. Д. Целочисленные представления циклической группы, имеющие две неприводимые рациональные компоненты. *Памяти Н.*

- Г. Чеботарева (1984–1947)*. Казань : Из-во Казанского ун-та, 1964. С. 18–29.
10. Берман С. Д. Число неприводимых представлений конечной группы над произвольным полем. *Докл. АН СССР*. 1956. Т. 106, № 5. С. 767–769.
 11. Бондаренко В. М., Бортош М. Ю. Нерозкладні та ізоморфні об'єкти в категорії мономіальних матриць над локальним кільцем. *Укр. мат. журн.* 2017. Т. 69, № 7. С. 889–904.
 12. Бондаренко В. М., Дрозд Ю. А. Представленческий тип конечных групп. *Модули и представления: Записки науч. семинаров ЛОМИ*. 1977. Вып. 71. С. 24–41.
 13. Бондаренко В. М. О подобии матриц над кольцом классов вычетов. *Матем. сборник*. Киев. : «Наукова думка», 1976. С. 275–277.
 14. Бондаренко В. М. Представления диэдральных групп над полем характеристики 2. *Мат. сб.* 1975. Вып. 96, № 1. С. 63–74.
 15. Борович З. И., Фадеев Д. К. Теория гомологий в группах. II. *Вестник Ленингр. гос. ун-та. Серия математика, механика и астрономия* 1959. № 7. С. 72–87.
 16. Бортош М. Ю. Лінійно-алгебраїчні властивості категорій мономіальних матриць над локальними кільцями: дис. . . . канд. фіз.-мат. наук: 01.01.06 / НАН України, Ін-т математики., Київ., 2017. 179 с.
 17. Бортош М. Ю., Тилищак О. А. Приводимость некоторых мономиальных матриц над коммутативными локальными кольцами. *На-*

уковий часопис НПУ ім. М. П. Драгоманова. Серія 1. Фіз.-мат. науки. Київ. : НПУ ім. М. П. Драгоманова. 2013. № 14. С. 68–78.

18. Вальвачев Р. Т. p -подгруппы Силова полной линейной группы. *Изв. АН СССР. Серия математика* 1963. Вып. 27, № 5. С. 1031–1054.
19. Ващук Ф. Г., Гудивок П. М. Целочисленные p -адические представления конечных абелевых p -групп. *Доп. АН УССР. Серия А.* 1986. № 1. С. 3–6.
20. Газарян Т. Г. Подобие инволютивных матриц над локальным кольцом характеристики $2k$. *Дискрет. математика.* 1995. Vol. 7, No 4. Р. 145–156.
21. Гантмахер Ф. Р. Теория матриц : учебное пособие. Москва : Наука, 2010. 560 с.
22. Гудивок П. М., Дроботенко В. С., Лихтман А. И. О представлениях конечных групп над кольцом классов вычетов по модулю m . *Укр. мат. журн.* 1964. Т. 16, № 1. С. 81–89.
23. Гудивок П. М., Кіндюх С. П. Про дикі скінченні 2-групи над локальними областями цілісності характеристики нуль. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики.* 2009. Вип. 18. С. 54–61.
24. Гудивок П. М., Кіндюх С. П. Про матричні зображення скінченних 2-груп над локальними областями цілісності характеристики нуль. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики.* 2006. Вип. 12–13. С. 59–64.

25. Гудивок П. М. Несколько замечаний о целочисленных представлениях конечных групп. *Укр. мат. журн.* 1974. Т. 26, № 4. С. 539–545.
26. Гудивок П. М. Об эквивалентности матриц над коммутативными кольцами. *Бесконечные группы и примыкающие алгебраические структуры*. Киев. : Ин-т математики НАН Украины, 1993. С. 431–437.
27. Гудивок П. М. О модулярных и целочисленных представлениях конечных групп. *Докл. АН СССР*. 1974. Т. 214, № 5. С. 993–996.
28. Гудивок П. М. О модулярных представления конечных групп *Докл. и сообщ. Ужгород. ун-та. Серия физ.-мат. наук* 1961. № 4. С. 86–87.
29. Гудивок П. М. О силовских p -подгруппах полной линейной группы над кольцом целых чисел. *Алгебра и анализ*. 1990. Вып. 2, № 6. С. 121–128.
30. Гудивок П. М. О силовских подгруппах полной линейной группы над полными дискретно нормированными кольцами. *Укр. мат. журн.* 1991. Т. 43, № 7–8. С. 918–924.
31. Гудивок П. М., Погориляк В. И. О неразложимых представлениях конечных p -групп над коммутативными локальными кольцами. *Доп. НАН України*. 1996, № 5. С. 7–11.
32. Гудивок П. М., Погориляк В. И. Матричные представления конечных p -групп над коммутативными локальными кольцами характеристики p^s . *Укр. мат. журн.* 2002. Т. 54, № 8. С. 1150–1156.

33. Гудивок П. М., Погориляк Е. Я. О модулярных представлениях конечных групп над областями целостности. *Труды мат. ин-та АН СССР*. 1990. Вып. 183. С. 78–86.
34. Гудивок П. М., Погориляк Е. Я. О теореме Крулля – Шмидта для представлений групп над кольцом P -целых чисел. *Мат. заметки*. 1970. Т. 7, № 1. С. 125–135.
35. Гудивок П. М., Погоріляк В. Й. Зображення скінченних p -груп над локальними кільцями додатньої характеристики. *Доп. АН УРСР. Серія А*. 1989, № 2, С. 5–8.
36. Гудивок П. М., Погоріляк В. Й. О неразложимых матричных представлениях конечных p -групп над коммутативными локальными кольцами характеристики p^s . *Наук. вісник Ужгород. ун-ту. Серія математика* 1999. Вип. 4. С. 43–46.
37. Гудивок П. М. Представления конечных групп над коммутативными локальными кольцами : монография. Ужгород : Ужгород. нац. ун-т, 2003. 118 с.
38. Гудивок П. М. Про обмеженість степенів нерозкладних модулярних зображень скінченних груп над кільцями головних ідеалів. *Доп. АН УРСР. Серія А*. 1971. № 8. С. 683–685.
39. Гудивок П. М., Рудько В. П. Об изоморфизме силовских p -подгрупп полной линейной группы над кольцом целых чисел. *Доп. НАН України*. 1992. № 9. С. 3–5.
40. Гудивок П. М., Рудько В. П. О силовских подгруппах полной линейной группы над областями целостности. *Доп. НАН України*. 1995. № 8. С. 5–7.

41. Гудивок П. М., Рудько В. П. Про p -адичні цілочислові зображення циклічної p -групи. *Доп. АН УРСР. Серія А*. 1966. № 9. С. 1111–1113.
42. Гудивок П. М., Сигетій І. П., Чухрай І. Б. Про число матричних зображень даного степеня скінченної p -групи над деякими комутативними кільцями характеристики p^s . *Наук. вісник Ужгород. ун-ту. Серія математика* 1999. Вип. 4. С. 47–53.
43. Гудивок П. М. Силовские p -подгруппы полной линейной группы над дискретно нормированными кольцами. *Доп. АН УРСР. Серія А*. 1979. № 5. С. 326–329.
44. Гудивок П. М., Тилищак О. А. Про незвідні модулярні зображення скінченних p -груп над комутативними локальними кільцями. *Наук. вісник Ужгород. ун-ту. Серія математика*. 1998. Вип. 3. С. 78–83.
45. Гудивок П. М., Шапочка І. В. О черниковских p -группах. *Укр. мат. журн.* 1999. Т. 51, № 3. С. 291–304.
46. Гудивок П. М., Чухрай І. Б. Про число нерозкладних матричних зображень даного степеня скінченної p -групи над комутативними локальними кільцями характеристики p^s . *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2000. Вип. 5. С. 33–40.
47. Динис Р. Ф., Тилищак О. А. Про еквівалентність матриць деякого вигляду над локальними областями головних ідеалів. *Десята наукова відкрита конф. інституту прикладної математики та фундаментальних наук ІМФН* : зб. матеріалів та програма конф. [«PSC-IMFS-10»] (Львів, 17–18 травня 2012 р.). Львів : Видавництво Львівської політехніки, 2012. С. А31.

48. Динис Р., Тилищак О. Про звідність деяких мономіальних матриць над комутативними кільцями. *Вісник Київ. нац. ун-ту ім. Т. Шевченка. Серія: математики і механіки*. 2014. Вип. 2 (32). С. 20–23.
49. Динис Р. Ф., Тилищак О. А. Про звідність матриць деякого вигляду над комутативними локальними кільцями головних ідеалів. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2012. Вип. 23, № 1. С. 57–62.
50. Динис Р. Ф., Тилищак О. А., Юрченко Н. В. Про нерозкладність мономіальних матриць спеціального вигляду над локальними кільцями. *Міжнар. мат. конф. «Методика викладання та методи досліджень в математиці»* : матеріали конф., Берегове, 21–23 квітня 2016. Ужгород : ТОВ «РІК-У», 2016. С. 28.
51. Дроботенко В. С., Дроботенко Э. С., Жилинская З. П., Погориляк Е. Я. Представления циклической группы простого порядка p над кольцом классов вычетов по модулю p^s . *Укр. мат. журн.* 1965. Т. 17, № 5. С. 28–42.
52. Дроботенко В. С., Рудько В. П. Зображення циклічної групи групами автоморфізмів деякого класу модулів. *Доп. АН УССР*. 1968. С. 302–304.
53. Дрозд Ю. А. О ручных и диких матричных задачах. *Матричные задачи*. Киев: Ин-т математики АН УССР, 1977. С. 104–114.
54. Залесский А. Е. Силовские p -подгруппы полной линейной группы над телом. *Изв. АН СССР. Серия математика* 1967. Т. 31, № 5. С. 1149–1158.

55. Залесский А. Е., Конюх В. С. P -подгруппы Силова классических групп. *Матем. сб.* 1976. Вып. 101, № 2. С. 231–251.
56. Зарисский О., Самюэль П. Коммутативная алгебра : монография : в 2 т. Москва : ИЛ, 1963. Т. 1. 378 с.
57. Иванов Е. Н. Теория групп и ее применения в физике : уч. пособие. Москва : МИЭТ, 2006. 160 с.
58. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп : монография. 2-е изд. Москва : Наука, 1977. 240 с.
59. Конюх В. С. О линейных p -группах. *Изв. АН БССР. Серия физ.-мат. наук* 1987. № 1. С. 3–8.
60. Кругляк С. А. О представлениях группы (p, p) над полем характеристики p . *Докл. АН СССР*. 1963. Т. 153, № 6. С. 1263–1265.
61. Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр : монография. Москва : Наука, 1969. 668 с.
62. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки : монография. Москва : Связь, 1974. 744 с.
63. Мальцев А. И. О некоторых классах бесконечных разрешимых групп. *Мат. сб.* 1951. Вып. 28, № 3. С. 567–588.
64. Назарова Л. А. Целочисленные представления четверной группы. *Докл. АН СССР*. 1961. Т. 140, № 5. С. 1101–1014.
65. Нечаев А. А. О подобии матриц над коммутативным локальным артиновым кольцом. *Труды сем. им. И. Г. Петровского*. 1983. Вып. 9. С. 81–101.

66. Орос Віктор Михайлович. Про зображення скінченних p -груп над деякими факторіальними кільцями : Дис. ... канд. фіз.-мат. наук : 01.01.06 / НАН України, Ін-т математики., Київ., 1993. 54 с.
67. Петечук В. М. О триангулируемости некоторых унепотентных матричных групп над телами. *Известия АН БССР. Серия физ.-тех. н.* 1987. № 6. С. 44–46.
68. Петричкович В. М. Узагальнена еквівалентність матриць і їх наборів та факторизація матриць над кільцями : монографія. Львів : Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України, 2015. 312 с.
69. Пецык А. Л. О силовских p -подгруппах групп $SL_n(K)$ и $PSL_n(K)$. Москва, 1981. 14 с. Деп.: ВИНТИ, № 1182–81.
70. Платонов В. П. Теория алгебраических линейных групп и периодические группы. *Изв. АН СССР. Серия математика* 1966. Вып. 30. С. 573–620.
71. Ройтер А. В. О представлениях циклической группы четвертого порядка целочисленными матрицами. *Вестн. Ленингр. ун-та.* 1960. № 19. С. 65–74.
72. Сидоров С. В. О подобии матриц третьего порядка над кольцом целых чисел, имеющих приводимый характеристический многочлен. *Вест. Нижегородского ун-та им. Н. И. Лобачевского. Серия мат. моделирование. Опт. управление.* 2009, № 1. С. 119–127.
73. Стойка М. В. Матричні зображення груп та схрещених групових кілець над локальними комутативними кільцями: дис. ... канд. фіз.-мат. наук: 01.01.06 / Ужг. нац. ун-т., Ужгород, 2015. 143 с.

74. Супруненко Д. А. Группы матриц : монография. Москва : Наука, 1972. 352 с.
75. Супруненко Д. А. Линейные p -группы. *Докл. АН БССР*. 1960. Т. 4, № 6. С. 233–235.
76. Тавгенъ О. И., Синьсун Я. Унипотентность образа представления $F_2(x, y)$ в $GL(6, C)$ при условии отображения примитивных элементов в унипотентные матрицы. *Вестн. БГУ. Серия 1*. 2010. № 2. С. 114–119.
77. Тилищак О. А. Зображення 2-го степеня групи дієдра порядку $2p$ над деякими комутативними локальними кільцями. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2008. Вип. 16. С. 188–192.
78. Тилищак О. А. Про максимальні уніпотентні підгрупи спеціальної лінійної групи над комутативним кільцем. *Укр. мат. журн.* 2019. Т. 71, № 8. С. 1150–1156.
79. Тилищак О. А. Про модулярні зображення циклічної 2-групи над локальною областю цілісності. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2005. Вип. 10–11. С. 135–139.
80. Тилищак О. А. Про незвідні зображення скінченних p -груп над деякими локальними кільцями характеристики p . *Наук. вісник Ужгород. ун-ту. Серія математика* 1999. Вип. 4. С. 104–110.
81. Тилищак О. А. Про незвідні модулярні зображення 2-групи даного степеня над напівпервісним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2004. Вип. 9. С. 103–106.

82. Тилищак О. А. Про незвідні модулярні зображення даного степеня скінченної p -групи над комутативним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2002. Вип. 7. С. 108–114.
83. Тилищак О. А. Про незвідні модулярні зображення даного степеня скінченної p -групи над напівпервісним комутативним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2003. Вип. 8. С. 156–159.
84. Тилищак О. А. Про незвідність мономіальних матриць 7-го порядку над локальними кільцями. *Вісник Київ. нац. ун-ту ім. Т. Шевченка. Серія: фіз.-мат. науки*. 2018. Вип. № 3. С. 37–44.
85. Тилищак О. А. Про силовські p -підгрупи повної лінійної групи над комутативним локальним кільцем характеристики p^s . *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2000. Вип. 5. С. 95–102.
86. Тилищак О. А. Про силовські p -підгрупи спеціальної лінійної групи над комутативним кільцем характеристики p^s . *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2001. Вип. 6. С. 140–142.
87. Тилищак О. А. Про спадково незвідні унімономіальні зображення циклічних p -груп над локальними кільцями характеристики p . *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2019. Вип. № 1 (34). С. 52–59.

88. Тилищак О. А. Про число нерозкладних модулярних зображень циклічної p -групи над локальним кільцем скінченної довжини. *Мат. методи та фіз.-мех. поля*. 2019. Вип. 62, № 1. С. 74–82.
89. Тилищак О. А. Про число нерозкладних модулярних зображень циклічної p -групи над скінченим локальним кільцем. *Прикл. проблеми механіки і математики*. 2018. Вип. 16. С. 19–29.
90. Тилищак О. А., Юрченко Н. В., Цімболинець Р. Ф. Нерозкладність однієї матриці довільного порядку над локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2016. Вип. № 1 (28). С. 137–141.
91. Тилищак О. Деякі нерозкладні модулярні зображення циклічної p -групи над локальним кільцем скінченної довжини. *Між-нар. наукова конф. «Сучасні проблеми механіки та математики» : збірник наукових праць : у 3-х т. / за заг. ред. А. М. Самойленка та Р. М. Кушніра [Електронний ресурс] (Львів, 22–25 травня 2018). Львів, 2018. Т. 3. С. 237. URL: http://www.iapmm.lviv.ua/mpmm2018/Volume_3.pdf (дата звернення 28.03.2020).*
92. Федоров Е. С. Симметрия и структура кристаллов : монография. Москва : Издат. АН СССР, 1949. 632 с.
93. Цімболинець Р. Ф. Бімономіальні матриці над комутативними кільцями: дис. ... канд. фіз.-мат. наук: 01.01.06 / Київ. нац. ун-т ім. Т. Шевченка, Київ, 2018. 176 с.

94. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел. *Известия вузов. Серия математика*. 2006. № 4. С. 57–64.
95. Щедрик В. П. Факторизація матриць над кільцями елементарних дільників : монографія. Львів : Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України, 2017. 304 с.
96. Яковлев А. В. Классификация 2-адических представлений циклической группы восьмого порядка. *Зап. научн. сем. ЛОМИ*. 1972. Вып. 28. С. 93–129.
97. Guralnick R. M. Similarity of matrices over commutative rings. *Linear Algebra Appl.* 1991. Vol. 157. P. 55–68.
98. Höfert C., Kimmerle W. On torsion units of integral group rings of groups of small order. *Groups, Rings and Group Rings* : Proceedings of the conference, Ubatuba, Brazil, July 26–31, 2004. In honor of the 60th birthday of Prof. César Polcino Milies. Boca Raton : Chapman & Hall/CRC, 2006.
99. Avni N., Onn U., Prasad A., Vaserstein L. Similarity classes of 3×3 matrices over a local principal ideal ring. *Comm. Algebra*. 2009. Vol. 37, No 8. P. 2601–2615.
100. Azumay G. Corrections and supplementaries to my paper concerning Krull – Remak – Schidt’s theorem. *Nagoya Math. J.* 1950. Vol. 1. P. 117–124.
101. Berlekamp E. R. Key Papers in the Development of Coding Theory : monograph. New York : I.E.E.E. Press, 1974.

102. Bernhardt F. Landrock P., Manz O. The extended Golay codes considered as ideals. *J. Combin. Theory. Series A*. 1990. Vol. 55, No 2. P. 235–246.
103. Bondarenko V., Dinis R., Tylyshchak A. On irreducibility of some matrices over p -adic integers. *Fifth International Conference on Analytic Number Theory and Spatial Tessellations* : abstracts, Kiev, September 16–20, 2013. Kyiv : Institute of Mathematics of NAS of Ukraine, 2013. P. 6.
104. Bondarenko V., Gildea J., Salim M., Tylyshchak A. On the number of indecomposable representations of given degree of a cyclic group over local rings of finite length. *The Second International Conference on Groups, Group Rings and Related Topics* : abstracts [electronic resource], Khorfakkan (UAE), November 19–22, 2017. Khorfakkan (UAE), 2017. P. 10. URL: https://conferences.uaeu.ac.ae/ggrt2017/en/abstracts_ggrt.pdf (date of appeal: 28.03.2020).
105. Bondarenko V. M., Bortos M. Yu., Dinis R. F., Tylyshchak A. A. Indecomposable and irreducible t -monomial matrices over commutative rings. *Algebra and Discrete Math*. 2016. Vol. 22, No 1. P. 11–20.
106. Bondarenko V. M., Bortos M. Yu., Dinis R. F., Tylyshchak A. A. Reducibility and Irreducibility of Monomial Matrices over Commutative Rings. *Algebra Discret Math*. 2013. Vol. 16, No 2. P. 171–187.
107. Bondarenko V. M., Gildea J., Tylyshchak A. A., Yurchenko N. V. On hereditary reducibility of 2-monomial matrices over commutative rings. *Algebra and Discrete Math*. 2019. Vol. 27, No 1. P. 1–11.

- 108. Bondarenko V. M., Tylyshchak A. A., Stoika M. V. On the equivalence of matrices over commutative rings modulo ideals. *Algebra and Discrete Math.* 2014. Vol. 17, No 1. P. 12–19.
- 109. Bourbaki N. Elements of mathematics. Algebra: Algebraic structures, Linear algebra, I : monograph. Edinburgh : Addison-Wesley, 1974. 710 p.
- 110. Bovdi V., Grishkov A., Konovalov A. Kimmerle conjecture for the Held and O’Nan sporadic simple groups. *Sci. Math. Jpn.* 2009. Vol. 69, No 3. P. 353–361.
- 111. Bovdi V., Höfert C., Kimmerle W. On the first Zassenhaus conjecture for integral group rings. *Publ. Math. Debrecen.* 2004. Vol. 65, No 3–4. P. 291–303.
- 112. Bovdi V., Hertweck M. Zassenhaus conjecture for central extensions of S_5 . *J. Group Theory.* 2008. Vol. 11, No 1. P. 63–74.
- 113. Bovdi V., Jespers E., Konovalov A. B. Torsion units in integral group rings of Janko simple groups. *Math. Comp.* 2011. Vol. 80, No 273. P. 593–615.
- 114. Bovdi V., Konovalov, A. B. Integral group ring of Rudvalis simple group. *Ukrainian Math. J.* 2009. Vol. 61, No 1. P. 1–13.
- 115. Bovdi V., Konovalov A. B. Integral group ring of the first Mathieu simple group. *London Math. Soc. Lecture Note Ser.* Cambridge : Cambridge Univ. Press, 2007. Vol. 339, P. 237–245.
- 116. Bovdi V., Konovalov A. B. Integral group ring of the Mathieu simple group M_{23} . *Comm. Algebra.* 2008. Vol. 36, No 7. P. 2670–2680.

117. Bovdi V., Konovalov A. B. Integral group ring of the Mathieu simple group M_{24} . *J. Algebra Appl.* 2012. Vol. 11, No 1. P. 1250016, 10.
118. Bovdi V., Konovalov, A. B. Integral group ring of the McLaughlin simple group. *Algebra and Discrete Math.* 2007. No 2. P. 43–53.
119. Bovdi V., Konovalov A. B., Linton, S. Torsion units in integral group rings of Conway simple groups. *Internat. J. Algebra Comput.* 2011. Vol. 21, No 4. P. 615–634.
120. Bovdi V., Konovalov A. B., Linton S. Torsion units in integral group ring of the Mathieu simple group M_{22} . *LMS J. Comput. Math.* 2008. Vol. 11. P. 28–39.
121. Bovdi V., Konovalov A. B., Marcos E. N. Integral group ring of the Suzuki sporadic simple group. *Publ. Math. Debrecen.* 2008. Vol. 72, No 3–4. P. 487–503.
122. Bovdi V., Konovalov A. B., Siciliano S. Integral group ring of the Mathieu simple group M_{12} . *Rend. Circ. Mat. Palermo (2)* 2007. Vol. 56, No 1. P. 125–136.
123. Bovdi V., Konovalov A., Rossmanith R., Schneider C. GAP package LAGUNA – Lie AlGebras and UNits of group Algebras. URL: <https://www.gap-system.org/Packages/laguna.html> (date of appeal: 28.04.2020).
124. Bovdi V., Konovalov A. B. Torsion units in integral group ring of Higman-Sims simple group. *Studia Sci. Math. Hungar.* 2010. Vol. 47, No 1. P. 1–11.

125. Brauer R. Über die Darstellungen von Gruppen in Galoischen Feldern. *Act. Sci. In.* 1935. Vol. 195. P. 323–335.
126. Brawley J. Jr. Similar involutory matrices (mod p^m). *Amer. Math. Monthly.* 1966. Vol. 73. P. 499–501.
127. Brenner S. Modular representations of p -groups. *J. Algebra.* 1970. Vol. 15, Is. 1. P. 89–102.
128. Brown W. C. Matrices over commutative rings : monograph. New York : Marcel Dekker, Inc., 1993. 282 p.
129. Burnside W. On Groups of Order $p^\alpha q^\beta$. *Proceedings of the London Mathematical Society.* 1904. Vol. s2-1, Is. 1. P. 388–392.
130. Burnside W. Theory of groups of finite order : monograph. Second edition. Cambridge : Cambridge University Press, 1911. 512 p.
131. Cai J. X. A note on the theory of unitary similarity of matrices over a strong p -division ring. *J. Math. Res. Exposition.* 1990. Vol. 10, No 3. P. 474.
132. Camara M. C., Rodman L., Spitkovsky I. M. One sided invertibility of matrices over commutative rings, corona problems, and Toeplitz operators with matrix symbols. *Linear Algebra Appl.* 2014. Vol. 459. P. 58–82.
133. Cohn J. A., Livingstone D. On the structure of group algebras I. *Canad. J. Math.* 1965. Vol. 17. P. 583–593.
134. Coxeter H. S. M., Moser W. O. J. Generators and relations for discrete groups : monograph. 3-rd ed. New York : Springer-Verlag, 1972. 162 p.

135. Curtis C. W., Reiner I. Methods of representation theory : monograph : in 2 vol. New York : John Willems & Sons Inc, 1981. Vol. 1. 820 p.
136. Dinis R. F., Tylyshchak A. A., Yurchenko N. V. On indecomposability of some monomial matrices over local rings. *X International Algebraic Conference in Ukraine dedicated to the 70th anniversary of Yu. A. Drozd* : abstracts, Odessa, August 20–27, 2015. Odessa : TES, 2015. P. 32.
137. Dobbs D. E., Lancaster M. J. The probability of invertibility for a matrix over a finite commutative ring. *C. R. Math. Rep. Acad. Sci. Canada*. 1991. Vol. 13, No 5. P. 217–222.
138. Dobbs D. E., Lancaster M. J., McConnel R. M. The probability of maximal rank for a matrix over a finite commutative ring. *C. R. Math. Rep. Acad. Sci. Canada*. 1993. Vol. 15, No 5. P. 207–212.
139. Donovan P., Freislich M. R. Representable functions on the category of modular representations of a finite group with cyclic Sylow subgroup. *J. Algebra*. 1974. Vol. 32, Is. 2. P. 356–364.
140. Dougherty S., Gildea J., Korban A., Kaya A., Tylyshchak A., Yildiz B. Bordered Constructions of Self-Dual Codes from Group Rings and New Extremal Binary Self-Dual Codes. *Finite Fields and Their Applications*. 2019. Vol. 57. P. 108–127.
141. Dougherty S. T. Algebraic Coding Theory Over Finite Commutative Rings : monograph. Cham : Springer Verlag, 2017. 103 p.
142. Dougherty S. T., Gildea J., Taylor R., Tylyshchak A. Group rings, G -codes and constructions of self-dual and formally self-dual codes. *Designs, Codes and Cryptography*. 2018. Vol. 86, Is. 9. P. 2115–2138.

143. Dougherty St., Gildea J., Taylor R., Tylyshchak A. Constructions of Self-Dual and Formally Self-Dual Codes from Group Rings. ArXiv preprint arXiv:1604.07863v1, 2016. 20 p. URL: <https://arxiv.org/abs/1604.07863v1> (date of appeal: 28.03.2020).
144. Feit W., Thompson J. Solvability of groups of odd order. *Pacific Journal of Mathematics*. 1963. Vol. 13, No 3. P. 775–1029.
145. GAP – Groups, Algorithms, Programming – a System for Computational Discrete Algebra. The GAP Group. URL: <http://www.gap-system.org> (last updated: 30.01.2020).
146. Gauger M. A., Byrnes Ch. I. Characteristic free, improved decidability criteria for the similarity problem. *Linear and Multilinear Algebra*. 1977/78. Vol. 5, No 3. P. 153–158.
147. Gildea J. Zassenhaus conjecture for integral group ring of simple linear groups. *J. Algebra Appl.* 2013. Vol. 12 Is. 6. 1350016, 10 p.
148. Gildea J., Kaya A., Taylor R., Yildiz B. Constructions for Self-dual Codes Induced from Group Rings. *Finite Fields Appl.* 2018. Vol. 51. P. 71–92.
149. Gildea J., Tylyshchak A. Torsion units in the integral group ring of $PSL(3, 4)$. *J. Algebra Appl.* 2016. Vol. 15, No 1, 1650013. 9 p.
150. Golay M. J. Notes on digital coding. *Proc. I. R. E.* 1949. Vol. 37, Is. 6. P. 657.
151. Gow R., Huppert B., Knörr R., Manz O., Willems W. Representation theory in arbitrary characteristic : monograph. Trento : Casa Editrice Dott. Antonio Milani, 1993. 184 p.

152. Gudivok P. M., Chukhraj I. B. On indecomposable matrix representations of the given degree of a finite p -group over commutative local ring of characteristic p^s . *A N. St. Univ. Ovidius Constanta*. 2000. Vol. 8. P. 27–36.
153. Gudivok P. M., Rud'ko V. P. On isomorphism of Sylow subgroups of the general linear group over the ring of integers. *J. Math. Sci.* 2000. Vol. 102, No 3. P. 3998–4008.
154. Guralnick R. M. Similarity of matrices over local rings. *Linear Algebra Appl.* 1981. Vol. 41. P. 161–174.
155. Hannula T. The integral representation ring $a(R_k G)$. *Trans. Amer. Math. Soc.* 1968. Vol. 133. P. 553–559.
156. Heller A., Reiner I. Representations of cyclic groups in rings of integers II. *Ann. of Math.* 1963. Vol. 77. P. 318–328.
157. Heller A., Reiner I. Representations of cyclic groups in rings of integers. *Ann. of Math.* 1962. Vol. 76. P. 73–92.
158. Helmer O. The elementary divisor theorem for certain rings without chain conditions. *Bull. Amer. Math. Soc.* 1943. Vol. 49. P. 225–236.
159. Hertweck M. Contributions to the integral representation theory of groups : habilitationsschrift. Stuttgart : University of Stuttgart. 2004. 192 p. URL: <http://elib.uni-stuttgart.de/opus/volltexte/2004/1638> (date of appeal: 28.03.2020).
160. Hertweck M. On the torsion units of some integral group rings. *Algebra Colloq.* 2006. Vol. 13, Is. 2. P. 329–348.

161. Hertweck M. Partial augmentations and Brauer character values of torsion units in group rings. ArXiv preprint arXiv:math/0612429, 2007. 16 p. URL: <https://arxiv.org/abs/math/0612429> (date of appeal: 28.03.2020).
162. Hertweck M. Zassenhaus conjecture for A_6 . *Proc. Indian Acad. Sci. Math. Sci.* 2008. Vol. 118, Is. 2. P. 189–195.
163. Hertweck M., Höfert C., Kimmerle W. Finite groups of units and their composition factors in the integral group rings of the group $PSL(2, q)$. *J. Group Theory*. 2009. Vol. 12, Is. 6. P. 873–882.
164. Higman D. G. Indecomposable representations at characteristic p . *Duke Math. J.* 1954. Vol. 21. P. 377–381.
165. Huffman W. C., Pless V. Fundamentals of error-correcting codes : textbook. Cambridge : Cambridge University Press, 2003. xviii + 646 p.
166. Hurley T. Group Rings and Rings of Matrices. *Int. Jour. Pure and Appl. Math.* 2006. Vol. 31, No 3. P. 319–335.
167. Jones A. Groups with a finite number of indecomposable integral representations. *Michigan Math. J.* 1963. Vol. 10. P. 257–261.
168. Jones A. Integral representations of cyclic p -groups. *An. Acad. Brasil. Cienc.* 1982. Vol. 54, No 1. P. 19–22.
169. Kane G. Modern Elementary Particle Physics: Explaining and Extending the Standard Model : textbook. Cambridge: Cambridge University Press, 2017. 226 p.
170. Kanemasu M. Golay codes. *MIT Undergraduate J. Math.* 1999. Vol. 1. P. 95–99.

171. Kaplansky I. Elementary divisor ring and modules. *Trans. Amer. Math. Soc.* 1949. Vol. 66. P. 464–491.
172. Kida K. On representations of cyclic groups over a ring of integers. *Comm. Algebra.* 2012. Vol. 40, No 10. P. 3753–3758.
173. Kimmerle W. On the prime graph of the unit group of integral group rings of finite groups. *Groups, Rings and Algebras, Contemporary Mathematics.* 2006. Vol. 420.
174. Kolchin E. R. On certain concepts in the theory of algebraic matrix groups. *Ann. of Math.* 1948. Vol. 49. P. 774–789.
175. Lam T. Y. Exercises in Classical Ring Theory : Problem Books in Mathematics. New York : Springer Verlag, 1995. 288 p.
176. Leedham-Green C. R., Plesken W. Some remarks of Sylow subgroups of general linear groups. *Math. Z.* 1986. Vol. 191. P. 529–535.
177. Luthar I. S. Passi I. B. S. Zassenhaus conjecture for A_5 . *Proc. Indian Acad. Sci. Math. Sci.* 1989. Vol. 99 Is. 1. P. 1–5.
178. Luthar I. S., Trama P. Zassenhaus conjecture for S_5 . *Comm. Algebra.* 1991. Vol. 19 Is. 8. P. 2353–2362.
179. Noether E. Hypercomplexe Grossen und Darstellungstheorie. *Math. Z.* 1929. Vol. 30. P. 641–692.
180. MacWilliams F. J., Sloane N. J. A. The Theory of Error-Correcting Codes : Mathematical Studies. Amsterdam : North Holland Publishing Co., 1977. 762 p.

181. Maranda J. M. On the equivalence of representations of finite groups of automorphisms of modules over Dedekind domain. *Canad. J. Math.* 1955. Vol. 7. P. 401–404.
182. Marciniak Z., Ritter J., Sehgal S. K., Weiss A. Torsion units in integral group rings of some metabelian groups. II. *J. Number Theory*. 1987. Vol. 25 Is. 3. P. 340–352.
183. McDonald B. R. Similarity of matrices over Artinian principal ideal rings. *Linear Algebra Appl.* 1978. Vol. 21, No 2. P. 153–162.
184. McDonald B. R. Linear algebra over commutative ring : monograph. New York : Marcel Dekker, 1984. 544 p.
185. McLoughlin I., Hurley T. A group ring construction of the extended binary Golay code. *IEEE Trans. Inform. Theory*. 2008. Vol. 9 Is. 54. P. 4381–4383.
186. McLoughlin I. Dihedral codes: Ph.D. thesis: submitted in June 2009 / National University of Ireland, Galway (Ireland)., 2009. 106 p.
187. McNinch G. Abelian unipotent subgroups of reductive groups. *J. Pure Appl. Algebra*. 2002. Vol. 167 Is. 2–3. P. 269–300.
188. Mini-Workshop, Arithmetik von Gruppenringen / Ed. E. Jespers, Z. Marciniak, G. Nebe and W. Kimmerle *Oberwolfach Reports*. Zurich : EMS Publish. House, 2007. Vol. 4, No 4. P. 3209–3240.
189. Mitsuda T. Integral representations of cyclic groups of order pq . *Proceedings of the 14th Symposium on Ring Theory*. 1981. Okayama : Okayama Univ. P. 85–92.

190. Reiner I. Integral representations of cyclic groups of order p^2 . *Proc. Amer. Math. Soc.* 1976. Vol. 58. P. 8–12.
191. Tu B. X. Unitary similarity theory for square matrices over strong p -division rings II. *J. Math. Res. Exposition.* 1988. Vol. 8, No 1. P. 11–21.
192. Peng X. H., Farrell P. G. On construction of the (24, 12, 8) Golay codes. *IEEE Trans. Inform. Theory.* 2006. Vol. 8, Is. 52. P. 3669–3675.
193. Pizarro A. Similarity classes of 3×3 matrices over a discrete valuation ring. *Linear Algebra Appl.* 1983. Vol. 54. P. 29–51.
194. Platonov Vol. P., Potapchik A. New combinatorial properties of linear groups. *J. Algebra.* 2001. Vol. 235, Is. 1. P. 399–415.
195. Prasad A., Singla P., Spallone S. Similarity of matrices over local rings of length two. ArXiv preprint arXiv:1212.6157, 2013. 46 p. URL: <https://arxiv.org/abs/1212.6157> (date of appeal: 28.03.2020).
196. Prasad A., Singla P. Similarity of matrices over local rings of length two. *Indiana Univ. Math. J.* 2015. Vol. 64, No 2. P. 471–514.
197. Radaelli P. G. Symmetry in Crystallography: Understanding the International Tables : monograph. Oxford : Oxford University Press, 2016. 2011 p.
198. Rains E. M. Shadow Bounds for Self Dual Codes. *IEEE Trans. Inf. Theory.* 1998. Vol. 44. P. 134–139.
199. Recski A. Combinatorial optimization methods to determine the rank of a matrix over a commutative ring, with engineering applications. *Progress in combinatorial optimization.* London : ISTE, 2012. P. 343–352.

- 200. Reiner I. A survey of integral representations theory. *Bull. Amer. Math. Soc.* 1970. Vol. 76, Is. 2. P. 159–227.
- 201. Reiner I. Integral representations of cyclic groups of prime order. *Proc. Am. Math. Soc.* 1957. Vol. 8. P. 142–146.
- 202. Reiner I. Relations between integral and modular representations. *Mich. Math. J.* 1966. Vol. 13. P. 357–372.
- 203. Ringel C. The indecomposable representations of dihedral 2-groups. *Math. Ann.* 1975. Vol. 214, No 1. P. 19–34.
- 204. Roggenkamp K., Scott L. Isomorphisms of p -adic group rings. *Ann. of Math.* 1987. Vol. 126, Is. 2. P. 593–647.
- 205. Roggenkamp K. W. R -orders in a split algebra have finitely many non-isomorphic irreducible lattice as soon as R has finite class number. *Canad. J. Math.* 1971. Vol. 14. P. 405–409.
- 206. Salim M. Torsion units in the integral group ring of the alternating group of degree 6. *Comm. in Algebra.* 2007. Vol. 35, No 12. P. 4198–4204.
- 207. Simion I. I. Witt overgroups for unipotent elements in exceptional algebraic groups of bad characteristic. *Mathematica (Cluj.)*. 2015. Vol. 57 (80), No 1–2. P. 104–116.
- 208. Smith H. J. S. On systems of linear indeterminate equation and congruences. *Phil. Trans. Roy. Soc. London.* 1861. Vol. 151, No 2. P. 293–326.
- 209. Stasinski A. Similarity and commutators of matrices over principal ideal rings. *Trans. Amer. Math. Soc.* 2016. Vol. 368, No 4. P. 2333–2354.

210. Stoika M. V., Tylyshchak A. A. On classifying the matrices over commutative rings up to equivalence. *International Conference of Young Mathematicians* : book of abstracts, Kyiv, June 3–6, 2015. Kyiv : Institute of Mathematics of NAS of Ukraine, 2015. P. 23.
211. Swan R. Induced representations and projektive modules. *Ann. of Math.* 1960. Vol. 71. P. 552–578.
212. Thevenaz J. Representations of finite groups in characteristic p^r . *J. Algebra*. 1981. Vol. 72, Is. 2. P. 478–500.
213. Tu B. X. Unitary similarity theory for square matrices over strong p -division rings I. *J. Math. Res. Exposition*. 1987. Vol. 7, No 3. P. 393–402.
214. Tu B. X. Unitary similarity theory for square matrices over strong p -division rings III. *J. Math. Res. Exposition*. 1989. Vol. 9, No 1. P. 1–8.
215. Tylyshchak A. A. On irreducibility of monomial matrices of order 7 over local rings. *XII International Algebraic Conference in Ukraine dedicated to the 215th anniversary of V. Bunyakovsky* : abstracts, 2019, July 02-06, Vinnytsia, Ukraine. Vinnytsia : Vasyl' Stus Donetsk National University, 2019. P. 117–118.
216. Tylyshchak A., Bortosh M. On Reducibility of Monomial Matrixes over Commutative Local Rings. *IX International Algebraic Conference in Ukraine* : abstracts of reports, L'viv, July 8–13, 2013. L'viv : Ivan Franko National University of L'viv, 2013. P. 201.
217. Tylyshchak A. On maximal unipotent subgroups of the general linear group over commutative ring. *XI International Mathematical Kravchuk Conference* : conference materials, (Алгебра, геометрія. Математич-

- ний та чисельний аналіз), Kyiv, May 18–20, 2006. Kyiv. : TOV «Zadruha», 2006. P. 616.
218. Tylyshchak A. A. On Irreducible Modular Representations of Given Degree of Finite Group over Commutative Local Ring. *International Conference of Humboldt-Kolleg Series in Kyiv «Humboldt Cosmos: Science and Society»*, Kyiv, November 19–22, 2009 : abstracts, Kyiv, November 19–22, 2009. Kyiv : Embassy of the Federal Republic of Germany Kyiv, 2009. P. 45.
219. Tylyshchak A. A. On maximal unipotent subgroups of the general linear group over commutative rings. *Bulletin of University of Kyiv. Ser.: Phys. & Math.* 2010. Vol. No 3. P. 115–117.
220. Tylyshchak A. A. On the estimation of the number of indecomposable representations of given degree of a cyclic group. *XI International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko* : abstracts, Kyiv, July 3–7, 2017. Kyiv : Institute of Mathematics of NAS of Ukraine, 2017. P. 137.
221. Tylyshchak O. Irreducible modular representation of the given degree of finite p -group over commutative local ring of characteristic p^s . *IV International Algebraic Conference in Ukraine* : abstracts, L'viv, August 4–9, 2003. L'viv : Ivan Franko National University of L'viv, 2003. P. 222–223.
222. Weiss A. Rigidity of p -adic p -torsion. *Ann. of Math.* 1988. Vol. 127, Is. 2. P. 317–332.

- 223. Witt E. Die algebraische Struktur des Gruppenringes endlichen Gruppe über einem Zahlenkörper. *J. für Math.* 1952. Vol. 190. P. 231–245.
- 224. Zassenhaus H. On the torsion units of finite group rings. *Studies in Mathematics*. Lisboa: Instituto de Alta Cultura. 1974. P. 119–126.
- 225. Zimmerman K.-H. Beiträge zur algebraischen Codierungstheorie mittels modularer Darstellungstheorie : habilitationsschrift. Bayreuth : Bayreuther Math. Schr., 1994, No 48. 278 p.

ДОДАТОК А.

ОБЧИСЛЕННЯ ЧИСЛОВИХ ХАРАКТЕРИСТИК МНОЖИНИ УНІМОНОМІАЛЬНИХ ЗОБРАЖЕНЬ НАД ЛОКАЛЬНИМИ КІЛЬЦЯМИ СКІНЧЕННОЇ ДОВЖИНИ

Всюди в межах додатку через K будемо позначати комутативне локальне кільце довжини l характеристики p , що не є полем; через K^* — групу його оборотних елементів відносно множення, через t — твірний елемент радикала Джекобсона $\text{Rad } K$ кільця K , через $H = \langle a \rangle$ — циклічну p -групу порядку m . Подані в даному додатку результати числових експериментів отримані за допомогою наведених програм, реалізованих у системі GAP 4.10.1.

А.1. Підрахунок числа нерозкладних нееквівалентних унімономіальних зображень

Підрахуємо спочатку число $U(l, n)$ неперіодичних послідовностей $\bar{w} = (s_1, s_2, \dots, s_n)$, кожна з яких найменша в лексикографічному порядку серед собі циклічно еквівалентних, де $s_i \in \{0, 1, \dots, l-1\}$ ($i = 1, 2, \dots, n$). Для підрахунку числа $U(2, 6)$ можна використати, наприклад, таку серію команд.

```
l:=2;n:=6;
                                # Формуємо n-у декартову степінь множин {0, 1, ..., l-1}
L:=Cartesian(List([1..n],i->[0..l-1]));;
M:=Filtered(L,f->                                # Вибираємо неперіодичні послідовності
    not(ForAny([1..n-1],i->ForAll([1..n],j->f[j]=f[(j+i-1) mod n+1])))
);
```



```

repeat
  if not(ForAny([1..n-1], i->
    # Перевірка на неперіодичність
    ForAll([1..n], j->f[j]=f[(j+i-1) mod n+1]))
  )) then y:=y+1; fi;
  # формуємо наступну послідовність з n-ї декартової степені множин {0..l-1}
  for i in [1..n] do if f[i]=l-1 then f[i]:=0;
    else f[i]:=f[i]+1; break; fi; od;
until Sum(f)=0;
Print(y/n, "\n");      # Кількість класів циклічно еквівалентних послідовностей

```

В результаті обчислень також одержуємо $U(2, 6) = 9$.

Модифікуємо останній варіант коду, що обчислює число $U(l, n)$ неперіодичних послідовностей $\bar{w} = (s_1, s_2, \dots, s_n)$, кожна з яких найменша в лексикографічному порядку серед собі циклічно еквівалентних, де $s_i \in \{0, 1, \dots, l-1\}$ ($i = 1, 2, \dots, n$) до відшукування числа $V(k, l, n)$ послідовностей $(s_1, s_2, \dots, s_n, \varepsilon)$, $s_i \in \{0, 1, \dots, l-1\}$ ($i = 1, 2, \dots, n$), таких, що $(s_1, s_2, \dots, s_n)$ — неперіодична послідовність, найменша в лексикографічному порядку серед її циклічно еквівалентних, ε належить множині оборотних представників всіх різних суміжних класів $K/Ann(t^s) = K/t^{l-s}K$ ($s = \max(s_1, s_2, \dots, s_n)$) для скінченного локального кільця K довжини $l > 1$ з порядком $k = |K/\text{Rad } K|$ поля лишків кільця K . В підрозділі 4.3 казано, що число нерозкладних матриць $M(\bar{w}, \bar{\varepsilon})$ порядку $n > 1$ розглядуваних з точністю до подібності над скінченим локальним кільцем K довжини $l > 1$ з порядком $k = |K/\text{Rad } K|$ поля лишків кільця K не менше числа $V(k, l, n)$.

Приєднаємо для кожної послідовності $\bar{w} = (s_1, s_2, \dots, s_n)$ обчислення найбільшого її елемента s , домноження кількостей послідовностей з однаковим s на $(k-1)k^{l-s-1}$, що за лемою 4.9 є кількістю оборотних представників $K/Ann(t^s) = K/t^{l-s}K$, де k оголошується цілочисловою невідомою, та сумування одержаних добутків для обчислення числа

$V(k, l, n)$. При $l = 4, n = 3$ число $V(k, 4, 3)$ можна обчислити, наприклад, такою серією команд.

```
l:=4;n:=3;maxlist:=[];matnumblist:=[];k:=Indeterminate(Integers,"k");
f:=List([1..n], x->0); # формуємо послідовність з n нулів
repeat
  if not(ForAny([1..n-1],i-> # Перевірка на неперіодичність
    ForAll([1..n],j->f[j]=f[(j+i-1) mod n+1]))
  ) then Add(maxlist,Maximum(f)); fi;
  # формуємо наступну послідовність з n-ї декарто-ї степені множин {0..l-1}
  for i in [1..n] do if f[i]=l-1 then f[i]:=0;
    else f[i]:=f[i]+1; break; fi; od;
until Sum(f)=0;
for s in [1..l-1] do # Рахуємо кількість класів послідовностей з однаковими s
  Add(matnumblist, Number(maxlist,x->x=s)/n*(k-1)*k^(l-s-1)); od;
Print(Sum(matnumblist),"\n");
```

В результаті обчислень одержуємо $V(k, 4, 3) = 2k^3 + 4k^2 + 6k - 12$.

Модифікуємо код, що обчислює число $V(k, l, n)$ до відшукування числа $W(k, l, m, n)$ послідовностей $(s_1, s_2, \dots, s_n, \varepsilon)$, $s_i \in \{0, 1, \dots, l-1\}$ ($i = 1, 2, \dots, n$), таких, що $(s_1, s_2, \dots, s_n)$ — неперіодична послідовність, найменша в лексикографічному порядку серед її циклічно еквівалентних, $\sum_{j=0}^{m-1} s_{i+j} \geq l$ ($i = 1, 2, \dots, n; m > 1$), ε належить множині оборотних представників всіх різних суміжних класів $K/Ann(t^s) = K/t^{l-s}K$ ($s = \max(s_1, s_2, \dots, s_n)$) для скінченного локального кільця K довжини $l > 1$ з порядком $k = |K/\text{Rad } K|$ поля лишків кільця K . В підрозділі 4.3 казано, що число нерозкладних зображень вигляду (4.5) степеня n з точністю до еквівалентності циклічної p -групи $H = \langle a \rangle$ порядку m над скінченим локальним кільцем K довжини $l > 1$ з порядком $k = |K/\text{Rad } K|$ поля лишків кільця K не менше числа $W(k, l, m, n)$. Для зручності ми знаходитимемо $W(k, l, m, n)$ також у випадку, коли m не є степенем жодного простого числа.

Залишається приєднати перевірку, чи послідовність $\bar{w} = (s_1, s_2, \dots, s_n)$, $s_i \in \{0, 1, \dots, l-1\}$ задовольняє умові $\sum_{j=0}^{m-1} s_{i+j} \geq l$ ($i = 1, 2, \dots, n$; $m > 1$). При $l = 4$, $m = 2$, $n = 3$ число $W(k, 4, 2, 3)$ можна обчислити, наприклад, такою серією команд.

```
l:=4;m:=2;n:=3;maxlist:=[];matnumblist:=[];
k:=Indeterminate(Integers,"k");
f:=List([1..n], x->0);                                # формуємо послідовність з n нулів
repeat
  if not(ForAny([1..n-1],                                # Перевірка на неперіодичність та зображення
    i->ForAll([1..n],j->f[j]=f[(j+i-1) mod n+1]))) then
  if ForAll([1..n],i->Sum([0..m-1],j->f[(j+i-1) mod n+1])>=l) then
    Add(maxlist,Maximum(f)); fi;fi;
    # формуємо наступну послідовність з n-ї декарто-ї степені множин {0..l-1}
  for i in [1..n] do if f[i]=l-1 then f[i]:=0;
    else f[i]:=f[i]+1; break; fi; od;
until Sum(f)=0;
# Рахуємо кількість класів ц. еквівалентних послідовностей з однаковими s
for s in [1..l-1] do
  Add(matnumblist, Number(maxlist,x->x=s)/n*(k-1)*k^(l-s-1)); od;
Print(Sum(matnumblist),"\n");
```

В результаті одержимо $W(k, 4, 2, 3) = 3k - 3$ ($V(k, 4, 3) = 2k^3 + 4k^2 + 6k - 12$). Подамо результати повторного запуск коду для обчислення $W(k, l, m, n)$ при деяких значеннях l , m , n таблицями. При незначній зміні m значення $W(k, l, m, n)$ часто повторюються. Тому для кращої наочності ризкою відмічені значення, які повторюють вказані при попередньому m .

Таблиця А.1. Результати обчислення $W(k, l, m, n)$ при $l = 2$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$
$m = 2$	0	0	0	0	0	0	0	0	0
$m = 3$	—	$k - 1$	$k - 1$	$k - 1$	$k - 1$	$2k - 2$	$2k - 2$	$3k - 3$	$4k - 4$
$m = 4$	$k - 1$	—	$2k - 2$	$3k - 3$	$3k - 3$	$6k - 6$	$8k - 8$	$14k - 14$	$20k - 20$
$m = 5$	—	—	—	$5k - 5$	$6k - 6$	$10k - 10$	$15k - 15$	$27k - 27$	$43k - 43$
$m = 6$	—	$2k - 2$	—	—	$8k - 8$	$14k - 14$	$21k - 21$	$37k - 37$	$63k - 63$
$m = 7$	—	—	—	—	—	$17k - 17$	$26k - 26$	$45k - 45$	$77k - 77$
$m = 8$	—	—	$3k - 3$	—	—	—	$29k - 29$	$51k - 51$	$87k - 87$
$m = 9$	—	—	—	—	—	—	—	$55k - 55$	$94k - 94$
$m = 10$	—	—	—	$6k - 6$	—	—	—	—	$98k - 98$
$m = 11$	—	—	—	—	—	—	—	—	—
$m = 12$	—	—	—	—	$9k - 9$	—	—	—	—
$m = 13$	—	—	—	—	—	—	—	—	—
$m = 14$	—	—	—	—	—	$18k - 18$	—	—	—
$m = 15$	—	—	—	—	—	—	—	—	—
$m = 16$	—	—	—	—	—	—	$30k - 30$	—	—
$m = 17$	—	—	—	—	—	—	—	—	—
$m = 18$	—	—	—	—	—	—	—	$56k - 56$	—

Таблица А.2. Результаты обчислення $W(k, l, m, n)$ при $l = 3$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$
$m = 2$	$k - 1$	$k - 1$	$k - 1$	$2k - 2$	$2k - 2$	$4k - 4$	$5k - 5$	$8k - 8$
$m = 3$	—	$5k - 5$	$7k - 7$	$14k - 14$	$27k - 27$	$61k - 61$	$122k - 122$	$265k - 265$
$m = 4$	$2k - 2$	—	$k^2 +$ $13k - 14$	$k^2 +$ $28k - 29$	$k^2 + 61k -$ 62	$k^2 + 155k -$ 156	$k^2 + 368k -$ 369	$2k^2 + 909k -$ 911
$m = 5$	—	$k^2 + 4k -$ 5	—	$3k^2 +$ $38k - 41$	$3k^2 + 86k -$ 89	$4k^2 + 223k -$ 227	$5k^2 + 564k -$ 569	$8k^2 + 1480k -$ 1488
$m = 6$	$k^2 +$ $k - 2$	$k^2 + 5k -$ 6	—	—	$6k^2 +$ $100k - 106$	$9k^2 + 260k -$ 269	$11k^2 +$ $677k - 688$	$18k^2 +$ $1811k - 1829$
$m = 7$	—	—	$2k^2 +$ $12k - 14$	—	—	$14k^2 +$ $279k - 293$	$19k^2 +$ $729k - 748$	$29k^2 +$ $1977k - 2006$
$m = 8$	—	—	$2k^2 +$ $13k - 15$	$4k^2 +$ $37k - 41$	—	—	$26k^2 +$ $753k - 779$	$42k^2 +$ $2045k - 2087$
$m = 9$	—	$2k^2 +$ $4k - 6$	—	$5k^2 +$ $36k - 41$	—	—	—	$51k^2 +$ $2076k - 2127$
$m = 10$	—	—	—	$5k^2 +$ $37k - 42$	$7k^2 + 99k -$ 106	—	—	—

Таблица А.3. Результаты обчислення $W(k, l, m, n)$ при $l = 4$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$m = 2$	$2k - 2$	$3k - 3$	$5k - 5$	$11k - 11$	$19k - 19$	$41k - 41$	$78k - 78$
$m = 3$	$k^2 + k - 2$	$3k^2 + 8k - 11$	$3k^2 + 21k - 24$	$5k^2 + 63k - 68$	$7k^2 + 186k - 193$	$15k^2 + 553k - 568$	$23k^2 + 1603k - 1626$
$m = 4$	$2k^2 + k - 3$	—	$11k^2 + 30k - 41$	$19k^2 + 104k - 123$	$34k^2 + 354k - 388$	$77k^2 + 1229k - 1306$	$166k^2 + 4164k - 4330$
$m = 5$	—	$5k^2 + 6k - 11$	—	$k^3 + 36k^2 + 118k - 155$	$k^3 + 68k^2 + 432k - 501$	$k^3 + 160k^2 + 1588k - 1749$	$k^3 + 377k^2 + 5718k - 6096$
$m = 6$	—	$k^3 + 5k^2 + 6k - 12$	$k^3 + 11k^2 + 29k - 41$	—	$3k^3 + 98k^2 + 452k - 553$	$4k^3 + 230k^2 + 1713k - 1947$	$4k^3 + 561k^2 + 6354k - 6919$
$m = 7$	—	—	$k^3 + 13k^2 + 27k - 41$	$2k^3 + 35k^2 + 118k - 155$	—	$9k^3 + 278k^2 + 1740k - 2027$	$11k^3 + 681k^2 + 6542k - 7234$
$m = 8$	$k^3 + k^2 + k - 3$	—	$2k^3 + 13k^2 + 27k - 42$	$3k^3 + 36k^2 + 116k - 155$	—	—	$19k^3 + 753k^2 + 6577k - 7349$
$m = 9$	—	—	—	$3k^3 + 38k^2 + 114k - 155$	$5k^3 + 97k^2 + 451k - 553$	—	—
$m = 10$	—	—	—	$5k^3 + 37k^2 + 114k - 156$	$6k^3 + 98k^2 + 449k - 553$	$11k^3 + 276k^2 + 1740k - 2027$	—

Таблица А.4. Результаты обчислення $W(k, l, m, n)$ при $l = 5$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$m = 2$	$k^2 + 2k - 3$	$k^2 + 5k - 6$	$k^2 + 13k - 14$	$2k^2 + 35k - 37$	$2k^2 + 86k - 88$	$4k^2 + 226k - 230$	$5k^2 + 572k - 577$
$m = 3$	$2k^2 + k - 3$	$k^3 + 8k^2 + 10k - 19$	$k^3 + 14k^2 + 42k - 57$	$k^3 + 35k^2 + 175k - 211$	$k^3 + 87k^2 + 699k - 787$	$2k^3 + 230k^2 + 2718k - 2950$	$2k^3 + 567k^2 + 10420k - 10989$
$m = 4$	$k^3 + 2k^2 + k - 4$	$2k^3 + 7k^2 + 10k - 19$	$7k^3 + 31k^2 + 51k - 89$	$10k^3 + 88k^2 + 254k - 352$	$14k^3 + 265k^2 + 1182k - 1461$	$27k^3 + 853k^2 + 5390k - 6270$	$51k^3 + 2699k^2 + 24023k - 26773$
$m = 5$	—	$3k^3 + 8k^2 + 8k - 19$	—	$29k^3 + 122k^2 + 268k - 419$	$47k^3 + 399k^2 + 1341k - 1787$	$94k^3 + 1388k^2 + 6494k - 7976$	$200k^3 + 4780k^2 + 30660k - 35640$
$m = 6$	$2k^3 + k^2 + k - 4$	$5k^3 + 7k^2 + 8k - 20$	$10k^3 + 29k^2 + 50k - 89$	—	$k^4 + 88k^3 + 459k^2 + 1361k - 1909$	$k^4 + 183k^3 + 1658k^2 + 6771k - 8613$	$k^4 + 402k^3 + 5980k^2 + 32761k - 39144$
$m = 7$	—	—	$k^4 + 10k^3 + 30k^2 + 48k - 89$	$k^4 + 31k^3 + 119k^2 + 268k - 419$	—	$4k^4 + 265k^3 + 1752k^2 + 6798k - 8819$	$4k^4 + 595k^3 + 6453k^2 + 33212k - 40264$

Таблиця А.5. Результати обчислення $W(k, l, m, n)$ при $l = 6$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$
$m = 2$	$2k^2 + 2k - 4$	$3k^2 + 7k - 10$	$5k^2 + 25k - 30$	$11k^2 + 84k - 95$	$19k^2 + 267k - 286$	$41k^2 + 861k - 902$
$m = 3$	$k^3 + 2k^2 +$	$6k^3 + 11k^2 +$	$8k^3 + 34k^2 +$	$15k^3 + 121k^2 +$	$30k^3 + 430k^2 +$	$70k^3 + 1495k^2 +$
	$k - 4$	$12k - 29$	$69k - 111$	$373k - 509$	$1892k - 2352$	$9245k - 10810$
$m = 4$	$k^4 + 2k^3 +$	$k^4 + 6k^3 +$	$3k^4 + 29k^3 +$	$4k^4 + 66k^3 +$	$4k^4 + 169k^3 +$	$7k^4 + 490k^3 +$
	$k^2 + k - 5$	$10k^2 + 12k -$	$54k^2 + 78k -$	$236k^2 + 500k -$	$1014k^2 + 2954k -$	$4370k^2 + 16840k -$
		29	164	806	4141	21707
$m = 5$	—	$3k^4 + 6k^3 +$	$4k^4 + 28k^3 +$	$19k^4 + 122k^3 +$	$26k^4 + 345k^3 +$	$45k^4 + 1097k^3 +$
		$10k^2 + 10k -$	$54k^2 + 78k -$	$274k^2 + 514k -$	$1305k^2 + 3230k -$	$6116k^2 + 19460k -$
		29	164	929	4906	26718
$m = 6$	$2k^4 + k^3 +$	$5k^4 + 7k^3 +$	$7k^4 + 29k^3 +$	—	$69k^4 + 464k^3 +$	$128k^4 + 1543k^3 +$
	$k^2 + k - 5$	$8k^2 + 10k -$	$51k^2 + 77k -$		$1371k^2 + 3250k -$	$6711k^2 + 19989k -$
		30	164		5154	28371
$m = 7$	—	—	$11k^4 + 27k^3 +$	$26k^4 + 118k^3 +$	—	$k^5 + 233k^4 +$
			$51k^2 + 75k -$	$271k^2 + 514k -$		$1766k^3 + 6813k^2 +$
			164	929		$20016k - 28829$

Таблица А.6. Результаты обчислення $W(k, l, m, n)$ при $l = 7$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$
$m = 2$	$k^3 + 2k^2 + 2k - 5$	$k^3 + 5k^2 + 9k - 15$	$k^3 + 13k^2 + 41k - 55$	$2k^3 + 35k^2 + 168k - 205$	$2k^3 + 86k^2 + 658k - 746$	$4k^3 + 226k^2 + 2553k - 2783$
$m = 3$	$k^4 + k^3 + 2k^2 + k - 5$	$3k^4 + 11k^3 + 13k^2 + 14k - 41$	$3k^4 + 25k^3 + 61k^2 + 102k - 191$	$5k^4 + 71k^3 + 291k^2 + 679k - 1046$	$7k^4 + 220k^3 + 1349k^2 + 4191k - 5767$	$15k^4 + 674k^3 + 5996k^2 + 24816k - 31501$
$m = 4$	$2k^4 + 2k^3 + k^2 + k - 6$	$5k^4 + 10k^3 + 12k^2 + 14k - 41$	$k^5 + 23k^4 + 56k^3 + 81k^2 + 111k - 272$	$k^5 + 43k^4 + 206k^3 + 482k^2 + 866k - 1598$	$k^5 + 91k^4 + 793k^3 + 2699k^2 + 6196k - 9780$	$k^5 + 231k^4 + 3180k^3 + 14746k^2 + 42505k - 60663$
$m = 5$	$k^5 + k^4 + 2k^3 + k^2 + k - 6$	$k^5 + 8k^4 + 8k^3 + 12k^2 + 12k - 41$	$2k^5 + 23k^4 + 55k^3 + 81k^2 + 111k - 272$	$10k^5 + 113k^4 + 282k^3 + 520k^2 + 880k - 1805$	$12k^5 + 271k^4 + 1234k^3 + 3194k^2 + 6639k - 11350$	$17k^5 + 772k^4 + 5489k^3 + 18867k^2 + 47870k - 73015$
$m = 6$	$k^5 + 2k^4 + k^3 + k^2 + k - 6$	$3k^5 + 8k^4 + 9k^3 + 10k^2 + 12k - 42$	$5k^5 + 27k^4 + 52k^3 + 78k^2 + 110k - 272$	$11k^5 + 112k^4 + 282k^3 + 520k^2 + 880k - 1805$	$47k^5 + 454k^4 + 1388k^3 + 3260k^2 + 6659k - 11808$	$77k^5 + 1358k^4 + 6566k^3 + 19929k^2 + 48807k - 76737$
$m = 7$	—	—	$7k^5 + 31k^4 + 48k^3 + 78k^2 + 108k - 272$	$18k^5 + 115k^4 + 275k^3 + 517k^2 + 880k - 1805$	—	$184k^5 + 1763k^4 + 6845k^3 + 20031k^2 + 48834k - 77657$

Таблиця А.7. Результати обчислення $W(k, l, m, n)$ при $l = 8$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
$m = 2$	$2k^3 + 2k^2 +$ $2k - 6$	$3k^3 + 7k^2 + 11k -$ 21	$5k^3 + 25k^2 + 61k -$ 91	$11k^3 + 84k^2 + 297k -$ 392	$19k^3 + 267k^2 + 1387k -$ 1673
$m = 3$	$2k^4 + k^3 +$ $2k^2 + k - 6$	$k^5 + 9k^4 + 14k^3 +$ $15k^2 + 16k - 55$	$k^5 + 15k^4 + 51k^3 +$ $94k^2 + 141k - 302$	$k^5 + 36k^4 + 204k^3 +$ $568k^2 + 1115k - 1924$	$k^5 + 91k^4 + 855k^3 +$ $3259k^2 + 8122k - 12328$
$m = 4$	$2k^5 + 2k^4 +$ $k^3 + k^2 + k - 7$	$3k^5 + 9k^4 +$ $13k^3 + 14k^2 +$ $16k - 55$	$15k^5 + 55k^4 +$ $85k^3 + 114k^2 +$ $150k - 419$	$24k^5 + 166k^4 +$ $450k^3 + 848k^2 +$ $1376k - 2864$	$41k^5 + 560k^4 + 2337k^3 +$ $5844k^2 + 11552k -$ 20334
$m = 5$	—	$k^6 + 5k^5 + 11k^4 +$ $10k^3 + 14k^2 +$ $14k - 55$	$k^6 + 17k^5 + 53k^4 +$ $84k^3 + 114k^2 +$ $150k - 419$	$4k^6 + 94k^5 + 287k^4 +$ $530k^3 + 886k^2 +$ $1390k - 3191$	$4k^6 + 193k^5 + 1115k^4 +$ $3120k^3 + 6603k^2 +$ $12228k - 23263$
$m = 6$	$k^6 + 2k^5 + k^4 +$ $k^3 + k^2 + k - 7$	$3k^6 + 8k^5 + 9k^4 +$ $10k^3 + 12k^2 +$ $14k - 56$	$3k^6 + 24k^5 + 52k^4 +$ $80k^3 + 111k^2 +$ $149k - 419$	$6k^6 + 93k^5 + 286k^4 +$ $530k^3 + 886k^2 +$ $1390k - 3191$	$26k^6 + 420k^5 + 1408k^4 +$ $3280k^3 + 6669k^2 +$ $12248k - 24051$
$m = 7$	—	—	$7k^6 + 25k^5 + 54k^4 +$ $75k^3 + 111k^2 +$ $147k - 419$	$13k^6 + 104k^5 +$ $278k^4 + 523k^3 +$ $883k^2 + 1390k - 3191$	$27k^6 + 419k^5 + 1408k^4 +$ $3280k^3 + 6669k^2 +$ $12248k - 24051$

Таблица А.8. Результаты обчислення $W(k, l, m, n)$ при $l = 9$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
$m = 2$	$k^4 + 2k^3 + 2k^2 + 2k - 7$	$k^4 + 5k^3 + 9k^2 + 13k - 28$	$k^4 + 13k^3 + 41k^2 + 85k - 140$	$2k^4 + 35k^3 + 168k^2 + 481k - 686$	$2k^4 + 86k^3 + 658k^2 + 2614k - 3360$
$m = 3$	$k^5 + 2k^4 + k^3 + 2k^2 + k - 7$	$6k^5 + 14k^4 + 16k^3 + 17k^2 + 18k - 71$	$8k^5 + 38k^4 + 84k^3 + 133k^2 + 186k - 449$	$15k^5 + 129k^4 + 442k^3 + 974k^2 + 1703k - 3263$	$30k^5 + 472k^4 + 2342k^3 + 6674k^2 + 14311k - 23829$
$m = 4$	$k^6 + 2k^5 + 2k^4 + k^3 + k^2 + k - 8$	$2k^6 + 7k^5 + 13k^4 + 15k^3 + 16k^2 + 18k - 71$	$8k^6 + 49k^5 + 88k^4 + 118k^3 + 153k^2 + 195k - 611$	$11k^6 + 122k^5 + 402k^4 + 816k^3 + 1358k^2 + 2054k - 4763$	$15k^6 + 354k^5 + 1899k^4 + 5332k^3 + 11091k^2 + 19784k - 38475$
$m = 5$	$2k^6 + k^5 + 2k^4 + k^3 + k^2 + k - 8$	$6k^6 + 8k^5 + 13k^4 + 12k^3 + 16k^2 + 16k - 71$	$12k^6 + 48k^5 + 86k^4 + 117k^3 + 153k^2 + 195k - 611$	$k^7 + 69k^6 + 282k^5 + 543k^4 + 896k^3 + 1396k^2 + 2068k - 5255$	$k^7 + 121k^6 + 956k^5 + 2984k^4 + 6529k^3 + 12192k^2 + 20777k - 43560$
$m = 6$	$k^7 + 2k^6 + k^5 + k^4 + k^3 + k^2 + k - 8$	$k^7 + 8k^6 + 10k^5 + 11k^4 + 12k^3 + 14k^2 + 16k - 72$	$k^7 + 21k^6 + 51k^5 + 81k^4 + 113k^3 + 150k^2 + 194k - 611$	$3k^7 + 71k^6 + 279k^5 + 542k^4 + 896k^3 + 1396k^2 + 2068k - 5255$	$12k^7 + 359k^6 + 1416k^5 + 3312k^4 + 6689k^3 + 12258k^2 + 20797k - 44843$
$m = 7$	—	$2k^7 + 7k^6 + 10k^5 + 11k^4 + 12k^3 + 14k^2 + 16k - 72$	$3k^7 + 29k^6 + 48k^5 + 81k^4 + 108k^3 + 150k^2 + 192k - 611$	$8k^7 + 93k^6 + 273k^5 + 531k^4 + 889k^3 + 1393k^2 + 2068k - 5255$	$14k^7 + 358k^6 + 1415k^5 + 3312k^4 + 6689k^3 + 12258k^2 + 20797k - 44843$

Таблиця А.9. Результати обчислення $W(k, l, m, n)$ при $l = 10$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$
$m = 2$	$2k^4 + 2k^3 + 2k^2 + 2k - 8$	$3k^4 + 7k^3 + 11k^2 + 15k - 36$	$5k^4 + 25k^3 + 61k^2 + 113k - 204$	$11k^4 + 84k^3 + 297k^2 + 730k - 1122$
$m = 3$	$k^6 + k^5 + 2k^4 + k^3 + 2k^2 + k - 8$	$3k^6 + 12k^5 + 17k^4 + 18k^3 + 19k^2 + 20k - 89$	$3k^6 + 26k^5 + 70k^4 + 123k^3 + 178k^2 + 237k - 637$	$5k^6 + 72k^5 + 320k^4 + 808k^3 + 1531k^2 + 2465k - 5201$
$m = 4$	$k^7 + 2k^6 + 2k^5 + k^4 + k^3 + k^2 + k - 9$	$k^7 + 6k^6 + 11k^5 + 16k^4 + 17k^3 + 18k^2 + 20k - 89$	$3k^7 + 39k^6 + 88k^5 + 123k^4 + 157k^3 + 198k^2 + 246k - 854$	$4k^7 + 81k^6 + 340k^5 + 766k^4 + 1326k^3 + 2036k^2 + 2924k - 7477$
$m = 5$	—	$3k^7 + 11k^6 + 10k^5 + 15k^4 + 14k^3 + 18k^2 + 18k - 89$	$7k^7 + 41k^6 + 85k^5 + 121k^4 + 156k^3 + 198k^2 + 246k - 854$	$44k^7 + 262k^6 + 554k^5 + 911k^4 + 1406k^3 + 2074k^2 + 2938k - 8189$
$m = 6$	$2k^7 + 2k^6 + k^5 + k^4 + k^3 + k^2 + k - 9$	$k^8 + 8k^7 + 10k^6 + 11k^5 + 12k^4 + 14k^3 + 16k^2 + 18k - 90$	$k^8 + 16k^7 + 49k^6 + 81k^5 + 115k^4 + 152k^3 + 195k^2 + 245k - 854$	$k^8 + 51k^7 + 258k^6 + 551k^5 + 910k^4 + 1406k^3 + 2074k^2 + 2938k - 8189$
$m = 7$	$k^8 + k^7 + 2k^6 + k^5 + k^4 + k^3 + k^2 + k - 9$	—	$3k^8 + 21k^7 + 56k^6 + 75k^5 + 114k^4 + 147k^3 + 195k^2 + 243k - 854$	$4k^8 + 79k^7 + 266k^6 + 533k^5 + 899k^4 + 1399k^3 + 2071k^2 + 2938k - 8189$

А.2. Підрахунок числа нерозкладних $*$ -нееквівалентних унімономіальних зображень

Модифікуємо перший варіант коду, що обчислює число $U(l, n)$ неперіодичних послідовностей $\bar{w} = (s_1, s_2, \dots, s_n)$, кожна з яких найменша в лексикографічному порядку серед собі циклічно еквівалентних, де $s_i \in \{0, 1, \dots, l-1\}$ ($i = 1, 2, \dots, n$) до відшукування числа $X(l, m, n)$ послідовностей $(s_1, s_2, \dots, s_n, \varepsilon)$, $s_i \in \{0, 1, \dots, l-1\}$ $\sum_{j=0}^{m-1} s_{i+j} \geq l$ ($i = 1, \dots, n$), таких, що $(s_1, s_2, \dots, s_n)$ — неперіодична послідовність, найменша в лексикографічному порядку серед її циклічно еквівалентних. В підрозділі 4.4 показано, що число нерозкладних унімономіальних зображень вигляду (4.7) степеня n з точністю до $*$ -еквівалентності циклічної p -групи $H = \langle a \rangle$ порядку m над скінченним локальним кільцем K довжини $l > 1$ не менше числа $X(l, m, n)$. Для зручності ми знаходитимемо $X(l, m, n)$ також у випадку, коли m не є степенем жодного простого числа.

Таким чином обчислити, наприклад, $X(3, 3, 12)$ можна такою серією команд.

```
l:=3;m:=3;n:=12;
  # Формуємо n-у декартову степінь множин {0, 1, ..., l-1}
L:=Cartesian(List([1..n],i->[0..l-1]));;
  # Вибираємо неперіодичні послідовності
M:=Filtered(L,
  f->not(ForAny([1..n-1],i->ForAll([1..n],j->f[j]=f[(j+i-1) mod n+1]))));;
  # Вибираємо послідовності, які генерують зображення
N:=Filtered(M,
  f->ForAll([1..n],i->Sum([0..m-1],j->f[(j+i-1) mod n+1])>=1));
  # Рахуємо кількість класів циклічно еквівалентних послідовностей
Length(N)/n;
```


В результаті обчислень одержуємо $X(3, 3, 12) = 2665$ ($U(3, 12) = 44220$). Подамо результати повторного запуску коду для обчислення $X(l, m, n)$ при деяких значеннях l, m, n таблицями. При незначній зміні m значення $X(l, m, n)$ часто повторюються. Тому для кращої наочності рискою відмічені значення, які повторюють вказані при попередньому m .

Таблица А.10. Результаты обчислення $X(l, m, n)$ при $l = 2$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$	$n = 11$	$n = 12$
$m = 2$	0	0	0	0	0	0	0	0	0	0	0
$m = 3$	—	1	1	1	1	2	2	3	4	6	7
$m = 4$	1	—	2	3	3	6	8	14	20	34	51
$m = 5$	—	—	—	5	6	10	15	27	43	77	125
$m = 6$	—	2	—	—	8	14	21	37	63	115	197
$m = 7$	—	—	—	—	—	17	26	45	77	142	250
$m = 8$	—	—	3	—	—	—	29	51	87	160	284
$m = 9$	—	—	—	—	—	—	—	55	94	172	306
$m = 10$	—	—	—	6	—	—	—	—	98	180	320
$m = 11$	—	—	—	—	—	—	—	—	—	185	329
$m = 12$	—	—	—	—	9	—	—	—	—	—	334
$m = 13$	—	—	—	—	—	—	—	—	—	—	—
$m = 14$	—	—	—	—	—	18	—	—	—	—	—
$m = 15$	—	—	—	—	—	—	—	—	—	—	—
$m = 16$	—	—	—	—	—	—	30	—	—	—	—
$m = 17$	—	—	—	—	—	—	—	—	—	—	—
$m = 18$	—	—	—	—	—	—	—	56	—	—	—

Таблиця А.11. Результати обчислення $X(l, m, n)$ при $l = 3$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$	$n = 11$	$n = 12$
$m = 2$	1	1	1	2	2	4	5	8	11	18	25
$m = 3$	—	5	7	14	27	61	122	265	564	1232	2665
$m = 4$	2	—	15	30	63	157	370	913	2217	5528	13764
$m = 5$	—	6	—	44	92	231	574	1496	3865	10165	26721
$m = 6$	3	7	—	—	112	278	699	1847	4890	13175	35534
$m = 7$	—	—	16	—	—	307	767	2035	5428	14753	40216
$m = 8$	—	—	17	45	—	—	805	2129	5690	15516	42460
$m = 9$	—	8	—	46	—	—	—	2178	5813	15865	43483
$m = 10$	—	—	—	47	113	—	—	—	5874	16022	43930
$m = 11$	—	—	—	—	114	308	—	—	—	16097	44124
$m = 12$	—	—	18	—	115	309	—	—	—	—	44213
$m = 13$	—	—	—	—	—	310	806	—	—	—	—
$m = 14$	—	—	—	—	—	311	807	2179	—	—	—
$m = 15$	—	—	—	48	—	—	808	2180	—	—	—
$m = 16$	—	—	—	—	—	—	809	2181	5875	—	—
$m = 17$	—	—	—	—	—	—	—	2182	5876	16098	—
$m = 18$	—	—	—	—	116	—	—	2183	5877	16099	—

Таблица А.12. Результаты обчислення $X(l, m, n)$ при $l = 4$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$	$n = 11$	$n = 12$
$m = 2$	2	3	5	11	19	41	78	161	322	670	1368
$m = 3$	3	14	27	73	200	583	1649	4853	14303	42713	128248
$m = 4$	5	—	52	142	422	1383	4496	14911	49678	167959	571551
$m = 5$	—	16	—	193	571	1911	6475	22537	78882	279098	993939
$m = 6$	—	19	54	—	657	2185	7488	26410	94059	338961	1229600
$m = 7$	—	—	56	194	—	2323	7937	28119	100691	365098	1333383
$m = 8$	6	—	59	197	—	—	8140	28806	103339	375490	1374483
$m = 9$	—	—	—	199	660	—	—	29096	104332	379362	1389763
$m = 10$	—	—	—	203	663	2325	—	—	104726	380742	1395173
$m = 11$	—	—	—	—	665	2329	8141	—	—	381267	1397026
$m = 12$	—	20	—	—	669	2332	8145	—	—	—	1397703
$m = 13$	—	—	—	—	—	2334	8149	29099	—	—	—
$m = 14$	—	—	—	—	—	2339	8152	29104	104728	—	—
$m = 15$	—	—	—	—	—	—	8154	29108	104733	381268	—
$m = 16$	—	—	60	—	—	—	8159	29111	104738	381272	—
$m = 17$	—	—	—	—	—	—	—	29113	104742	381278	1397706
$m = 18$	—	—	—	—	—	—	—	29119	104745	381283	1397712

Таблица А.13. Результаты обчислення $X(l, m, n)$ при $l = 5$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$	$n = 11$	$n = 12$
$m = 2$	4	7	15	39	90	234	582	1509	3897	10254	27013
$m = 3$	5	29	73	248	876	3184	11560	43140	162185	616348	2360472
$m = 4$	8	30	134	460	1754	7177	29574	123636	521820	2229296	9598346
$m = 5$	—	33	—	599	2280	9552	40820	178143	784715	3490495	15646954
$m = 6$	9	37	138	—	2547	10640	45931	202815	906030	4090691	18611711
$m = 7$	—	—	142	603	—	11113	47919	212378	952801	4321945	19761681
$m = 8$	—	38	147	609	2549	—	48690	215724	969096	4402335	20160487
$m = 9$	—	39	—	614	2557	11114	—	216921	974379	4428307	20289217
$m = 10$	10	—	—	620	2563	11123	—	—	976150	4436259	20328530
$m = 11$	—	—	148	—	2569	11133	48697	—	—	4438796	20340033
$m = 12$	—	—	149	—	2576	11140	48710	216926	—	—	20343551
$m = 13$	—	—	—	621	—	11147	48720	216941	976152	—	—
$m = 14$	—	—	—	622	—	11155	48728	216956	976166	4438797	—
$m = 15$	—	40	—	623	—	—	48736	216966	976185	4438809	—
$m = 16$	—	—	—	—	2577	—	48745	216975	976200	4438831	20343559
$m = 17$	—	—	—	—	2578	—	—	216984	976211	4438852	20343581
$m = 18$	—	—	—	—	2579	11156	—	216994	976221	4438867	20343607

А.3. Підрахунок числа спадково незвідних нееквівалентних унімономіальних зображень

Модифікуємо останній варіант коду, що обчислює число $U(l, n)$ неперіодичних послідовностей $\bar{w} = (s_1, s_2, \dots, s_n)$, кожна з яких найменша в лексикографічному порядку серед собі циклічно еквівалентних, де $s_i \in \{0, 1, \dots, l-1\}$ ($i = 1, 2, \dots, n$) до відшукування числа $Y(k, l, m, n)$ послідовностей $(s_1, \dots, s_n, \varepsilon)$, таких, що $s_i \in \{0, 1, \dots, l-1\}$, $(\sum_{i=1}^n s_i, n) = 1$, $\sum_{i=1}^n s_i < l$, $\sum_{j=0}^{m-1} s_{i+j} \geq l$ ($i = 1, \dots, n$), ε належить множині представників всіх різних суміжних класів $(K/\text{Ann}(t^s))^* = (K/t^{l-s}K)^*$, $s = \max_{i=1}^n (s_i)$, $\bar{w} = (s_1, \dots, s_n)$ — найменша в лексикографічному порядку серед її циклічно еквівалентних. В підрозділі 4.5 показано, що число спадково незвідних нееквівалентних унімономіальних зображень вигляду (4.12) степеня n циклічної p -групи $H = \langle a \rangle$ порядку m над скінченним локальним кільцем K довжини $l > 1$ з порядком $k = |K/\text{Rad } K|$ поля лишків кільця K не менше числа $Y(k, l, m, n)$.

Для зручності ми знаходитимемо $Y(k, l, m, n)$ також у випадку, коли m не є степенем жодного простого числа. Таким чином обчислити $Y(k, 5, 8, 3)$ можна такою послідовністю команд.

```
l:=5;m:=8;n:=3;maxl:=[];maxnuml:=[];k:=Indeterminate(Integers,"k");
P:=Filtered([1..l-1],f->GcdInt(f,n)=1);          # Числа <l в.прості з n
f:=List([1..n], x->0);                            # формуємо послідовність з n нулів
repeat
  if Sum(f) in P then                               # послідовності чиї суми в.прості з n
    if ForAll([1..n],i->Sum([0..m-1],j->f[(j+i-1) mod n+1])>=l) then
      Add(maxl,Maximum(f)); fi;fi;
      # формуємо наступну послідовність з n-ї степені множин {0,...,l-1}
    for i in [1..n] do f[i]:=(f[i]+1)mod l; if f[i]=0 then break;fi;od;
until Sum(f)=0;
```

```

for s in [1..l-1] do Add(maxnuml,Number(maxl,x->x=s)*k^(l-s-1));od;
Print(Sum(maxnuml)*(k-1)/n);           # Враховуємо ц. еквівалентність.

```

В результаті виконання коду одержимо $Y(k, 5, 8, 3) = k^4 + k^3 - k - 1$. Подамо результати повторного запуску коду для обчислення $Y(k, l, t, n)$ при деяких значеннях l, t, n таблицями. При незначній зміні t значення $Y(k, l, t, n)$ часто повторюються. Тому для кращої наочності рискою відмічені значення, які повторюють вказані при попередньому t .

Таблица А.14. Результаты обчислення $Y(k, l, m, n)$ при $l = 3$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$
$m = 2$	0	0	0	0	0	0	0	0	0
$m = 3$	—	—	—	—	—	—	—	—	—
$m = 4$	—	—	—	—	—	—	—	—	—
$m = 5$	—	$k^2 - k$	—	—	—	—	—	—	—
$m = 6$	$k^2 - k$	$k^2 - 1$	—	—	—	—	—	—	—
$m = 7$	—	—	—	—	—	—	—	—	—
$m = 8$	—	—	—	$k^2 - k$	—	—	—	—	—
$m = 9$	—	$2k^2 - k - 1$	—	$2k^2 - 2k$	—	—	—	—	—
$m = 10$	—	—	—	$2k^2 - k - 1$	—	—	—	—	—
$m = 11$	—	—	—	—	—	$k^2 - k$	—	—	—
$m = 12$	—	—	$k^2 - k$	—	—	$2k^2 - 2k$	—	—	—
$m = 13$	—	—	—	—	—	$3k^2 - 3k$	—	—	—
$m = 14$	—	—	—	—	—	$3k^2 - 2k - 1$	—	$k^2 - k$	—
$m = 15$	—	—	—	$3k^2 - 2k - 1$	—	—	—	$2k^2 - 2k$	—
$m = 16$	—	—	—	—	—	—	—	$3k^2 - 3k$	—
$m = 17$	—	—	—	—	—	—	—	$4k^2 - 4k$	—
$m = 18$	—	—	—	—	$k^2 - k$	—	—	$4k^2 - 3k - 1$	—

Таблица А.15. Результаты обчислення $Y(k, l, m, n)$ при $l = 4$

	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$	$n=9$	$n=10$
$m=2$	0	0	0	0	0	0	0	0	0
$m=3$	$k^2 - k$	—	—	—	—	—	—	—	—
$m=4$	$k^2 - 1$	—	—	—	—	—	—	—	—
$m=5$	—	—	—	—	—	—	—	—	—
$m=6$	—	$k^3 - k$	$k^3 - k$	—	—	—	—	—	—
$m=7$	—	—	$k^3 + 2k^2 - 3k$	$k^3 - k^2$	—	—	—	—	—
$m=8$	$k^3 - 1$	—	$k^3 + 2k^2 - 2k - 1$	$2k^3 - 2k$	—	—	—	—	—
$m=9$	—	—	—	$2k^3 + 2k^2 - 4k$	—	—	—	—	—
$m=10$	—	—	—	$4k^3 + k^2 - 4k - 1$	—	$2k^3 - 2k^2$	—	—	—
$m=11$	—	—	—	—	—	$4k^3 - 2k^2 - 2k$	$k^3 - k^2$	—	—
$m=12$	—	$2k^3 - k^2 - k$	—	—	—	$5k^3 - k^2 - 4k$	$4k^3 - 3k^2 - k$	—	—
$m=13$	—	—	—	—	—	$5k^3 + k^2 - 6k$	$6k^3 - 3k^2 - 3k$	—	—
$m=14$	—	—	—	—	—	$8k^3 - k^2 - 6k - 1$	$7k^3 - 2k^2 - 5k$	—	—
								$2k^3$	$2k^2$

Таблица А.16. Результаты обчислення $Y(k, l, m, n)$ при $l = 5$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$m = 2$	0	0	0	0	0	0	0
$m = 3$	—	—	—	—	—	—	—
$m = 4$	$k^3 - k$	$k^3 - k^2$	—	—	—	—	—
$m = 5$	—	$2k^3 - 2k$	—	—	—	—	—
$m = 6$	—	$2k^3 - k - 1$	—	—	—	—	—
$m = 7$	—	—	$k^4 - k^3$	$k^4 + 2k^3 - 3k^2$	—	—	—
$m = 8$	—	$k^4 + k^3 - k - 1$	$k^4 + 2k^3 - 2k^2 - k$	$k^4 + 6k^3 - 5k^2 - 2k$	—	—	—
$m = 9$	—	$k^4 + 2k^3 - k^2 - k - 1$	—	$3k^4 + 5k^3 - 4k^2 - 4k$	—	$k^4 - k^3$	—
$m = 10$	$k^4 - k$	—	—	$3k^4 + 9k^3 - 7k^2 - 4k - 1$	—	$4k^4 + 2k^3 - 6k^2$	—
$m = 11$	—	—	—	—	—	$5k^4 + 8k^3 - 11k^2 - 2k$	—
$m = 12$	—	—	—	—	—	$6k^4 + 11k^3 - 13k^2 - 4k$	—
$m = 13$	—	—	—	$4k^4 + 8k^3 - 7k^2 - 4k - 1$	—	$10k^4 + 8k^3 - 12k^2 - 6k$	—
$m = 14$	—	—	—	$5k^4 + 7k^3 - 7k^2 - 4k - 1$	—	$10k^4 + 14k^3 - 17k^2 - 6k - 1$	$2k^4 - 2k^3$

Таблица А.17. Результаты обчислення $Y(k, l, m, n)$ при $l = 6$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$m = 2$	0	0	0	0	0	0	0
$m = 3$	$k^3 - k$	—	—	—	—	—	—
$m = 4$	$k^4 + k^3 - k^2 - 1$	$k^4 - k^2$	—	—	—	—	—
$m = 5$	—	$3k^4 - k^2 - 2k$	$k^4 - k^3$	—	—	—	—
$m = 6$	—	$3k^4 + 2k^3 - 2k^2 - 2k - 1$	$4k^4 - 3k^2 - k$	—	—	—	—
$m = 7$	—	—	$4k^4 + 2k^3 - 3k^2 - 3k$	—	—	—	—
$m = 8$	—	—	$k^5 + 6k^4 - 4k^2 - 2k - 1$	$k^5 + k^4 - 2k^3$	$k^5 + 6k^4 - 6k^3 - k^2$	—	—
$m = 9$	—	$k^5 + 3k^4 + k^3 - 2k^2 - 2k - 1$	—	$k^5 + 7k^4 - 8k^3$	$k^5 + 16k^4 - 9k^3 - 7k^2 - k$	$2k^5 + 2k^4 - 4k^3$	—
$m = 10$	—	—	—	$3k^5 + 9k^4 - 7k^3 - 4k^2 - k$	$k^5 + 19k^4 - 7k^3 - 10k^2 - 3k$	$3k^5 + 19k^4 - 16k^3 - 6k^2$	$2k^5 - k^4 - k^3$

Таблица А.18. Результаты обчислення $Y(k, l, m, n)$ при $l = 7$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$m = 2$	0	0	0	0	0	0	0
$m = 3$	$k^4 - k^3$	—	—	—	—	—	—
$m = 4$	$k^4 - k$	—	—	—	—	—	—
$m = 5$	$k^5 - k$	$k^5 + 2k^4 - 3k^3$	—	—	—	—	—
$m = 6$	$k^5 + k^4 - k^3 - k$	$3k^5 + 2k^4 - 2k^3 - 2k^2 - k$	$2k^5 - k^4 - k^3$	$k^5 - k^4$	—	—	—
$m = 7$	—	—	$4k^5 + 2k^4 - 6k^3$	$8k^5 + 2k^4 - 7k^3 - 3k^2$	—	—	—
$m = 8$	—	—	$4k^5 + 2k^4 - 3k^3 - 2k^2 - k$	$9k^5 + 8k^4 - 9k^3 - 6k^2 - 2k$	—	—	—
$m = 9$	—	—	—	$k^6 + 8k^5 + 9k^4 - 8k^3 - 6k^2 - 4k$	$k^6 + 4k^5 - 4k^4 - k^3$	$k^6 + 15k^5 - 12k^4 - 4k^3$	—
$m = 10$	—	—	$k^6 + 4k^5 + k^4 - 3k^3 - 2k^2 - k$	$k^6 + 16k^5 + 5k^4 - 11k^3 - 7k^2 - 3k - 1$	$k^6 + 15k^5 - 10k^4 - 6k^3$	$2k^6 + 39k^5 - 13k^4 - 22k^3 - 6k^2$	—

Таблиця А.19. Результати обчислення $Y(k, l, m, n)$ при $l = 8$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$
$m = 2$	0	0	0	0	0	0
$m = 3$	$k^4 - k$	—	—	—	—	—
$m = 4$	$k^5 + k^4 - k^2 - 1$	$2k^5 - k^3 - k^2$	—	—	—	—
$m = 5$	—	$k^6 + k^5 + 2k^4 - k^3 - k^2 - 2k$	$k^6 + 2k^5 - 2k^4 - k^3$	—	—	—
$m = 6$	$k^6 + k^5 - k^2 - 1$	$3k^6 + 4k^5 - 3k^3 - 2k^2 - k - 1$	$k^6 + 8k^5 - k^4 - 4k^3 - 3k^2 - k$	$2k^6 - k^5 - k^4$	—	—
$m = 7$	—	—	$5k^6 + 4k^5 + k^4 - 4k^3 - 3k^2 - 3k$	$9k^6 + 10k^5 - 9k^4 - 7k^3 - 3k^2$	$k^6 - k^5$	—
$m = 8$	—	—	$5k^6 + 10k^5 - 2k^4 - 6k^3 - 4k^2 - 2k - 1$	$15k^6 + 21k^5 - 15k^4 - 13k^3 - 6k^2 - 2k$	$17k^6 + 8k^5 - 17k^4 - 7k^3 - k^2$	—
$m = 9$	—	—	—	$15k^6 + 28k^5 - 13k^4 - 20k^3 - 6k^2 - 4k$	$21k^6 + 28k^5 - 24k^4 - 17k^3 - 7k^2 - k$	—
$m = 10$	—	—	—	$k^7 + 22k^6 + 24k^5 - 16k^4 - 17k^3 - 9k^2 - 4k - 1$	$k^7 + 22k^6 + 32k^5 - 22k^4 - 20k^3 - 10k^2 - 3k$	$k^7 + 11k^6 - 12k^5$

Таблица А.20. Результаты обчислення $Y(k, l, m, n)$ при $l = 9$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$
$m = 2$	0	0	0	0	0	0
$m = 3$	$k^5 - k^3$	—	—	—	—	—
$m = 4$	$k^6 + k^5 - k^3 - k$	$2k^6 + k^5 - k^4 - k^3 - k^2$	—	—	—	—
$m = 5$	—	$3k^6 + 5k^5 - k^4 - 4k^3 - k^2 - 2k$	—	—	—	—
$m = 6$	$k^7 + k^6 - k^3 - k$	$k^7 + 5k^6 + 4k^5 - 2k^4 - 3k^3 - 2k^2 - 2k - 1$	$k^7 + 6k^6 - 3k^5 - 3k^4 - k^3$	$2k^7 + 2k^6 - 3k^5 - k^4$	—	—
$m = 7$	—	$2k^7 + 4k^6 + 4k^5 - 2k^4 - 3k^3 - 2k^2 - 2k - 1$	$k^7 + 8k^6 + k^5 - 4k^4 - 6k^3$	$7k^7 + 24k^6 - 9k^5 - 12k^4 - 7k^3 - 3k^2$	—	—
$m = 8$	—	$3k^7 + 5k^6 + 2k^5 - 2k^4 - 3k^3 - 2k^2 - 2k - 1$	$5k^7 + 10k^6 - 2k^5 - 6k^4 - 4k^3 - 2k^2 - k$	$13k^7 + 40k^6 - 9k^5 - 23k^4 - 13k^3 - 6k^2 - 2k$	$3k^7 - 2k^6 - k^5$	$k^7 - k^6$
$m = 9$	—	$3k^7 + 5k^6 + 3k^5 - 3k^4 - 3k^3 - 2k^2 - 2k - 1$	—	$18k^7 + 53k^6 - 18k^5 - 23k^4 - 20k^3 - 6k^2 - 4k$	$18k^7 + 10k^6 - 20k^5 - 7k^4 - k^3$	$37k^7 + 27k^6 - 42k^5 - 18k^4 - 4k^3$

Таблиця А.21. Результати обчислення $Y(k, l, m, n)$ при $l = 10$

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$
$m = 2$	0	0	0	0	0	0
$m = 3$	$k^6 - k$	—	—	—	—	—
$m = 4$	$k^7 + k^6 + k^5 - k^4 - k^2 - 1$	$k^7 - k^5$	—	—	—	—
$m = 5$	—	$3k^7 + 5k^6 - 4k^5 - k^4 - 3k^3$	$4k^7 + 2k^6 - 3k^5 - 2k^4 - k^3$	—	—	—
$m = 6$	—	$k^8 + 5k^7 + 4k^6 - 2k^5 - 3k^4 - 2k^3 - 2k^2 - k$	$k^8 + 6k^7 + 9k^6 - 3k^5 - 5k^4 - 4k^3 - 3k^2 - k$	$k^8 + 7k^7 - 4k^6 - 3k^5 - k^4$	—	—
$m = 7$	$k^8 + k^6 + k^5 - k^4 - k^2 - 1$	—	$k^8 + 13k^7 + 11k^6 - 10k^5 - 5k^4 - 4k^3 - 3k^2 - 3k$	$4k^8 + 35k^7 + 4k^6 - 21k^5 - 12k^4 - 7k^3 - 3k^2$	—	—
$m = 8$	$k^8 + k^7 + k^5 - k^4 - k^2 - 1$	$3k^8 + 3k^7 + 4k^6 - 2k^5 - 3k^4 - 2k^3 - 2k^2 - k$	$5k^8 + 15k^7 + 8k^6 - 6k^5 - 9k^4 - 6k^3 - 4k^2 - 2k - 1$	$10k^8 + 55k^7 + 11k^6 - 31k^5 - 24k^4 - 13k^3 - 6k^2 - 2k$	—	$3k^8 - 2k^7 - k^6$

ДОДАТОК Б. ОБЧИСЛЕННЯ ОДИНИЦЬ СКІНЧЕННОГО ПОРЯДКУ ЦІЛОЧИСЛОВОГО ГРУПОВОГО КІЛЬЦЯ ГРУПИ $PSL(3, 4)$

Задамо групу $G = PSL(3, 4)$ командами системи GAP 4.10.1, перевіримо її простоту та підрахуємо її порядок $|G|$ та експоненту $\#G$, розклавши обидва ці числа на прості множники.

```
gap> G:=PSL(3,4);
Group([ ( 3, 4, 5)( 7, 9, 8)(10,14,18)(11,17,20)(12,15,21)(13,16,19),
  ( 1, 2, 6, 7,11, 3,10)( 4,14, 8,15,16,20,13)( 5,18, 9,19,21,17,12) ])
gap> IsSimple(G);
true
gap> Size(G);
20160
gap> PrintFactorsInt(Size(G));
2^6*3^2*5*7
gap> ExpG:=Exponent(G);
420
gap> PrintFactorsInt(ExpG);
2^2*3*5*7
```

Таким чином

$$|G| = 20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7,$$

$$\text{Exp}(G) = 420 = 2^2 \cdot 3 \cdot 5 \cdot 7.$$

Розіб'ємо елементи групи G класи спряжених елементів та знайдемо порядки елементів та число елементів у кожному.

```
gap> CC:=ConjugacyClasses(G);
[ ()^G, (2,6)(3,7)(4,8)(5,9)(14,18)(15,21)(16,19)(17,20)^G,
  (1,3,10,6)(2,7)(4,17,14,8)(5,20,18,9)(12,16,13,21)(15,19)^G,
  (1,4,10,6)(2,8)(3,21,18,7)(5,15,14,9)(11,19,13,17)(16,20)^G,
```



```

(1,5,10,6)(2,9)(3,16,14,7)(4,19,18,8)(11,15,12,20)(17,21)^G,
(1,3,11,10,7,2,6)(4,16,12,17,15,18,8)(5,21,13,20,19,14,9)^G,
(1,6,2,7,10,11,3)(4,8,18,15,17,12,16)(5,9,14,19,20,13,21)^G,
(1,4,3,5,2)(7,12,16,15,10)(8,17,21,20,14)(9,19,11,13,18)^G,
(1,5,4,2,3)(7,15,12,10,16)(8,20,17,14,21)(9,13,19,18,11)^G,
(3,4,5)(7,9,8)(10,14,18)(11,17,20)(12,15,21)(13,16,19)^G ]
gap> List( CC,x->[Order(Representative(x)),Size(x)]);
[ [ 1, 1 ], [ 2, 315 ], [ 4, 1260 ], [ 4, 1260 ], [ 4, 1260 ],
  [ 7, 2880 ], [ 7, 2880 ], [ 5, 4032 ], [ 5, 4032 ], [ 3, 2240 ] ]

```

Таким чином група G володіє 10-ма класами спряжених елементів.

Позначення класу	Порядки елементів	Число елементів
$1a$	1	1
$2a$	2	315
$3a$	3	2240
$4a$	4	1260
$4b$	4	1260
$4c$	4	1260
$5a$	5	4032
$5b$	5	4032
$7a$	7	2880
$7b$	7	2880

Перший символ позначення — порядок кожного елементу в класі, а другий — послідовна літера латинського алфавіту.

Для відшукування одиниць скінченного порядку шукаємо таблицю характеристик командою `CharacterTable`.

```

gap> tbl:=CharacterTable( "PSL(3,4)" );
CharacterTable( "L3(4)" )
gap> Display(tbl);

```

L3(4)

2	6	6	.	4	4	4	.	.	.	.
3	2	.	2	.	.	.	.	.	.	.
5	1	.	.	.	.	.	1	1	.	.
7	1	.	.	.	.	.	.	.	1	1

	1a	2a	3a	4a	4b	4c	5a	5b	7a	7b
2P	1a	1a	3a	2a	2a	2a	5b	5a	7a	7b
3P	1a	2a	1a	4a	4b	4c	5b	5a	7b	7a
5P	1a	2a	3a	4a	4b	4c	1a	1a	7b	7a
7P	1a	2a	3a	4a	4b	4c	5b	5a	1a	1a

X.1	1	1	1	1	1	1	1	1	1	1
X.2	20	4	2	.	.	.	.	.	-1	-1
X.3	35	3	-1	3	-1	-1	.	.	.	.
X.4	35	3	-1	-1	3	-1	.	.	.	.
X.5	35	3	-1	-1	-1	3	.	.	.	.
X.6	45	-3	.	1	1	1	.	.	B	/B
X.7	45	-3	.	1	1	1	.	.	/B	B
X.8	63	-1	.	-1	-1	-1	A	*A	.	.
X.9	63	-1	.	-1	-1	-1	*A	A	.	.
X.10	64	.	1	.	.	.	-1	-1	1	1

$$A = -E(5) - E(5)^4$$

$$= (1 - \sqrt{5})/2 = -b_5$$

$$B = E(7) + E(7)^2 + E(7)^4$$

$$= (-1 + \sqrt{-7})/2 = b_7$$

Таким чином таблиця характерів має вигляд:

Таблиця Б.1. Таблиця характерів $PSL(3, 4)$ ($p = 0$), де $A = -\alpha - \alpha^4$, $B = \zeta + \zeta^2 + \zeta^4$, $\alpha = e^{\frac{2\pi i}{5}}$ і $\zeta = e^{\frac{2\pi i}{7}}$

	1a	2a	3a	4a	4b	4c	5a	5b	7a	7b
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	20	4	2	0	0	0	0	0	-1	-1
χ_3	35	3	-1	3	-1	-1	0	0	0	0
χ_4	35	3	-1	-1	3	-1	0	0	0	0
χ_5	35	3	-1	-1	-1	3	0	0	0	0
χ_6	45	-3	0	1	1	1	0	0	B	$\overline{B}$
χ_7	45	-3	0	1	1	1	0	0	$\overline{B}$	B
χ_8	63	-1	0	-1	-1	-1	A	A^*	0	0
χ_9	63	-1	0	-1	-1	-1	A^*	A	0	0
χ_{10}	64	0	1	0	0	0	-1	-1	1	1

Тут $\overline{B} = \zeta^3 + \zeta^5 + \zeta^6$ — комплексно спряжений елемент до B , $A^* = -\alpha^2 - \alpha^3$.

Знайдемо таблицю характерів Брауера групи $PSL(3,4)$, що відповідають простому числу $p = 2$, за допомогою команд.

```
gap> tblmod2:= CharacterTable( "PSL(3,4)" ) mod 2;
BrauerTable( "L3(4)", 2 )
gap> Display(tblmod2);
L3(4)mod2
```

```

2  6  .  .  .  .  .
3  2  2  .  .  .  .
5  1  .  1  1  .  .
7  1  .  .  .  1  1
```

```

1a 3a 5a 5b 7a 7b
2P 1a 3a 5b 5a 7a 7b
3P 1a 1a 5b 5a 7b 7a
5P 1a 3a 1a 1a 7b 7a
7P 1a 3a 5b 5a 1a 1a
```

X.1	1	1	1	1	1	1
X.2	8	-1	A	*A	1	1
X.3	8	-1	*A	A	1	1
X.4	9	.	-1	-1	B	/B
X.5	9	.	-1	-1	/B	B
X.6	64	1	-1	-1	1	1

$$A = -E(5) - E(5)^4$$

$$= (1 - \sqrt{5})/2 = -b_5$$

$$B = 2E(7) + 2E(7)^2 + E(7)^3 + 2E(7)^4 + E(7)^5 + E(7)^6$$

$$= (-3 + \sqrt{-7})/2 = -1 + b_7$$

Таким чином таблиця характерів Брауера має вигляд:

Таблиця Б.2. Таблиця характерів $PSL(3, 4)$ ($p = 2$), де $A = -\alpha - \alpha^4$, $B = \zeta + \zeta^2 + \zeta^4$, $\alpha = e^{\frac{2\pi i}{5}}$ і $\zeta = e^{\frac{2\pi i}{7}}$

	$1a$	$3a$	$5a$	$5b$	$7a$	$7b$
χ_1	1	1	1	1	1	1
χ_2	8	-1	A	A*	1	1
χ_3	8	-1	A*	A	1	1
χ_4	9	0	-1	-1	B	$\overline{B}$
χ_5	9	0	-1	-1	$\overline{B}$	B
χ_6	64	1	-1	-1	1	1

Знайдемо таблицю характерів Брауера групи $PSL(3, 4)$, що відповідають простому числу $p = 2$, за допомогою команд.

```
gap> tblmod3:= CharacterTable( "PSL(3,4)" ) mod 3;
```

```
BrauerTable( "L3(4)", 3 )
```

```
gap> Display(tblmod3);
```

```
L3(4)mod3
```

2	6	6	4	4	4	.	.	.	.
3	2	.	.	.	.	.	.	.	.

```

5  1  .  .  .  .  1  1  .  .
7  1  .  .  .  .  .  .  1  1

```

```

      1a 2a 4a 4b 4c 5a 5b 7a 7b
2P 1a 1a 2a 2a 2a 5b 5a 7a 7b
3P 1a 2a 4a 4b 4c 5b 5a 7b 7a
5P 1a 2a 4a 4b 4c 1a 1a 7b 7a
7P 1a 2a 4a 4b 4c 5b 5a 1a 1a

```

```

X.1      1  1  1  1  1  1  1  1  1
X.2     15 -1  3 -1 -1  .  .  1  1
X.3     15 -1 -1  3 -1  .  .  1  1
X.4     15 -1 -1 -1  3  .  .  1  1
X.5     19  3 -1 -1 -1 -1 -1 -2 -2
X.6     45 -3  1  1  1  .  .  B /B
X.7     45 -3  1  1  1  .  . /B  B
X.8     63 -1 -1 -1 -1  A *A  .  .
X.9     63 -1 -1 -1 -1 *A  A  .  .

```

```

A = -E(5)-E(5)^4
   = (1-Sqrt(5))/2 = -b5
B = E(7)+E(7)^2+E(7)^4
   = (-1+Sqrt(-7))/2 = b7

```

Таким чином таблиця характерів Брауера має вигляд:

Таблиця Б.3. Таблиця характерів $PSL(3, 4)$ ($p = 3$), де $A = -\alpha - \alpha^4$, $B = \zeta + \zeta^2 + \zeta^4$, $\alpha = e^{\frac{2\pi i}{5}}$ і $\zeta = e^{\frac{2\pi i}{7}}$

	$1a$	$2a$	$4a$	$4b$	$4c$	$5a$	$5b$	$7a$	$7b$
χ_1	1	1	1	1	1	1	1	1	1
χ_2	15	-1	3	-1	-1	0	0	1	1
χ_3	15	-1	-1	3	-1	0	0	1	1
χ_4	15	-1	-1	-1	3	0	0	1	1
χ_5	19	3	-1	-1	-1	-1	-1	-2	-2
χ_6	45	-3	1	1	1	0	0	B	$\overline{B}$
χ_7	45	-3	1	1	1	0	0	$\overline{B}$	B
χ_8	63	-1	-1	-1	-1	A	A^*	0	0
χ_9	63	-1	-1	-1	-1	A^*	A	0	0

ДОДАТОК В. ЗНАХОДЖЕННЯ РОЗШИРЕНИХ БІНАРНИХ КОДІВ ГОЛЕЯ ЗА ГРУПОВИМ КІЛЬЦЕМ СКІНЧЕННИХ ГРУП ПОРЯДКУ 24

Знайдемо, з точністю до ізоморфізму, групи 24-го порядку командами системи GAP 4.10.1 та підрахуємо їх кількість.

```
gap> GroupList:=AllSmallGroups(24);;
gap> Size(GroupList);
15
```

Отже, існує 15 груп, з точністю до ізоморфізму, 24-го порядку. Опишемо ці групи за допомогою коду.

```
gap> for G in GroupList do
> Print(StructureDescription(G),", ");
> od;
C3 : C8, C24, SL(2,3), C3 : Q8, C4 x S3, D24, C2 x (C3 : C4), (C6 x C2) : C2,
C12 x C2, C3 x D8, C3 x Q8, S4, C2 x A4, C2 x C2 x S3, C6 x C2 x C2,
```

Таким чином групи порядку 24 вичерпуються групами

$$\begin{array}{ccccccccc}
 C_3 \rtimes C_8, & C_{24}, & SL(2,3), & C_3 \rtimes Q_8, & C_4 \times S_3, \\
 D_{24}, & C_2 \times (C_3 \rtimes C_4), & (C_6 \times C_2) \rtimes C_2, & C_{12} \times C_2, & C_3 \times D_8, \\
 C_3 \times Q_8, & S_4, & C_2 \times A_4, & C_2 \times C_2 \times S_3, & C_6 \times C_2 \times C_2.
 \end{array}$$

Задамо тепер групу Матьє M_{24} та з'ясуємо її порядок.

```
gap> M24:=MathieuGroup(24);
Group([ (1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23),
(3,17,10,7,9)(4,13,14,19,5)(8,18,11,12,23)(15,20,22,21,16),
(1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17)
(13,22)(15,19) ])
gap> Size(M24);
244823040
gap> PrintFactorsInt(Size(M24));
2^10*3^3*5*7*11*23
```

Список підгруп порядку 24 групи Матьє M_{24} можна отримати таким КОДОМ.

```
gap> SubgroupsList:=Filtered(
>      List(ConjugacyClassesSubgroups(M24),Representative),
>      x->Order(x)=24);
[ Group([ (1,9)(2,8,21,18)(3,11,15,22)(4,13)(5,7)(6,24,10,20)(12,16)
(14,19,23,17), (1,12)(2,8,18,21)(3,11,22,15)(4,13)(5,16)(6,24,20,10)
(7,9)(14,19,17,23) ]), Group([ (1,18,13)(2,3,22)(4,17,5)(6,21,14)
(7,10,16)(8,23,11)(9,15,12) (19,20,24), (1,18,19,20)(2,12)
(3,22,9,15)(4,17,6,21)(5,14)(7,10,8,23)(11,16)(13,24) ]),
.....

Group([ (1,21,12,4,20,16)(2,8,18,14,19,10)(3,17,24,6,15,11)
(5,9,23,13,7,22), (1,17,13,19,20,11,9,18,12,6,22,2)
(3,21,14,7,15,16,8,23,24,4,10,5) ]), Group([ (1,21)(2,20)(3,24)(4,13)
(5,23)(6,11)(7,17)(8,15)(9,16)(10,14)(12,18)(19,22), (1,2,17,18)
(3,12,5,10)(4,20,16,11)(6,19,14,8)(7,13,15,23)(9,21,24,22) ] ) ]
```

Знайдемо описання цих підгруп за допомогою коду.

```
gap> SubgroupsDescription:=List(SubgroupsList,StructureDescription);
[ "S4", "S4", "S4", "S4", "S4", "S4", "S4", "C2 x A4", "S4", "C2 x A4",
"C2 x A4", "C2 x A4", "S4", "C2 x C2 x S3", "C2 x C2 x S3",
"C2 x C2 x S3", "C2 x C2 x S3", "S4", "S4", "C2 x A4", "C2 x A4",
"C2 x A4", "C2 x A4", "C2 x A4", "S4", "C2 x A4", "SL(2,3)", "S4",
"C2 x A4", "C2 x A4", "C2 x A4", "C2 x A4", "S4", "SL(2,3)", "SL(2,3)",
"S4", "(C6 x C2) : C2", "C2 x A4", "S4", "S4", "S4", "(C6 x C2) : C2",
"(C6 x C2) : C2", "(C6 x C2) : C2", "C4 x S3", "D24", "D24", "C4 x S3",
"C3 x D8", "C3 x D8", "S4" ]
```

Сформуємо також список груп 24-го порядку, які ізоморфні підгрупам порядку 24 групи Матьє M_{24} і, отже, мають з ними однаковий опис.


```

gap> SmallGroupList:=Filtered(
>   GroupList,x->ForAny(SubgroupsDescription, y->StructureDescription(x)=y));
[ SL(2,3), C4 x S3, D24, (C6 x C2) : C2, C3 x D8, S4, C2 x A4,
  C2 x C2 x S3 ]
gap> Size(SmallGroupList);
8

```

Таким чином існує 8 груп, з точністю до ізоморфізму, порядку 24, які ізоморфні деяким підгрупам групи Матьє M_{24} :

$$\begin{array}{ccccccc}
 SL(2,3), & C_4 \times S_3, & D_{24}, & (C_6 \times C_2) \rtimes C_2, \\
 C_3 \times D_8, & S_4, & C_2 \times A_4, & C_2 \times C_2 \times S_3.
 \end{array}$$

Для кожної «малої» скінченної групи G в системі GAP передбачено індекс i в списку неізоморфних груп заданого порядку n , які можна одержати командою `IdGroup(G)`, що поверне список $[n, i]$. Обернений доступ одержуємо, наприклад, `AllSmallGroups(n)[i]` або `SmallGroup(n, i)`, що поверне групу ізоморфну G . Знайдемо індекс перерахованих груп в списку неізоморфних груп порядку 24 в системі GAP.

```

gap> SmallIdGroupList:=List(SmallGroupList,x->IdGroup(x)[2]);
[ 3, 5, 6, 8, 10, 12, 13, 14 ]
gap> for i in SmallIdGroupList do
>   Print("(" , i, ") ", StructureDescription(SmallGroup(24, i)), ", ");
> od;
(3) SL(2,3), (5) C4 x S3, (6) D24, (8) (C6 x C2) : C2, (10) C3 x D8,
(12) S4, (13) C2 x A4, (14) C2 x C2 x S3,

```

В.1. Знаходження кодів за групою $SL(2, 3)$

з'ясуємо інформацію, що стосується побудови розширених бінарних самодуальних кодів Голея за груповим кільцем групи $SL(2, 3)$. Групу можна визначити як $SL(2, 3) = \langle x, y \mid x^3 = y^3 = (xy)^2 \rangle$.

```

gap> G:=SmallGroup(24,3);;StructureDescription(G);
"SL(2,3)"
gap> f:=FreeGroup(2);
<free group on the generators [ f1, f2 ]>
gap> H:=f/[f.1^3*f.2^(-3),f.1*f.2*f.1*f.2*f.2^(-3)];
<fp group on the generators [ f1, f2 ]>
gap> IsomorphismGroups(H,G);
[ f1, f2 ] -> [ f1^2*f3, f1*f2*f4 ]

```

Образами символів x, y у $SL(2, 3)$ будуть матриці

$$x = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}, \quad y = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

```

gap> G:=SL(2,3);
SL(2,3)
gap> IsomorphismGroups(SmallGroup(24,3),G);
[ f1, f2, f3, f4 ] -> [ [ [ 0*Z(3), Z(3)^0 ], [ Z(3), Z(3) ] ],
  [ [ Z(3), Z(3) ], [ Z(3), Z(3)^0 ] ],
  [ [ 0*Z(3), Z(3) ], [ Z(3)^0, 0*Z(3) ] ],
  [ [ Z(3), 0*Z(3) ], [ 0*Z(3), Z(3) ] ] ]
gap> x:=[[Z(3),0*Z(3)],[Z(3)^0,Z(3)]];x in G;
true
gap> y:=[[Z(3),Z(3)^0],[0*Z(3),Z(3)]];y in G;
true
gap> H:=Group(x,y);
Group([ [ [ Z(3), 0*Z(3) ], [ Z(3)^0, Z(3) ] ],
  [ [ Z(3), Z(3)^0 ], [ 0*Z(3), Z(3) ] ] ])
gap> H=G;
true
gap> Ie:=[[Z(3)^0,0*Z(3)],[0*Z(3),Z(3)^0]];Ie in G;
true
gap> x^3=y^3;x^3=(x*y)^2;
true
true

```

Задамо порядок елементів на групі $SL(2, 3)$ порядку 24, та перевіримо, що вказані елементи при визначені порядку не повторюються.

```
gap> g:=[
>   1e,      x,      x^2,      x^3,      x^4,      x^5,
>   y,      x*y,     x^2*y,     x^3*y,     x^4*y,     x^5*y,
>   y^2,     x*y^2,   x^2*y^2,   x^3*y^2,   x^4*y^2,   x^5*y^2,
>   y^2*x,   x*y^2*x, x^2*y^2*x, x^3*y^2*x, x^4*y^2*x, x^5*y^2*x
> ];;
gap> Length(Set(g));
24
```

Знайдемо матрицю індексів дії регулярного зображення σ на довільному елементі

$$\begin{aligned}
 v = & \alpha_1 + \alpha_2 x + \alpha_3 x^2 + \alpha_4 x^3 + \alpha_5 x^4 + \alpha_6 x^5, \\
 & \alpha_7 y + \alpha_8 xy + \alpha_9 x^2 y + \alpha_{10} x^3 y + \alpha_{11} x^4 y + \alpha_{12} x^5 y, \\
 & \alpha_{13} y^2 + \alpha_{14} xy^2 + \alpha_{15} x^2 y^2 + \alpha_{16} x^3 y^2 + \alpha_{17} x^4 y^2 + \alpha_{18} x^5 y^2, \\
 & \alpha_{19} y^2 x + \alpha_{20} xy^2 x + \alpha_{21} x^2 y^2 x + \alpha_{22} x^3 y^2 x + \alpha_{23} x^4 y^2 x + \alpha_{24} x^5 y^2 x
 \end{aligned}$$

групового кільця $\mathbb{F}_2 SL(2, 3)$, що відповідає порядку обернених елементів до вказаних.

```
gap> Sg:=[];;
gap> for i in g do
>   A:=[];
>   for j in g do
>     Add(A,Position(g,i^(-1)*j));od;
>   Add(Sg,A);od;
gap> Sg;
[ [ 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 ],
  [ 6,1,2,3,4,5,12,7,8,9,10,11,18,13,14,15,16,17,24,19,20,21,22,23 ],
  [ 5,6,1,2,3,4,11,12,7,8,9,10,17,18,13,14,15,16,23,24,19,20,21,22 ],
  [ 4,5,6,1,2,3,10,11,12,7,8,9,16,17,18,13,14,15,22,23,24,19,20,21 ],
```

```
[ 3,4,5,6,1,2,9,10,11,12,7,8,15,16,17,18,13,14,21,22,23,24,19,20 ],
[ 2,3,4,5,6,1,8,9,10,11,12,7,14,15,16,17,18,13,20,21,22,23,24,19 ],
[ 16,22,8,13,19,11,1,21,14,4,24,17,7,20,5,10,23,2,18,12,6,15,9,3 ],
[ 11,16,22,8,13,19,17,1,21,14,4,24,2,7,20,5,10,23,3,18,12,6,15,9 ],
[ 19,11,16,22,8,13,24,17,1,21,14,4,23,2,7,20,5,10,9,3,18,12,6,15 ],
[ 13,19,11,16,22,8,4,24,17,1,21,14,10,23,2,7,20,5,15,9,3,18,12,6 ],
[ 8,13,19,11,16,22,14,4,24,17,1,21,5,10,23,2,7,20,6,15,9,3,18,12 ],
[ 22,8,13,19,11,16,21,14,4,24,17,1,20,5,10,23,2,7,12,6,15,9,3,18 ],
[ 10,15,21,7,18,24,16,6,20,13,3,23,1,12,19,4,9,22,2,17,11,5,14,8 ],
[ 24,10,15,21,7,18,23,16,6,20,13,3,22,1,12,19,4,9,8,2,17,11,5,14 ],
[ 18,24,10,15,21,7,3,23,16,6,20,13,9,22,1,12,19,4,14,8,2,17,11,5 ],
[ 7,18,24,10,15,21,13,3,23,16,6,20,4,9,22,1,12,19,5,14,8,2,17,11 ],
[ 21,7,18,24,10,15,20,13,3,23,16,6,19,4,9,22,1,12,11,5,14,8,2,17 ],
[ 15,21,7,18,24,10,6,20,13,3,23,16,12,19,4,9,22,1,17,11,5,14,8,2 ],
[ 9,14,20,12,17,23,15,5,19,18,2,22,6,11,24,3,8,21,1,16,10,4,13,7 ],
[ 23,9,14,20,12,17,22,15,5,19,18,2,21,6,11,24,3,8,7,1,16,10,4,13 ],
[ 17,23,9,14,20,12,2,22,15,5,19,18,8,21,6,11,24,3,13,7,1,16,10,4 ],
[ 12,17,23,9,14,20,18,2,22,15,5,19,3,8,21,6,11,24,4,13,7,1,16,10 ],
[ 20,12,17,23,9,14,19,18,2,22,15,5,24,3,8,21,6,11,10,4,13,7,1,16 ],
[ 14,20,12,17,23,9,5,19,18,2,22,15,11,24,3,8,21,6,16,10,4,13,7,1 ] ]
```

З допомогою подальшого коду з'ясовуємо, коли матриця $\sigma(v)$ буде симетрична ($\sigma(v) = \sigma(v)^T$).

```
gap> SymSg:=List([1..24],i->List([1..24],j->Sg[i][j]));;
gap> for i in [1..24] do
> for j in [1..24] do
> if Sg[i][j]>Sg[j][i] then
> dat:=true;
> for ki in [1..24] do
> for kj in [1..24] do
> if SymSg[ki][kj]=Sg[i][j] then
> if dat then Print("a",Sg[i][j],"=a",Sg[j][i]," ", " "); fi;
> dat:=false;
> SymSg[ki][kj]:=Sg[j][i];
> fi;
```

```

> od;od;
> fi;
> od;od;
a5=a3, a6=a2, a11=a8, a13=a10, a16=a7, a18=a15,
a19=a9, a21=a17, a22=a12, a23=a20, a24=a14,
gap> SymSg;
[ [ 1,2,3,4,3,2,7,8,9,10,8,12,10,14,15,7,17,15,9,20,17,12,20,14 ],
  [ 2,1,2,3,4,3,12,7,8,9,10,8,15,10,14,15,7,17,14,9,20,17,12,20 ],
  [ 3,2,1,2,3,4,8,12,7,8,9,10,17,15,10,14,15,7,20,14,9,20,17,12 ],
  [ 4,3,2,1,2,3,10,8,12,7,8,9,7,17,15,10,14,15,12,20,14,9,20,17 ],
  [ 3,4,3,2,1,2,9,10,8,12,7,8,15,7,17,15,10,14,17,12,20,14,9,20 ],
  [ 2,3,4,3,2,1,8,9,10,8,12,7,14,15,7,17,15,10,20,17,12,20,14,9 ],
  [ 7,12,8,10,9,8,1,17,14,4,14,17,7,20,3,10,20,2,15,12,2,15,9,3 ],
  [ 8,7,12,8,10,9,17,1,17,14,4,14,2,7,20,3,10,20,3,15,12,2,15,9 ],
  [ 9,8,7,12,8,10,14,17,1,17,14,4,20,2,7,20,3,10,9,3,15,12,2,15 ],
  [ 10,9,8,7,12,8,4,14,17,1,17,14,10,20,2,7,20,3,15,9,3,15,12,2 ],
  [ 8,10,9,8,7,12,14,4,14,17,1,17,3,10,20,2,7,20,2,15,9,3,15,12 ],
  [ 12,8,10,9,8,7,17,14,4,14,17,1,20,3,10,20,2,7,12,2,15,9,3,15 ],
  [ 10,15,17,7,15,14,7,2,20,10,3,20,1,12,9,4,9,12,2,17,8,3,14,8 ],
  [ 14,10,15,17,7,15,20,7,2,20,10,3,12,1,12,9,4,9,8,2,17,8,3,14 ],
  [ 15,14,10,15,17,7,3,20,7,2,20,10,9,12,1,12,9,4,14,8,2,17,8,3 ],
  [ 7,15,14,10,15,17,10,3,20,7,2,20,4,9,12,1,12,9,3,14,8,2,17,8 ],
  [ 17,7,15,14,10,15,20,10,3,20,7,2,9,4,9,12,1,12,8,3,14,8,2,17 ],
  [ 15,17,7,15,14,10,2,20,10,3,20,7,12,9,4,9,12,1,17,8,3,14,8,2 ],
  [ 9,14,20,12,17,20,15,3,9,15,2,12,2,8,14,3,8,17,1,7,10,4,10,7 ],
  [ 20,9,14,20,12,17,12,15,3,9,15,2,17,2,8,14,3,8,7,1,7,10,4,10 ],
  [ 17,20,9,14,20,12,2,12,15,3,9,15,8,17,2,8,14,3,10,7,1,7,10,4 ],
  [ 12,17,20,9,14,20,15,2,12,15,3,9,3,8,17,2,8,14,4,10,7,1,7,10 ],
  [ 20,12,17,20,9,14,9,15,2,12,15,3,14,3,8,17,2,8,10,4,10,7,1,7 ],
  [ 14,20,12,17,20,9,3,9,15,2,12,15,8,14,3,8,17,2,7,10,4,10,7,1 ] ]

```

Остання матриця вказує вигляд індексів у симетричній матриці $\sigma(v)$ після замін: $\alpha_5 = \alpha_3$, $\alpha_6 = \alpha_2$, $\alpha_{11} = \alpha_8$, $\alpha_{13} = \alpha_{10}$, $\alpha_{16} = \alpha_7$, $\alpha_{18} = \alpha_{15}$, $\alpha_{19} = \alpha_9$, $\alpha_{21} = \alpha_{17}$, $\alpha_{22} = \alpha_{12}$, $\alpha_{23} = \alpha_{20}$, $\alpha_{24} = \alpha_{14}$.

Задамо поле з двох елементів нульову матрицю над ним для подаль-

ших перевірок та підгрузимо пакет для роботи з кодами в GAP.

```
gap> F:=GF(2);
GF(2)
gap> ZM:=List([1..24],i->List([1..24],j->Zero(F)));;
LoadPackage("GUAVA");
```

Наступний код шукатиме всі лінійні коди породженні $\sigma(v)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $Rank(\sigma(\alpha)) = 12$ та обчисленнями командами пакету GUAVA шукатиме їх мінімальну відстань.

```
gap> i:=0;;DistList:=[];;
gap> for a1 in F do
> for a2 in F do
> for a3 in F do
> for a4 in F do
> for a7 in F do
> for a8 in F do
> for a9 in F do
> for a10 in F do
> for a12 in F do
> for a14 in F do
> for a15 in F do
> for a17 in F do
> for a20 in F do
> SgM:=
> [a1,a2,a3,a4,a3,a2,a7,a8,a9,a10,a8,a12,
a10,a14,a15,a7,a17,a15,a9,a20,a17,a12,a20,a14],
> [a2,a1,a2,a3,a4,a3,a12,a7,a8,a9,a10,a8,
a15,a10,a14,a15,a7,a17,a14,a9,a20,a17,a12,a20],
> [a3,a2,a1,a2,a3,a4,a8,a12,a7,a8,a9,a10,
a17,a15,a10,a14,a15,a7,a20,a14,a9,a20,a17,a12],
> [a4,a3,a2,a1,a2,a3,a10,a8,a12,a7,a8,a9,
a7,a17,a15,a10,a14,a15,a12,a20,a14,a9,a20,a17],
> [a3,a4,a3,a2,a1,a2,a9,a10,a8,a12,a7,a8,
```

```

a15,a7,a17,a15,a10,a14,a17,a12,a20,a14,a9,a20],
> [a2,a3,a4,a3,a2,a1,a8,a9,a10,a8,a12,a7,
a14,a15,a7,a17,a15,a10,a20,a17,a12,a20,a14,a9],
> [a7,a12,a8,a10,a9,a8,a1,a17,a14,a4,a14,
a17,a7,a20,a3,a10,a20,a2,a15,a12,a2,a15,a9,a3],
> [a8,a7,a12,a8,a10,a9,a17,a1,a17,a14,a4,a14,
a2,a7,a20,a3,a10,a20,a3,a15,a12,a2,a15,a9],
> [a9,a8,a7,a12,a8,a10,a14,a17,a1,a17,a14,a4,
a20,a2,a7,a20,a3,a10,a9,a3,a15,a12,a2,a15],
> [a10,a9,a8,a7,a12,a8,a4,a14,a17,a1,a17,a14,
a10,a20,a2,a7,a20,a3,a15,a9,a3,a15,a12,a2],
> [a8,a10,a9,a8,a7,a12,a14,a4,a14,a17,a1,a17,
a3,a10,a20,a2,a7,a20,a2,a15,a9,a3,a15,a12],
> [a12,a8,a10,a9,a8,a7,a17,a14,a4,a14,a17,a1,
a20,a3,a10,a20,a2,a7,a12,a2,a15,a9,a3,a15],
> [a10,a15,a17,a7,a15,a14,a7,a2,a20,a10,a3,a20,
a1,a12,a9,a4,a9,a12,a2,a17,a8,a3,a14,a8],
> [a14,a10,a15,a17,a7,a15,a20,a7,a2,a20,a10,a3,
a12,a1,a12,a9,a4,a9,a8,a2,a17,a8,a3,a14],
> [a15,a14,a10,a15,a17,a7,a3,a20,a7,a2,a20,a10,
a9,a12,a1,a12,a9,a4,a14,a8,a2,a17,a8,a3],
> [a7,a15,a14,a10,a15,a17,a10,a3,a20,a7,a2,a20,
a4,a9,a12,a1,a12,a9,a3,a14,a8,a2,a17,a8],
> [a17,a7,a15,a14,a10,a15,a20,a10,a3,a20,a7,a2,
a9,a4,a9,a12,a1,a12,a8,a3,a14,a8,a2,a17],
> [a15,a17,a7,a15,a14,a10,a2,a20,a10,a3,a20,a7,
a12,a9,a4,a9,a12,a1,a17,a8,a3,a14,a8,a2],
> [a9,a14,a20,a12,a17,a20,a15,a3,a9,a15,a2,a12,
a2,a8,a14,a3,a8,a17,a1,a7,a10,a4,a10,a7],
> [a20,a9,a14,a20,a12,a17,a12,a15,a3,a9,a15,a2,
a17,a2,a8,a14,a3,a8,a7,a1,a7,a10,a4,a10],
> [a17,a20,a9,a14,a20,a12,a2,a12,a15,a3,a9,a15,
a8,a17,a2,a8,a14,a3,a10,a7,a1,a7,a10,a4],
> [a12,a17,a20,a9,a14,a20,a15,a2,a12,a15,a3,a9,
a3,a8,a17,a2,a8,a14,a4,a10,a7,a1,a7,a10],

```

```

> [a20,a12,a17,a20,a9,a14,a9,a15,a2,a12,a15,a3,
      a14,a3,a8,a17,a2,a8,a10,a4,a10,a7,a1,a7],
> [a14,a20,a12,a17,a20,a9,a3,a9,a15,a2,a12,a15,
      a8,a14,a3,a8,a17,a2,a7,a10,a4,a10,a7,a1]
> ];
> if SgM^2=ZM then
>   if RankMat(SgM)=12 then
>     i:=i+1;C:= GeneratorMatCode( SgM, GF(2) );
>     m:=Minimum(List(AsSSortedList(C){[2..Size(C)]}, WeightCodeword ));
>     Add(DistList,m);
>     Print(i,"-",m,"-",Codeword(SgM[1]),"\n");
> fi;fi;
> od;od;od;od;od;od;od;od;od;od;od;od;od;od;
1-2-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 ]
2-2-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 ]
3-2-[ 0 0 0 0 0 0 0 0 1 0 0 1 0 1 0 0 1 0 1 1 1 1 1 ]
4-2-[ 0 0 0 0 0 0 0 0 1 0 0 1 0 1 1 0 1 1 1 0 1 1 0 ]
5-2-[ 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 ]

.....

60-2-[ 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 ]
61-2-[ 1 1 1 1 1 1 1 1 0 1 1 0 1 0 0 1 0 0 0 1 0 0 1 0 ]
62-2-[ 1 1 1 1 1 1 1 1 0 1 1 0 1 0 1 1 0 1 0 0 0 0 0 ]
63-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 ]
64-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 ]
gap> Collected(DistList);
[ [ 2, 64 ] ]

```

Таким чином є 64 елементів $v \in \mathbb{F}_2 SL(2, 3)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $Rank(\sigma(\alpha)) = 12$, а з лінійних кодів породжених $\sigma(v)$ $[24, 12, 2]$ -кодів є 64 і нема **жодного** $[24, 12, 8]$ -коду.

В.2. Знаходження кодів за групою $C_4 \times S_3$

З'ясуємо інформацію, що стосується побудови розширених бінарних самодуальних кодів Голея за груповим кільцем групи $C_4 \times S_3$. Групу можна визначити як $C_4 \times S_3 = \langle x, y, z \mid x^4 = y^3 = z^2 = 1, yx = xy, zx = xz, zy = y^{-1}z \rangle$.

```
gap> G:=SmallGroup(24,5);;StructureDescription(G);
"C4 x S3"
gap> f:=FreeGroup(3);
<free group on the generators [ f1, f2, f3 ]>
gap> H:=f/[f.1^4,f.2^3,f.3^2,
  f.1*f.2*f.1^3*f.2^2,f.1*f.3*f.1^3*f.3,f.2*f.3*f.2*f.3];
<fp group on the generators [ f1, f2, f3 ]>
gap> IsomorphismGroups(H,G);
[ f1, f2, f3 ] -> [ f2, f4, f1*f3*f4 ]
```

Образами символів x, y, z у S_{24} будуть, наприклад, підстановки

$$x = (1, 2, 3, 4), \quad y = (5, 6, 7), \quad z = (5, 6).$$

```
gap> x:=(1,2,3,4);;
gap> y:=(5,6,7);;
gap> z:=(5,6);;
gap> Ie:=();;
gap> x^4=Ie;y^3=Ie;z^2=Ie;
true
true
true
gap> x*y=y*x;x*z=z*x;z*y=y^(-1)*z;
true
true
true
gap> H:=Group(x,y,z);
```

```

Group([ (1,2,3,4), (5,6,7), (5,6) ])
gap> IsomorphismGroups(H,G);
[ (1,2,3,4), (5,6,7), (5,6) ] -> [ f2, f4, f1*f4 ]

```

Нам буде зручно вибрати іншу систему твірних: $a = xy$, z .

```

gap> a:=x*y;
(1,2,3,4)(5,6,7)
gap> a^12=Ie;
true
gap> z*a=a^5*z;
true
gap> H:=Group(a,z);
Group([ (1,2,3,4)(5,6,7), (5,6) ])
gap> IsomorphismGroups(H,G);
[ (1,2,3,4)(5,6,7), (5,6) ] -> [ f2*f4, f1*f4 ]

```

Отже, a, z задовольняє співвідношенням: $a^{12} = z^2 = 1$, $za = a^5z$ і ці співвідношення визначають групу $C_4 \times S_3$.

```

gap> f:=FreeGroup(2);
<free group on the generators [ f1, f2 ]>
gap> H:=f/[f.1^12,f.2^2,f.2*f.1*f.2*f.1^7];
<fp group on the generators [ f1, f2 ]>
gap> IsomorphismGroups(H,G);
[ f1, f2 ] -> [ f2*f3*f4, f1*f3*f4^2 ]

```

Задамо порядок елементів на групі $C_4 \times S_3$ порядку 24, та перевіримо, що вказані елементи при визначені порядку не повторюються.

```

gap> g:=
> Ie,a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^10, a^11,
> z,a*z,a^2*z,a^3*z,a^4*z,a^5*z,a^6*z,a^7*z,a^8*z,a^9*z,a^10*z,a^11*z
> ];;
gap> Length(Set(g));
24

```

Знайдемо матрицю індексів дії регулярного зображення σ на довільному елементі

$$v = \alpha_1 + \alpha_2 a + \alpha_3 a^2 + \alpha_4 a^3 + \alpha_5 a^4 + \alpha_6 a^5 + \alpha_7 a^6 + \\ \alpha_8 a^7 + \alpha_9 a^8 + \alpha_{10} a^9 + \alpha_{11} a^{10} + \alpha_{12} a^{11} + \\ \alpha_{13} z + \alpha_{14} a z + \alpha_{15} a^2 z + \alpha_{16} a^3 z + \alpha_{17} a^4 z + \alpha_{18} a^5 z + \alpha_{19} a^6 z + \\ \alpha_{20} a^7 z + \alpha_{21} a^8 z + \alpha_{22} a^9 z + \alpha_{23} a^{10} z + \alpha_{24} a^{11} z$$

групового кільця $\mathbb{F}_2(C_4 \times S_3)$, що відповідає порядку обернених елементів до вказаних.

```
gap> for i in g do
> A:=[];
> for j in g do
> Add(A,Position(g,i^(-1)*j));od;
> Add(Sg,A);od;
gap> Sg;
[ [ 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 ],
[ 12,1,2,3,4,5,6,7,8,9,10,11,24,13,14,15,16,17,18,19,20,21,22,23 ],
[ 11,12,1,2,3,4,5,6,7,8,9,10,23,24,13,14,15,16,17,18,19,20,21,22 ],
[ 10,11,12,1,2,3,4,5,6,7,8,9,22,23,24,13,14,15,16,17,18,19,20,21 ],
[ 9,10,11,12,1,2,3,4,5,6,7,8,21,22,23,24,13,14,15,16,17,18,19,20 ],
[ 8,9,10,11,12,1,2,3,4,5,6,7,20,21,22,23,24,13,14,15,16,17,18,19 ],
[ 7,8,9,10,11,12,1,2,3,4,5,6,19,20,21,22,23,24,13,14,15,16,17,18 ],
[ 6,7,8,9,10,11,12,1,2,3,4,5,18,19,20,21,22,23,24,13,14,15,16,17 ],
[ 5,6,7,8,9,10,11,12,1,2,3,4,17,18,19,20,21,22,23,24,13,14,15,16 ],
[ 4,5,6,7,8,9,10,11,12,1,2,3,16,17,18,19,20,21,22,23,24,13,14,15 ],
[ 3,4,5,6,7,8,9,10,11,12,1,2,15,16,17,18,19,20,21,22,23,24,13,14 ],
[ 2,3,4,5,6,7,8,9,10,11,12,1,14,15,16,17,18,19,20,21,22,23,24,13 ],
[ 13,18,23,16,21,14,19,24,17,22,15,20,1,6,11,4,9,2,7,12,5,10,3,8 ],
[ 20,13,18,23,16,21,14,19,24,17,22,15,8,1,6,11,4,9,2,7,12,5,10,3 ],
[ 15,20,13,18,23,16,21,14,19,24,17,22,3,8,1,6,11,4,9,2,7,12,5,10 ],
[ 22,15,20,13,18,23,16,21,14,19,24,17,10,3,8,1,6,11,4,9,2,7,12,5 ],
[ 17,22,15,20,13,18,23,16,21,14,19,24,5,10,3,8,1,6,11,4,9,2,7,12 ],
[ 24,17,22,15,20,13,18,23,16,21,14,19,12,5,10,3,8,1,6,11,4,9,2,7 ],
```

```
[ 19,24,17,22,15,20,13,18,23,16,21,14,7,12,5,10,3,8,1,6,11,4,9,2 ],
[ 14,19,24,17,22,15,20,13,18,23,16,21,2,7,12,5,10,3,8,1,6,11,4,9 ],
[ 21,14,19,24,17,22,15,20,13,18,23,16,9,2,7,12,5,10,3,8,1,6,11,4 ],
[ 16,21,14,19,24,17,22,15,20,13,18,23,4,9,2,7,12,5,10,3,8,1,6,11 ],
[ 23,16,21,14,19,24,17,22,15,20,13,18,11,4,9,2,7,12,5,10,3,8,1,6 ],
[ 18,23,16,21,14,19,24,17,22,15,20,13,6,11,4,9,2,7,12,5,10,3,8,1 ] ]
```

З допомогою подальшого коду з'ясуємо, коли матриця $\sigma(v)$ буде симетрична ($\sigma(v) = \sigma(v)^T$).

```
gap> SymSg:=List([1..24],i->List([1..24],j->Sg[i][j]));;
gap> for i in [1..24] do
> for j in [1..24] do
> if Sg[i][j]>Sg[j][i] then
> dat:=true;
> for ki in [1..24] do
> for kj in [1..24] do
> if SymSg[ki][kj]=Sg[i][j] then
> if dat then Print("a",Sg[i][j],"=a",Sg[j][i]," "); fi;
> dat:=false;
> SymSg[ki][kj]:=Sg[j][i];
> fi;
> od;od;
> fi;
> od;od;
a8=a6, a9=a5, a10=a4, a11=a3, a12=a2, a20=a14, a22=a16, a24=a18,
gap> SymSg;
[ [ 1,2,3,4,5,6,7,6,5,4,3,2,13,14,15,16,17,18,19,14,21,16,23,18 ],
[ 2,1,2,3,4,5,6,7,6,5,4,3,18,13,14,15,16,17,18,19,14,21,16,23 ],
[ 3,2,1,2,3,4,5,6,7,6,5,4,23,18,13,14,15,16,17,18,19,14,21,16 ],
[ 4,3,2,1,2,3,4,5,6,7,6,5,16,23,18,13,14,15,16,17,18,19,14,21 ],
[ 5,4,3,2,1,2,3,4,5,6,7,6,21,16,23,18,13,14,15,16,17,18,19,14 ],
[ 6,5,4,3,2,1,2,3,4,5,6,7,14,21,16,23,18,13,14,15,16,17,18,19 ],
[ 7,6,5,4,3,2,1,2,3,4,5,6,19,14,21,16,23,18,13,14,15,16,17,18 ],
[ 6,7,6,5,4,3,2,1,2,3,4,5,18,19,14,21,16,23,18,13,14,15,16,17 ],
[ 5,6,7,6,5,4,3,2,1,2,3,4,17,18,19,14,21,16,23,18,13,14,15,16 ],
```

[4,5,6,7,6,5,4,3,2,1,2,3,16,17,18,19,14,21,16,23,18,13,14,15],
 [3,4,5,6,7,6,5,4,3,2,1,2,15,16,17,18,19,14,21,16,23,18,13,14],
 [2,3,4,5,6,7,6,5,4,3,2,1,14,15,16,17,18,19,14,21,16,23,18,13],
 [13,18,23,16,21,14,19,18,17,16,15,14,1,6,3,4,5,2,7,2,5,4,3,6],
 [14,13,18,23,16,21,14,19,18,17,16,15,6,1,6,3,4,5,2,7,2,5,4,3],
 [15,14,13,18,23,16,21,14,19,18,17,16,3,6,1,6,3,4,5,2,7,2,5,4],
 [16,15,14,13,18,23,16,21,14,19,18,17,4,3,6,1,6,3,4,5,2,7,2,5],
 [17,16,15,14,13,18,23,16,21,14,19,18,5,4,3,6,1,6,3,4,5,2,7,2],
 [18,17,16,15,14,13,18,23,16,21,14,19,2,5,4,3,6,1,6,3,4,5,2,7],
 [19,18,17,16,15,14,13,18,23,16,21,14,7,2,5,4,3,6,1,6,3,4,5,2],
 [14,19,18,17,16,15,14,13,18,23,16,21,2,7,2,5,4,3,6,1,6,3,4,5],
 [21,14,19,18,17,16,15,14,13,18,23,16,5,2,7,2,5,4,3,6,1,6,3,4],
 [16,21,14,19,18,17,16,15,14,13,18,23,4,5,2,7,2,5,4,3,6,1,6,3],
 [23,16,21,14,19,18,17,16,15,14,13,18,3,4,5,2,7,2,5,4,3,6,1,6],
 [18,23,16,21,14,19,18,17,16,15,14,13,6,3,4,5,2,7,2,5,4,3,6,1]]

Остання матриця вказує вигляд індексів у симетричній матриці $\sigma(v)$ після замін: $\alpha_8 = \alpha_6$, $\alpha_9 = \alpha_5$, $\alpha_{10} = \alpha_4$, $\alpha_{11} = \alpha_3$, $\alpha_{12} = \alpha_2$, $\alpha_{20} = \alpha_{14}$, $\alpha_{22} = \alpha_{16}$, $\alpha_{24} = \alpha_{18}$.

Далі використаємо умови

$$\left\{ \begin{array}{l} \alpha_6 = \alpha_2, \\ \alpha_{23} = \alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{17} + \alpha_{19} + \alpha_{21}, \\ (\alpha_1 + \alpha_7)(\alpha_{16} + \alpha_{18}) + (\alpha_{13} + \alpha_{19})(\alpha_{14} + \alpha_{16}) + (\alpha_{15} + \alpha_{21})(\alpha_{14} + \alpha_{18}) = 0, \\ \alpha_3^2 + \alpha_5^2 + \alpha_{19}^2 + \alpha_{15}^2 + (\alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{17} + \alpha_{21})(\alpha_{15} + \alpha_{19}) + \alpha_{15}\alpha_{19} + \\ \alpha_{13}\alpha_{17} + \alpha_{13}\alpha_{21} + \alpha_{17}\alpha_{21} = 0, \\ (\alpha_{13} + \alpha_{19})(\alpha_{14} + \alpha_{18}) + (\alpha_{15} + \alpha_{21})(\alpha_{14} + \alpha_{16}) + \\ (\alpha_1 + \alpha_7 + \alpha_{13} + \alpha_{15} + \alpha_{19} + \alpha_{21})(\alpha_{16} + \alpha_{18}) = 0, \end{array} \right.$$

які еквівалентні умові $\sigma(\kappa_2)^2 = 0_{24 \times 24}$, за аналізам здійсненим у під-розділі 7.2.2 формула 7.6.

Наступний код шукатиме всі лінійні коди породженні $\sigma(v)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $Rank(\sigma(\alpha)) = 12$ та обчисленнями командами

пакету GUAVA шукатиме їх мінімальну відстань.

```

pap> i:=0;;DistList:=[];;
> for a1 in F do
> for a3 in F do
> for a4 in F do
> for a5 in F do
> for a5 in F do
> for a6 in F do
> for a7 in F do
> for a13 in F do
> for a14 in F do
> for a15 in F do
> for a16 in F do
> for a17 in F do
> for a18 in F do
> for a19 in F do
> for a21 in F do
> a6:=a2;
> a23:=a1+a7+a13+a15+a17+a19+a21;
> if (a1+a7)*(a16+a18)+(a13+a19)*(a14+a16)+(a15+a21)*(a14+a18)=Zero(F) then
> if a3+a5+a19+a15+(a1+a7+a13+a17+a21)*(a15+a19)+a15*a19+a13*a17+
                                a13*a21+a17*a21=Zero(F) then
> if (a13+a19)*(a14+a18)+(a15+a21)*(a14+a16)+
                                (a1+a7+a13+a15+a19+a21)*(a16+a18)=Zero(F) then
> SgM:=[
> [a1,a2,a3,a4,a5,a6,a7,a6,a5,a4,a3,a2,
                                a13,a14,a15,a16,a17,a18,a19,a14,a21,a16,a23,a18],
> [a2,a1,a2,a3,a4,a5,a6,a7,a6,a5,a4,a3,
                                a18,a13,a14,a15,a16,a17,a18,a19,a14,a21,a16,a23],
> [a3,a2,a1,a2,a3,a4,a5,a6,a7,a6,a5,a4,
                                a23,a18,a13,a14,a15,a16,a17,a18,a19,a14,a21,a16],
> [a4,a3,a2,a1,a2,a3,a4,a5,a6,a7,a6,a5,
                                a16,a23,a18,a13,a14,a15,a16,a17,a18,a19,a14,a21],
> [a5,a4,a3,a2,a1,a2,a3,a4,a5,a6,a7,a6,
                                a21,a16,a23,a18,a13,a14,a15,a16,a17,a18,a19,a14],

```

```

> [a6,a5,a4,a3,a2,a1,a2,a3,a4,a5,a6,a7,
    a14,a21,a16,a23,a18,a13,a14,a15,a16,a17,a18,a19],
> [a7,a6,a5,a4,a3,a2,a1,a2,a3,a4,a5,a6,
    a19,a14,a21,a16,a23,a18,a13,a14,a15,a16,a17,a18],
> [a6,a7,a6,a5,a4,a3,a2,a1,a2,a3,a4,a5,
    a18,a19,a14,a21,a16,a23,a18,a13,a14,a15,a16,a17],
> [a5,a6,a7,a6,a5,a4,a3,a2,a1,a2,a3,a4,
    a17,a18,a19,a14,a21,a16,a23,a18,a13,a14,a15,a16],
> [a4,a5,a6,a7,a6,a5,a4,a3,a2,a1,a2,a3,
    a16,a17,a18,a19,a14,a21,a16,a23,a18,a13,a14,a15],
> [a3,a4,a5,a6,a7,a6,a5,a4,a3,a2,a1,a2,
    a15,a16,a17,a18,a19,a14,a21,a16,a23,a18,a13,a14],
> [a2,a3,a4,a5,a6,a7,a6,a5,a4,a3,a2,a1,
    a14,a15,a16,a17,a18,a19,a14,a21,a16,a23,a18,a13],
> [a13,a18,a23,a16,a21,a14,a19,a18,a17,a16,a15,a14,
    a1,a6,a3,a4,a5,a2,a7,a2,a5,a4,a3,a6],
> [a14,a13,a18,a23,a16,a21,a14,a19,a18,a17,a16,a15,
    a6,a1,a6,a3,a4,a5,a2,a7,a2,a5,a4,a3],
> [a15,a14,a13,a18,a23,a16,a21,a14,a19,a18,a17,a16,
    a3,a6,a1,a6,a3,a4,a5,a2,a7,a2,a5,a4],
> [a16,a15,a14,a13,a18,a23,a16,a21,a14,a19,a18,a17,
    a4,a3,a6,a1,a6,a3,a4,a5,a2,a7,a2,a5],
> [a17,a16,a15,a14,a13,a18,a23,a16,a21,a14,a19,a18,
    a5,a4,a3,a6,a1,a6,a3,a4,a5,a2,a7,a2],
> [a18,a17,a16,a15,a14,a13,a18,a23,a16,a21,a14,a19,
    a2,a5,a4,a3,a6,a1,a6,a3,a4,a5,a2,a7],
> [a19,a18,a17,a16,a15,a14,a13,a18,a23,a16,a21,a14,
    a7,a2,a5,a4,a3,a6,a1,a6,a3,a4,a5,a2],
> [a14,a19,a18,a17,a16,a15,a14,a13,a18,a23,a16,a21,
    a2,a7,a2,a5,a4,a3,a6,a1,a6,a3,a4,a5],
> [a21,a14,a19,a18,a17,a16,a15,a14,a13,a18,a23,a16,
    a5,a2,a7,a2,a5,a4,a3,a6,a1,a6,a3,a4],
> [a16,a21,a14,a19,a18,a17,a16,a15,a14,a13,a18,a23,
    a4,a5,a2,a7,a2,a5,a4,a3,a6,a1,a6,a3],
> [a23,a16,a21,a14,a19,a18,a17,a16,a15,a14,a13,a18,

```

```

a3,a4,a5,a2,a7,a2,a5,a4,a3,a6,a1,a6],
> [a18,a23,a16,a21,a14,a19,a18,a17,a16,a15,a14,a13,
a6,a3,a4,a5,a2,a7,a2,a5,a4,a3,a6,a1]
> ];
> if RankMat(SgM)=12 then
> i:=i+1;C:= GeneratorMatCode( SgM, GF(2) );
> m:=Minimum(List(AsSSortedList(C){[2..Size(C)]}, WeightCodeword ));
> Add(DistList,m);
> Print(i,"-",m,"-",Codeword(SgM[1]),"\n");
> fi;fi;fi;fi;
> od;od;od;od;od;od;od;od;od;od;od;od;od;od;od;od;
1-2-[ 0 1 0 0 0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 0 0 1 1 1 ]
2-2-[ 0 1 0 0 0 1 0 1 0 0 0 1 0 0 1 1 1 0 0 0 1 1 1 0 ]
3-2-[ 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 ]
4-2-[ 0 1 0 0 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 1 1 1 0 0 ]
5-2-[ 0 1 0 0 0 1 0 1 0 0 0 1 1 0 0 0 1 1 1 0 0 0 1 1 ]
.....
1916-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 0 1 1 0 1 0 0 ]
1917-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 ]
1918-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 0 1 1 ]
1919-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 0 1 ]
1920-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 0 ]
gap> Collected(DistList);
[ [ 2, 352 ], [ 4, 1568 ] ]

```

Таким чином є 1920 елементів $v \in \mathbb{F}_2(C_4 \times S_3)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$ а з лінійних кодів породжених $\sigma(v)$ $[24, 12, 2]$ -кодів є 352, $[24, 12, 4]$ -кодів є 1568 і нема **жодного** $[24, 12, 8]$ -коду.

В.3. Знаходження кодів за групою $(C_6 \times C_2) \rtimes C_2$

З'ясуємо інформацію, що стосується побудови розширених бінарних самодуальних кодів Голя за груповим кільцем групи $(C_6 \times C_2) \rtimes C_2$. Групу

МОЖНА ВИЗНАЧИТИ ЯК $(C_6 \times C_2) \rtimes C_2 = \langle x, y, z \mid x^3 = y^4 = z^2 = 1, yz = zy^3, xy = yx^2, xz = zx \rangle$.

```
gap> G:=SmallGroup(24,8);;StructureDescription(G);
"(C6 x C2) : C2"
gap> f:=FreeGroup(3);
<free group on the generators [ f1, f2, f3 ]>
gap> H:=f/[f.1^3,f.2^4,f.3^2,
>          f.2*f.3*f.2*f.3,f.1*f.2*f.1*f.2^3,f.1*f.3*f.1^2*f.3];
<fp group on the generators [ f1, f2, f3 ]>
gap> IsomorphismGroups(H,G);
[ f1, f2, f3 ] -> [ f4, f1*f2, f2 ]
```

Образами символів x, y, z у S_{24} будуть, наприклад, підстановки

$$x = (1, 2, 3)(4, 5, 6), \quad y = (2, 3)(5, 6)(7, 8, 9, 10), \quad z = (8, 10).$$

```
gap> x:=(1,2,3)(4,5,6);;
gap> y:=(2,3)(5,6)(7,8,9,10);;
gap> z:=(8,10);;
gap> Ie:=();;
gap> x^3=Ie;y^4=Ie;z^2=Ie;
true
true
true
gap> y*z=z*y^3;x*y=y*x^2;x*z=z*x;
true
true
true
gap> H:=Group(x,y,z);
Group([ (1,2,3)(4,5,6), (2,3)(5,6)(7,8,9,10), (8,10) ])
gap> IsomorphismGroups(H,G);
[ (1,2,3)(4,5,6), (2,3)(5,6)(7,8,9,10), (8,10) ] -> [ f4, f1*f2*f3*f4^2, f2*f3 ]
```

Задамо порядок елементів на групі $(C_6 \times C_2) \rtimes C_2$ порядку 24, та перевіriamo, що вказані елементи при визначенні порядку не повторюються.

```

gap> g:=
> 1e,      y,      y^2,      y^3,
> x,      x*y,      x*y^2,      x*y^3,
> x^2,      x^2*y,      x^2*y^2,      x^2*y^3,
> z,      y*z,      y^2*z,      y^3*z,
> x*z,      x*y*z,      x*y^2*z,      x*y^3*z,
> x^2*z, x^2*y*z, x^2*y^2*z, x^2*y^3*z
> ];;
gap> Length(Set(g));
24

```

Знайдемо матрицю індексів дії регулярного зображення σ на довільному елементі

$$\begin{aligned}
 v = & \alpha_1 + \alpha_2 y + \alpha_3 y^2 + \alpha_4 y^3 + \\
 & \alpha_5 x + \alpha_6 xy + \alpha_7 xy^2 + \alpha_8 xy^3 + \\
 & \alpha_9 x^2 + \alpha_{10} x^2 y + \alpha_{11} x^2 y^2 + \alpha_{12} x^2 y^3 + \\
 & \alpha_{13} z + \alpha_{14} yz + \alpha_{15} y^2 z + \alpha_{16} y^3 z + \\
 & \alpha_{17} xz + \alpha_{18} xyz + \alpha_{19} xy^2 z + \alpha_{20} xy^3 z + \\
 & \alpha_{21} x^2 z + \alpha_{22} x^2 yz + \alpha_{23} x^2 y^2 z + \alpha_{24} x^2 y^3 z
 \end{aligned}$$

групового кільця $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$, що відповідає порядку обернених елементів до вказаних.

```

gap> for i in g do
> A:=[];
> for j in g do
> Add(A,Position(g,i^(-1)*j));od;
> Add(Sg,A);od;
gap> Sg;
[ [ 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 ],
  [ 4,1,2,3,12,9,10,11,8,5,6,7,16,13,14,15,24,21,22,23,20,17,18,19 ],
  [ 3,4,1,2,7,8,5,6,11,12,9,10,15,16,13,14,19,20,17,18,23,24,21,22 ],

```

```

[ 2,3,4,1,10,11,12,9,6,7,8,5,14,15,16,13,22,23,24,21,18,19,20,17 ],
[ 9,10,11,12,1,2,3,4,5,6,7,8,21,22,23,24,13,14,15,16,17,18,19,20 ],
[ 8,5,6,7,4,1,2,3,12,9,10,11,20,17,18,19,16,13,14,15,24,21,22,23 ],
[ 11,12,9,10,3,4,1,2,7,8,5,6,23,24,21,22,15,16,13,14,19,20,17,18 ],
[ 6,7,8,5,2,3,4,1,10,11,12,9,18,19,20,17,14,15,16,13,22,23,24,21 ],
[ 5,6,7,8,9,10,11,12,1,2,3,4,17,18,19,20,21,22,23,24,13,14,15,16 ],
[ 12,9,10,11,8,5,6,7,4,1,2,3,24,21,22,23,20,17,18,19,16,13,14,15 ],
[ 7,8,5,6,11,12,9,10,3,4,1,2,19,20,17,18,23,24,21,22,15,16,13,14 ],
[ 10,11,12,9,6,7,8,5,2,3,4,1,22,23,24,21,18,19,20,17,14,15,16,13 ],
[ 13,16,15,14,17,20,19,18,21,24,23,22,1,4,3,2,5,8,7,6,9,12,11,10 ],
[ 14,13,16,15,22,21,24,23,18,17,20,19,2,1,4,3,10,9,12,11,6,5,8,7 ],
[ 15,14,13,16,19,18,17,20,23,22,21,24,3,2,1,4,7,6,5,8,11,10,9,12 ],
[ 16,15,14,13,24,23,22,21,20,19,18,17,4,3,2,1,12,11,10,9,8,7,6,5 ],
[ 21,24,23,22,13,16,15,14,17,20,19,18,9,12,11,10,1,4,3,2,5,8,7,6 ],
[ 18,17,20,19,14,13,16,15,22,21,24,23,6,5,8,7,2,1,4,3,10,9,12,11 ],
[ 23,22,21,24,15,14,13,16,19,18,17,20,11,10,9,12,3,2,1,4,7,6,5,8 ],
[ 20,19,18,17,16,15,14,13,24,23,22,21,8,7,6,5,4,3,2,1,12,11,10,9 ],
[ 17,20,19,18,21,24,23,22,13,16,15,14,5,8,7,6,9,12,11,10,1,4,3,2 ],
[ 22,21,24,23,18,17,20,19,14,13,16,15,10,9,12,11,6,5,8,7,2,1,4,3 ],
[ 19,18,17,20,23,22,21,24,15,14,13,16,7,6,5,8,11,10,9,12,3,2,1,4 ],
[ 24,23,22,21,20,19,18,17,16,15,14,13,12,11,10,9,8,7,6,5,4,3,2,1 ] ]

```

З допомогою подальшого коду з'ясуємо, коли матриця $\sigma(v)$ буде симетрична ($\sigma(v) = \sigma(v)^T$).

```

gap> SymSg:=List([1..24],i->List([1..24],j->Sg[i][j]));
gap> for i in [1..24] do
> for j in [1..24] do
> if Sg[i][j]>Sg[j][i] then
> dat:=true;
> for ki in [1..24] do
> for kj in [1..24] do
> if SymSg[ki][kj]=Sg[i][j] then
> if dat then Print("a",Sg[i][j],"=a",Sg[j][i]," "); fi;
> dat:=false;
> SymSg[ki][kj]:=Sg[j][i];

```

```

> fi;
> od;od;
> fi;
> od;od;
a4=a2, a8=a6, a9=a5, a11=a7, a12=a10, a21=a17, a23=a19,
gap> SymSg;
[ [ 1,2,3,2,5,6,7,6,5,10,7,10,13,14,15,16,17,18,19,20,17,22,19,24 ],
  [ 2,1,2,3,10,5,10,7,6,5,6,7,16,13,14,15,24,17,22,19,20,17,18,19 ],
  [ 3,2,1,2,7,6,5,6,7,10,5,10,15,16,13,14,19,20,17,18,19,24,17,22 ],
  [ 2,3,2,1,10,7,10,5,6,7,6,5,14,15,16,13,22,19,24,17,18,19,20,17 ],
  [ 5,10,7,10,1,2,3,2,5,6,7,6,17,22,19,24,13,14,15,16,17,18,19,20 ],
  [ 6,5,6,7,2,1,2,3,10,5,10,7,20,17,18,19,16,13,14,15,24,17,22,19 ],
  [ 7,10,5,10,3,2,1,2,7,6,5,6,19,24,17,22,15,16,13,14,19,20,17,18 ],
  [ 6,7,6,5,2,3,2,1,10,7,10,5,18,19,20,17,14,15,16,13,22,19,24,17 ],
  [ 5,6,7,6,5,10,7,10,1,2,3,2,17,18,19,20,17,22,19,24,13,14,15,16 ],
  [ 10,5,10,7,6,5,6,7,2,1,2,3,24,17,22,19,20,17,18,19,16,13,14,15 ],
  [ 7,6,5,6,7,10,5,10,3,2,1,2,19,20,17,18,19,24,17,22,15,16,13,14 ],
  [ 10,7,10,5,6,7,6,5,2,3,2,1,22,19,24,17,18,19,20,17,14,15,16,13 ],
  [ 13,16,15,14,17,20,19,18,17,24,19,22,1,2,3,2,5,6,7,6,5,10,7,10 ],
  [ 14,13,16,15,22,17,24,19,18,17,20,19,2,1,2,3,10,5,10,7,6,5,6,7 ],
  [ 15,14,13,16,19,18,17,20,19,22,17,24,3,2,1,2,7,6,5,6,7,10,5,10 ],
  [ 16,15,14,13,24,19,22,17,20,19,18,17,2,3,2,1,10,7,10,5,6,7,6,5 ],
  [ 17,24,19,22,13,16,15,14,17,20,19,18,5,10,7,10,1,2,3,2,5,6,7,6 ],
  [ 18,17,20,19,14,13,16,15,22,17,24,19,6,5,6,7,2,1,2,3,10,5,10,7 ],
  [ 19,22,17,24,15,14,13,16,19,18,17,20,7,10,5,10,3,2,1,2,7,6,5,6 ],
  [ 20,19,18,17,16,15,14,13,24,19,22,17,6,7,6,5,2,3,2,1,10,7,10,5 ],
  [ 17,20,19,18,17,24,19,22,13,16,15,14,5,6,7,6,5,10,7,10,1,2,3,2 ],
  [ 22,17,24,19,18,17,20,19,14,13,16,15,10,5,10,7,6,5,6,7,2,1,2,3 ],
  [ 19,18,17,20,19,22,17,24,15,14,13,16,7,6,5,6,7,10,5,10,3,2,1,2 ],
  [ 24,19,22,17,20,19,18,17,16,15,14,13,10,7,10,5,6,7,6,5,2,3,2,1 ] ]

```

Остання матриця вказує вигляд індексів у симетричній матриці $\sigma(v)$ після заміни: $\alpha_4 = \alpha_2$, $\alpha_8 = \alpha_6$, $\alpha_9 = \alpha_5$, $\alpha_{11} = \alpha_7$, $\alpha_{12} = \alpha_{10}$, $\alpha_{21} = \alpha_{17}$, $\alpha_{23} = \alpha_{19}$.

Наступний код шукатиме всі лінійні коди породженні $\sigma(v)$, що $\sigma(\alpha) =$

$\sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$ та обчисленнями командами пакету GUAVA шукатиме їх мінімальну відстань. Додатково врахуємо, що $\sigma(\alpha)^2 = 0_{24 \times 24}$, тільки коли

$$\begin{cases} \alpha_{19} = \alpha_5 + \alpha_7 + \alpha_{17} + \alpha_{14}\alpha_{18} + \alpha_{16}\alpha_{20} + \alpha_{14}\alpha_{22} + \alpha_{18}\alpha_{22} + \alpha_{16}\alpha_{24} + \alpha_{20}\alpha_{24}, \\ \alpha_{24} = \alpha_1 + \alpha_3 + \alpha_{13} + \alpha_{14} + \alpha_{15} + \alpha_{16} + \alpha_{18} + \alpha_{20} + \alpha_{22}, \end{cases}$$

як це показано в підрозділі 7.2.3 формула (7.7).

```
gap> i:=0;;DistList:=[];;
> for a1 in F do
> for a2 in F do
> for a3 in F do
> for a5 in F do
> for a6 in F do
> for a7 in F do
> for a10 in F do
> for a13 in F do
> for a14 in F do
> for a15 in F do
> for a16 in F do
> for a17 in F do
> for a18 in F do
> for a20 in F do
> for a22 in F do
> a24:=a1+a3+a13+a14+a15+a16+a18+a20+a22;
> a19:=a5+a7+a17+a14*a18+a16*a20+a14*a22+a18*a22+a16*a24+a20*a24;
> SgM:=[[a1,a2,a3,a2,a5,a6,a7,a6,a5,a10,a7,a10,
          a13,a14,a15,a16,a17,a18,a19,a20,a17,a22,a19,a24],
> [a2,a1,a2,a3,a10,a5,a10,a7,a6,a5,a6,a7,
          a16,a13,a14,a15,a24,a17,a22,a19,a20,a17,a18,a19],
> [a3,a2,a1,a2,a7,a6,a5,a6,a7,a10,a5,a10,
          a15,a16,a13,a14,a19,a20,a17,a18,a19,a24,a17,a22],
> [a2,a3,a2,a1,a10,a7,a10,a5,a6,a7,a6,a5,
          a14,a15,a16,a13,a22,a19,a24,a17,a18,a19,a20,a17],
> [a5,a10,a7,a10,a1,a2,a3,a2,a5,a6,a7,a6,
```

```

a17,a22,a19,a24,a13,a14,a15,a16,a17,a18,a19,a20],
> [a6,a5,a6,a7,a2,a1,a2,a3,a10,a5,a10,a7,
a20,a17,a18,a19,a16,a13,a14,a15,a24,a17,a22,a19],
> [a7,a10,a5,a10,a3,a2,a1,a2,a7,a6,a5,a6,
a19,a24,a17,a22,a15,a16,a13,a14,a19,a20,a17,a18],
> [a6,a7,a6,a5,a2,a3,a2,a1,a10,a7,a10,a5,
a18,a19,a20,a17,a14,a15,a16,a13,a22,a19,a24,a17],
> [a5,a6,a7,a6,a5,a10,a7,a10,a1,a2,a3,a2,
a17,a18,a19,a20,a17,a22,a19,a24,a13,a14,a15,a16],
> [a10,a5,a10,a7,a6,a5,a6,a7,a2,a1,a2,a3,
a24,a17,a22,a19,a20,a17,a18,a19,a16,a13,a14,a15],
> [a7,a6,a5,a6,a7,a10,a5,a10,a3,a2,a1,a2,
a19,a20,a17,a18,a19,a24,a17,a22,a15,a16,a13,a14],
> [a10,a7,a10,a5,a6,a7,a6,a5,a2,a3,a2,a1,
a22,a19,a24,a17,a18,a19,a20,a17,a14,a15,a16,a13],
> [a13,a16,a15,a14,a17,a20,a19,a18,a17,a24,a19,a22,
a1,a2,a3,a2,a5,a6,a7,a6,a5,a10,a7,a10],
> [a14,a13,a16,a15,a22,a17,a24,a19,a18,a17,a20,a19,
a2,a1,a2,a3,a10,a5,a10,a7,a6,a5,a6,a7],
> [a15,a14,a13,a16,a19,a18,a17,a20,a19,a22,a17,a24,
a3,a2,a1,a2,a7,a6,a5,a6,a7,a10,a5,a10],
> [a16,a15,a14,a13,a24,a19,a22,a17,a20,a19,a18,a17,
a2,a3,a2,a1,a10,a7,a10,a5,a6,a7,a6,a5],
> [a17,a24,a19,a22,a13,a16,a15,a14,a17,a20,a19,a18,
a5,a10,a7,a10,a1,a2,a3,a2,a5,a6,a7,a6],
> [a18,a17,a20,a19,a14,a13,a16,a15,a22,a17,a24,a19,
a6,a5,a6,a7,a2,a1,a2,a3,a10,a5,a10,a7],
> [a19,a22,a17,a24,a15,a14,a13,a16,a19,a18,a17,a20,
a7,a10,a5,a10,a3,a2,a1,a2,a7,a6,a5,a6],
> [a20,a19,a18,a17,a16,a15,a14,a13,a24,a19,a22,a17,
a6,a7,a6,a5,a2,a3,a2,a1,a10,a7,a10,a5],
> [a17,a20,a19,a18,a17,a24,a19,a22,a13,a16,a15,a14,
a5,a6,a7,a6,a5,a10,a7,a10,a1,a2,a3,a2],
> [a22,a17,a24,a19,a18,a17,a20,a19,a14,a13,a16,a15,
a10,a5,a10,a7,a6,a5,a6,a7,a2,a1,a2,a3],

```



```

gap> IntSgM:=
> [ [ 0,0,1,0,0,0,0,0,0,1,0,1,0,0,0,1,0,0,1,1,0,0,1,1 ],
> [ 0,0,0,1,1,0,1,0,0,0,0,0,0,1,0,0,0,1,0,0,1,1,0,0,1 ],
> [ 1,0,0,0,0,0,0,0,0,1,0,1,0,1,0,0,1,1,0,0,1,1,0,0 ],
> [ 0,1,0,0,1,0,1,0,0,0,0,0,0,0,0,1,0,0,1,1,0,0,1,1,0 ],
> [ 0,1,0,1,0,0,1,0,0,0,0,0,0,0,0,1,1,0,0,0,1,0,0,1,1 ],
> [ 0,0,0,0,0,0,0,1,1,0,1,0,1,0,0,1,1,0,0,0,1,0,0,1 ],
> [ 0,1,0,1,1,0,0,0,0,0,0,0,0,0,1,1,0,0,0,1,0,0,1,1,0,0 ],
> [ 0,0,0,0,0,1,0,0,1,0,1,0,0,1,1,0,0,0,1,0,0,1,1,0 ],
> [ 0,0,0,0,0,1,0,1,0,0,1,0,0,0,1,1,0,0,1,1,0,0,0,1 ],
> [ 1,0,1,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1,0,0 ],
> [ 0,0,0,0,0,1,0,1,1,0,0,0,0,1,1,0,0,1,1,0,0,0,1,0,0 ],
> [ 1,0,1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,1,0,0,0,1,0 ],
> [ 0,1,0,0,0,1,1,0,0,1,1,0,0,0,0,1,0,0,0,0,0,0,1,0,1 ],
> [ 0,0,1,0,0,0,1,1,0,0,1,1,0,0,0,1,1,0,1,0,0,0,0,0 ],
> [ 0,0,0,1,1,0,0,1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,1,0,1 ],
> [ 1,0,0,0,1,1,0,0,1,1,0,0,0,0,1,0,0,1,0,1,0,0,0,0,0 ],
> [ 0,1,1,0,0,1,0,0,0,0,1,1,0,0,1,0,1,0,0,1,0,0,0,0,0 ],
> [ 0,0,1,1,0,0,1,0,0,0,1,1,0,0,0,0,0,0,0,0,0,1,1,0,1,0 ],
> [ 1,0,0,1,0,0,0,1,1,0,0,1,0,1,0,1,1,0,0,0,0,0,0,0,0 ],
> [ 1,1,0,0,1,0,0,0,1,1,0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,0 ],
> [ 0,1,1,0,0,1,1,0,0,1,0,0,0,0,0,0,0,0,0,1,0,1,0,0,1,0 ],
> [ 0,0,1,1,0,0,1,1,0,0,1,0,1,0,1,0,0,0,0,0,0,0,0,0,1 ],
> [ 1,0,0,1,1,0,0,1,0,0,0,0,1,0,0,0,0,0,1,0,1,1,0,0,0,0 ],
> [ 1,1,0,0,1,1,0,0,1,0,0,0,0,1,0,1,0,0,0,0,0,0,1,0,0 ] ];;
gap> C:= GeneratorMatCode( IntSgM, GF(2) );
a linear [24,12,1..8]4 code defined by generator matrix over GF(2)
gap> Minimum(List(AsSSortedList(C){[2..Size(C)]}, WeightCodeword ));
8

```

Таким чином було побудовано $[24,12,8]$ -код за груповим кільцем групи $(C_6 \times C_2) \rtimes C_2$.

В.4. Знаходження кодів за групою $C_3 \times D_8$

З'ясуємо інформацію, що стосується побудови розширених бінарних самодуальних кодів Голя за груповим кільцем групи $C_3 \times D_8$. Групу можна визначити як $C_3 \times D_8 = \langle x, y, z \mid x^3 = y^4 = z^2 = 1, xy = yx, xz = zx, yzyz = 1 \rangle$.

```
gap> G:=SmallGroup(24,10);;StructureDescription(G);
"C3 x D8"
gap> f:=FreeGroup(3);
<free group on the generators [ f1, f2, f3 ]>
gap> H:=f/[f.1^3,f.2^4,f.3^2,
          f.1*f.2*f.1^2*f.2^3,f.1*f.3*f.1^2*f.3,f.2*f.3*f.2*f.3];
<fp group on the generators [ f1, f2, f3 ]>
gap> IsomorphismGroups(H,G);
[ f1, f2, f3 ] -> [ f3^2, f1*f2, f2 ]
```

Образами символів x, y, z у S_{24} будуть, наприклад, підстановки

$$x = (1, 2, 3), \quad y = (4, 5, 6, 7), \quad z = (4, 6).$$

```
gap> x:=(1,2,3);;
gap> y:=(4,5,6,7);;
gap> z:=(4,6);;
gap> Ie:=();;
gap> x^3=Ie;y^4=Ie;z^2=Ie;
true
true
true
gap> x*y=y*x;x*z=z*x;y*z*y*z=Ie;
true
true
true
gap> H:=Group(x,y,z);
```

```

Group([ (1,2,3), (4,5,6,7), (4,6) ])
gap> IsomorphismGroups(H,G);
[ (1,2,3), (4,5,6,7), (4,6) ] -> [ f3, f1*f2*f4, f1 ]

```

Задамо порядок елементів на групі $C_3 \times D_8$ порядку 24, та перевіримо, що вказані елементи при визначені порядку не повторюються.

```

gap> g:=
>   1e,      y,      y^2,      y^3,
>   x,      y*x,     y^2*x,     y^3*x,
>   x^2,     y*x^2,   y^2*x^2,   y^3*x^2,
>   z,      z*y,     z*y^2,     z*y^3,
>   z*x,     z*y*x,   z*y^2*x,   z*y^3*x,
>   z*x^2,   z*y*x^2, z*y^2*x^2, z*y^3*x^2
> ];;
gap> Length(Set(g));
24

```

Знайдемо матрицю індексів дії регулярного зображення σ на довільному елементі

$$\begin{aligned}
 v = & \alpha_1 + \alpha_2 y + \alpha_3 y^2 + \alpha_4 y^3 + \\
 & \alpha_5 x + \alpha_6 yx + \alpha_7 y^2 x + \alpha_8 y^3 x + \\
 & \alpha_9 x^2 + \alpha_{10} yx^2 + \alpha_{11} y^2 x^2 + \alpha_{12} y^3 x^2 + \\
 & \alpha_{13} z + \alpha_{14} zy + \alpha_{15} zy^2 + \alpha_{16} zy^3 + \\
 & \alpha_{17} zx + \alpha_{18} zyx + \alpha_{19} zy^2 x + \alpha_{20} zy^3 x + \\
 & \alpha_{21} zx^2 + \alpha_{22} zyx^2 + \alpha_{23} zy^2 x^2 + \alpha_{24} zy^3 x^2
 \end{aligned}$$

групового кільця $\mathbb{F}_2(C_3 \times D_8)$, що відповідає порядку обернених елементів до вказаних.

```

gap> Sg:=[];;
gap> for i in g do

```

```

> A:=[];
> for j in g do
> Add(A,Position(g,i^(-1)*j));od;
> Add(Sg,A);od;
gap> Sg;
[ [ 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 ],
  [ 4,1,2,3,8,5,6,7,12,9,10,11,14,15,16,13,18,19,20,17,22,23,24,21 ],
  [ 3,4,1,2,7,8,5,6,11,12,9,10,15,16,13,14,19,20,17,18,23,24,21,22 ],
  [ 2,3,4,1,6,7,8,5,10,11,12,9,16,13,14,15,20,17,18,19,24,21,22,23 ],
  [ 9,10,11,12,1,2,3,4,5,6,7,8,21,22,23,24,13,14,15,16,17,18,19,20 ],
  [ 12,9,10,11,4,1,2,3,8,5,6,7,22,23,24,21,14,15,16,13,18,19,20,17 ],
  [ 11,12,9,10,3,4,1,2,7,8,5,6,23,24,21,22,15,16,13,14,19,20,17,18 ],
  [ 10,11,12,9,2,3,4,1,6,7,8,5,24,21,22,23,16,13,14,15,20,17,18,19 ],
  [ 5,6,7,8,9,10,11,12,1,2,3,4,17,18,19,20,21,22,23,24,13,14,15,16 ],
  [ 8,5,6,7,12,9,10,11,4,1,2,3,18,19,20,17,22,23,24,21,14,15,16,13 ],
  [ 7,8,5,6,11,12,9,10,3,4,1,2,19,20,17,18,23,24,21,22,15,16,13,14 ],
  [ 6,7,8,5,10,11,12,9,2,3,4,1,20,17,18,19,24,21,22,23,16,13,14,15 ],
  [ 13,14,15,16,17,18,19,20,21,22,23,24,1,2,3,4,5,6,7,8,9,10,11,12 ],
  [ 14,15,16,13,18,19,20,17,22,23,24,21,4,1,2,3,8,5,6,7,12,9,10,11 ],
  [ 15,16,13,14,19,20,17,18,23,24,21,22,3,4,1,2,7,8,5,6,11,12,9,10 ],
  [ 16,13,14,15,20,17,18,19,24,21,22,23,2,3,4,1,6,7,8,5,10,11,12,9 ],
  [ 21,22,23,24,13,14,15,16,17,18,19,20,9,10,11,12,1,2,3,4,5,6,7,8 ],
  [ 22,23,24,21,14,15,16,13,18,19,20,17,12,9,10,11,4,1,2,3,8,5,6,7 ],
  [ 23,24,21,22,15,16,13,14,19,20,17,18,11,12,9,10,3,4,1,2,7,8,5,6 ],
  [ 24,21,22,23,16,13,14,15,20,17,18,19,10,11,12,9,2,3,4,1,6,7,8,5 ],
  [ 17,18,19,20,21,22,23,24,13,14,15,16,5,6,7,8,9,10,11,12,1,2,3,4 ],
  [ 18,19,20,17,22,23,24,21,14,15,16,13,8,5,6,7,12,9,10,11,4,1,2,3 ],
  [ 19,20,17,18,23,24,21,22,15,16,13,14,7,8,5,6,11,12,9,10,3,4,1,2 ],
  [ 20,17,18,19,24,21,22,23,16,13,14,15,6,7,8,5,10,11,12,9,2,3,4,1 ] ]

```

З допомогою подальшого коду з'ясуємо, коли матриця $\sigma(v)$ буде симетрична ($\sigma(v) = \sigma(v)^T$).

```

gap> SymSg:=List([1..24],i->List([1..24],j->Sg[i][j]));;
gap> for i in [1..24] do
> for j in [1..24] do

```

```

> if Sg[i][j]>Sg[j][i] then
> dat:=true;
> for ki in [1..24] do
> for kj in [1..24] do
> if SymSg[ki][kj]=Sg[i][j] then
> if dat then Print("a",Sg[i][j],"=a",Sg[j][i]," ", " "); fi;
> dat:=false;
> SymSg[ki][kj]:=Sg[j][i];
> fi;
> od;od;
> fi;
> od;od;
a4=a2, a9=a5, a10=a8, a11=a7, a12=a6, a21=a17, a22=a18, a23=a19, a24=a20,
gap> SymSg;
[ [ 1,2,3,2,5,6,7,8,5,8,7,6,13,14,15,16,17,18,19,20,17,18,19,20 ],
  [ 2,1,2,3,8,5,6,7,6,5,8,7,14,15,16,13,18,19,20,17,18,19,20,17 ],
  [ 3,2,1,2,7,8,5,6,7,6,5,8,15,16,13,14,19,20,17,18,19,20,17,18 ],
  [ 2,3,2,1,6,7,8,5,8,7,6,5,16,13,14,15,20,17,18,19,20,17,18,19 ],
  [ 5,8,7,6,1,2,3,2,5,6,7,8,17,18,19,20,13,14,15,16,17,18,19,20 ],
  [ 6,5,8,7,2,1,2,3,8,5,6,7,18,19,20,17,14,15,16,13,18,19,20,17 ],
  [ 7,6,5,8,3,2,1,2,7,8,5,6,19,20,17,18,15,16,13,14,19,20,17,18 ],
  [ 8,7,6,5,2,3,2,1,6,7,8,5,20,17,18,19,16,13,14,15,20,17,18,19 ],
  [ 5,6,7,8,5,8,7,6,1,2,3,2,17,18,19,20,17,18,19,20,13,14,15,16 ],
  [ 8,5,6,7,6,5,8,7,2,1,2,3,18,19,20,17,18,19,20,17,14,15,16,13 ],
  [ 7,8,5,6,7,6,5,8,3,2,1,2,19,20,17,18,19,20,17,18,15,16,13,14 ],
  [ 6,7,8,5,8,7,6,5,2,3,2,1,20,17,18,19,20,17,18,19,16,13,14,15 ],
  [ 13,14,15,16,17,18,19,20,17,18,19,20,1,2,3,2,5,6,7,8,5,8,7,6 ],
  [ 14,15,16,13,18,19,20,17,18,19,20,17,2,1,2,3,8,5,6,7,6,5,8,7 ],
  [ 15,16,13,14,19,20,17,18,19,20,17,18,3,2,1,2,7,8,5,6,7,6,5,8 ],
  [ 16,13,14,15,20,17,18,19,20,17,18,19,2,3,2,1,6,7,8,5,8,7,6,5 ],
  [ 17,18,19,20,13,14,15,16,17,18,19,20,5,8,7,6,1,2,3,2,5,6,7,8 ],
  [ 18,19,20,17,14,15,16,13,18,19,20,17,6,5,8,7,2,1,2,3,8,5,6,7 ],
  [ 19,20,17,18,15,16,13,14,19,20,17,18,7,6,5,8,3,2,1,2,7,8,5,6 ],
  [ 20,17,18,19,16,13,14,15,20,17,18,19,8,7,6,5,2,3,2,1,6,7,8,5 ],
  [ 17,18,19,20,17,18,19,20,13,14,15,16,5,6,7,8,5,8,7,6,1,2,3,2 ],

```

[18,19,20,17,18,19,20,17,14,15,16,13,8,5,6,7,6,5,8,7,2,1,2,3],
 [19,20,17,18,19,20,17,18,15,16,13,14,7,8,5,6,7,6,5,8,3,2,1,2],
 [20,17,18,19,20,17,18,19,16,13,14,15,6,7,8,5,8,7,6,5,2,3,2,1]]

Остання матриця вказує вигляд індексів у симетричній матриці $\sigma(v)$ після замін: $\alpha_4 = \alpha_2$, $\alpha_9 = \alpha_5$, $\alpha_{10} = \alpha_8$, $\alpha_{11} = \alpha_7$, $\alpha_{12} = \alpha_6$, $\alpha_{21} = \alpha_{17}$, $\alpha_{22} = \alpha_{18}$, $\alpha_{23} = \alpha_{19}$, $\alpha_{24} = \alpha_{20}$.

Наступний код шукатиме всі лінійні коди породженні $\sigma(v)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$ та обчисленнями командами пакету GUAVA шукатиме їх мінімальну відстань. Додатково врахуємо, що $\sigma(\alpha)^2 = 0_{24 \times 24}$, тільки коли

$$\begin{cases} \alpha_8 &= \alpha_6, \\ \alpha_{16} &= \alpha_1 + \alpha_3 + \alpha_{13} + \alpha_{14} + \alpha_{15}, \\ \alpha_{20} &= \alpha_5 + \alpha_7 + \alpha_{17} + \alpha_{18} + \alpha_{19}, \end{cases}$$

як це показано в підрозділі 7.2.4 формула (7.7).

```
gap> i:=0;;DistList:=[];;
> for a2 in F do
> for a3 in F do
> for a5 in F do
> for a6 in F do
> for a7 in F do
> for a13 in F do
> for a14 in F do
> for a15 in F do
> for a17 in F do
> for a18 in F do
> for a19 in F do
> a8:=a6;
> a16:=a1+a3+a13+a14+a15;
> a20:=a5+a7+a17+a18+a19;
> SgM:=[]
```

```

> [a1,a2,a3,a2,a5,a6,a7,a8,a5,a8,a7,a6,
    a13,a14,a15,a16,a17,a18,a19,a20,a17,a18,a19,a20],
> [a2,a1,a2,a3,a8,a5,a6,a7,a6,a5,a8,a7,
    a14,a15,a16,a13,a18,a19,a20,a17,a18,a19,a20,a17],
> [a3,a2,a1,a2,a7,a8,a5,a6,a7,a6,a5,a8,
    a15,a16,a13,a14,a19,a20,a17,a18,a19,a20,a17,a18],
> [a2,a3,a2,a1,a6,a7,a8,a5,a8,a7,a6,a5,
    a16,a13,a14,a15,a20,a17,a18,a19,a20,a17,a18,a19],
> [a5,a8,a7,a6,a1,a2,a3,a2,a5,a6,a7,a8,
    a17,a18,a19,a20,a13,a14,a15,a16,a17,a18,a19,a20],
> [a6,a5,a8,a7,a2,a1,a2,a3,a8,a5,a6,a7,
    a18,a19,a20,a17,a14,a15,a16,a13,a18,a19,a20,a17],
> [a7,a6,a5,a8,a3,a2,a1,a2,a7,a8,a5,a6,
    a19,a20,a17,a18,a15,a16,a13,a14,a19,a20,a17,a18],
> [a8,a7,a6,a5,a2,a3,a2,a1,a6,a7,a8,a5,
    a20,a17,a18,a19,a16,a13,a14,a15,a20,a17,a18,a19],
> [a5,a6,a7,a8,a5,a8,a7,a6,a1,a2,a3,a2,
    a17,a18,a19,a20,a17,a18,a19,a20,a13,a14,a15,a16],
> [a8,a5,a6,a7,a6,a5,a8,a7,a2,a1,a2,a3,
    a18,a19,a20,a17,a18,a19,a20,a17,a14,a15,a16,a13],
> [a7,a8,a5,a6,a7,a6,a5,a8,a3,a2,a1,a2,
    a19,a20,a17,a18,a19,a20,a17,a18,a15,a16,a13,a14],
> [a6,a7,a8,a5,a8,a7,a6,a5,a2,a3,a2,a1,
    a20,a17,a18,a19,a20,a17,a18,a19,a16,a13,a14,a15],
> [a13,a14,a15,a16,a17,a18,a19,a20,a17,a18,a19,a20,
    a1,a2,a3,a2,a5,a6,a7,a8,a5,a8,a7,a6],
> [a14,a15,a16,a13,a18,a19,a20,a17,a18,a19,a20,a17,
    a2,a1,a2,a3,a8,a5,a6,a7,a6,a5,a8,a7],
> [a15,a16,a13,a14,a19,a20,a17,a18,a19,a20,a17,a18,
    a3,a2,a1,a2,a7,a8,a5,a6,a7,a6,a5,a8],
> [a16,a13,a14,a15,a20,a17,a18,a19,a20,a17,a18,a19,
    a2,a3,a2,a1,a6,a7,a8,a5,a8,a7,a6,a5],
> [a17,a18,a19,a20,a13,a14,a15,a16,a17,a18,a19,a20,
    a5,a8,a7,a6,a1,a2,a3,a2,a5,a6,a7,a8],
> [a18,a19,a20,a17,a14,a15,a16,a13,a18,a19,a20,a17,

```


Таким чином є 1600 елементів $v \in \mathbb{F}_2(C_3 \times D_8)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$, а з лінійних кодів породжених $\sigma(v)$ $[24, 12, 2]$ -кодів є 128, $[24, 12, 4]$ -кодів є 1216, $[24, 12, 6]$ -кодів є 128, $[24, 12, 8]$ -кодів є **128**.

Розглянемо, для прикладу, код, що відповідає послідовності $(\alpha_i) = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$ та визначимо його розмірність простору кодових слів та мінімальну відстань

```
gap> IntSgM:=
> [ [ 1,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,0,0,1,1,0,0 ],
> [ 0,1,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,1,0,0,1,1,0,0,1 ],
> [ 0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,1,0,0,1,1,0,0,1,1 ],
> [ 0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,1,1,0,1,1,0,0,1,1,0 ],
> [ 0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0,0,0,1,1,1,1,0,0,0 ],
> [ 0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,1,1,1,1,0,1,0,0,1 ],
> [ 0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,1,0,1,0,0,1,1,1 ],
> [ 0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,1,0,1,0,1,1,0,1,1,0 ],
> [ 0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,1,0,0,1,1,0,0,0,1,1,1 ],
> [ 0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,0,0,1,0,0,1,1,1,1,0 ],
> [ 0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1,0,0,1,1,1,0,1,1 ],
> [ 0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1,0,0,1,1,1,0,1 ],
> [ 0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1,0,0,1,1,0,1,1 ],
> [ 0,1,1,1,1,1,0,0,1,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 1,1,1,0,1,0,0,1,1,0,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 1,1,0,1,0,0,1,1,0,0,1,1,0,0,1,0,0,0,0,0,0,0,0,0,0 ],
> [ 1,0,1,1,0,1,1,0,0,1,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0 ],
> [ 1,1,0,0,0,1,1,1,1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0 ],
> [ 1,0,0,1,1,1,1,0,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 0,0,1,1,1,1,0,1,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 0,1,1,0,1,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 1,1,0,0,1,1,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 1,0,0,1,1,0,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 0,0,1,1,0,0,1,1,1,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 0,1,1,0,0,1,1,0,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 0,1,1,0,0,1,1,0,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,1 ] ];;
gap> C:= GeneratorMatCode( IntSgM, GF(2) );
a linear [24,12,1..8]4 code defined by generator matrix over GF(2)
```



```

gap> Codeword( GeneratorMat( StandardFormCode( C )));
[ [ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 0 0 1 1 0 0 ],
  [ 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 0 1 1 0 0 1 ],
  [ 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 0 1 1 0 0 1 1 ],
  [ 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 1 1 0 1 1 0 0 1 1 0 ],
  [ 0 0 0 0 1 0 0 0 0 0 0 0 0 1 1 0 0 0 1 1 1 1 1 0 0 ],
  [ 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 1 1 1 1 0 1 0 0 1 ],
  [ 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 1 1 0 1 0 0 1 1 ],
  [ 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 1 0 1 1 0 1 1 0 ],
  [ 0 0 0 0 0 0 0 0 1 0 0 0 0 1 1 0 0 1 1 0 0 0 1 1 1 ],
  [ 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 1 1 0 0 1 1 1 1 0 ],
  [ 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 0 1 1 1 1 0 1 ],
  [ 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 0 0 1 1 0 1 0 1 1 ] ]
gap> Minimum(List(AsSSortedList(C){[2..Size(C)]}, WeightCodeword ));
8

```

Отже, було побудовано $[24,12,8]$ -код за груповим кільцем групи $C_3 \times D_8$.

В.5. Знаходження кодів за групою $C_2 \times A_4$

З'ясуємо інформацію, що стосується побудови розширених бінарних самодуальних кодів Голея за груповим кільцем групи $C_2 \times A_4$. Групу можна визначити як $C_2 \times A_4 = \langle x, y, z, w \mid x^2 = y^2 = z^2 = w^3 = 1, xy = yx, xz = zx, xw = wx, yz = zy, yw = wyz, zw = wy \rangle$.

```

gap> G:=SmallGroup(24,13);;StructureDescription(G);
"C2 x A4"
gap> y*z=z*y;
gap> f:=FreeGroup(4);
<free group on the generators [ f1, f2, f3, f4 ]>
gap> H:=f/[f.1^2,f.2^2,f.3^2,f.4^3,
> f.1*f.2*f.1*f.2,
> f.1*f.3*f.1*f.3,

```

```

> f.1*f.4*f.1*f.4^2,
> f.2*f.3*f.2*f.3,
> f.2*f.4*f.2*f.3*f.4^2,
> f.3*f.4*f.2*f.4^2
> ];
<fp group on the generators [ f1, f2, f3, f4 ]>
gap> IsomorphismGroups(H,G);
[ f1, f2, f3, f4 ] -> [ f1, f3, f4, f2^2*f3 ]

```

Образами символів x, y, z у S_{24} будуть, наприклад, підстановки

$$x = (1, 2), \quad y = (3, 4)(5, 6), \quad z = (3, 5)(4, 6), \quad w = (3, 4, 5).$$

```

gap> x:=(1,2);;
gap> y:=(3,4)(5,6);;
gap> z:=(3,5)(4,6);;
gap> w:=(3,4,5);;
gap> Ie:=();;
gap> x^2=Ie;y^2=Ie;z^2=Ie;w^3=Ie;
true
true
true
true
gap> x*y=y*x;x*z=z*x;x*w=w*x;y*z=z*y;y*w=w*y*z;z*w=w*y;
true
true
true
true
true
true
gap> H:=Group(x,y,z,w);
Group([ (1,2), (3,4)(5,6), (3,5)(4,6), (3,4,5) ])
gap> IsomorphismGroups(H,G);
[ (1,2), (3,4)(5,6), (3,5)(4,6), (3,4,5) ] -> [ f1, f3*f4, f4, f2*f4 ]

```

Задамо порядок елементів на групі $C_2 \times A_4$ порядку 24, та перевіримо, що вказані елементи при визначені порядку не повторюються.

```
gap> g:=[
> 1e, y, z, y*z, w, y*w, z*w, y*z*w,
> w^2, y*w^2, z*w^2, y*z*w^2,
> x, x*y, x*z, x*y*z, x*w, x*y*w, x*z*w, x*y*z*w,
> x*w^2, x*y*w^2, x*z*w^2, x*y*z*w^2
> ];;
gap> Length(Set(g));
24
```

Знайдемо матрицю індексів дії регулярного зображення σ на довільному елементі

$$\begin{aligned}
v = & \alpha_1 + \alpha_2 y + \alpha_3 z + \alpha_4 yz + \alpha_5 w + \alpha_6 yw + \\
& \alpha_7 zw + \alpha_8 yzw + \alpha_9 w^2 + \alpha_{10} yw^2 + \alpha_{11} zw^2 + \alpha_{12} yzw^2 + \\
& \alpha_{13} x + \alpha_{14} xy + \alpha_{15} xz + \alpha_{16} xyz + \alpha_{17} xw + \alpha_{18} xyw + \\
& \alpha_{19} xzw + \alpha_{20} xyzw + \alpha_{21} xw^2 + \alpha_{22} xyw^2 + \alpha_{23} xzw^2 + \alpha_{24} xyzw^2
\end{aligned}$$

групового кільця $\mathbb{F}_2(C_2 \times A_4)$, що відповідає порядку обернених елементів до вказаних.

```
gap> Sg:=[];;
gap> for i in g do
> A:=[];
> for j in g do
> Add(A,Position(g,i^(-1)*j));od;
> Add(Sg,A);od;
gap> Sg;
[ [ 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 ],
[ 2,1,4,3,6,5,8,7,10,9,12,11,14,13,16,15,18,17,20,19,22,21,24,23 ],
[ 3,4,1,2,7,8,5,6,11,12,9,10,15,16,13,14,19,20,17,18,23,24,21,22 ],
[ 4,3,2,1,8,7,6,5,12,11,10,9,16,15,14,13,20,19,18,17,24,23,22,21 ],
```

```
[ 9,12,10,11,1,4,2,3,5,8,6,7,21,24,22,23,13,16,14,15,17,20,18,19 ],
[ 12,9,11,10,4,1,3,2,8,5,7,6,24,21,23,22,16,13,15,14,20,17,19,18 ],
[ 10,11,9,12,2,3,1,4,6,7,5,8,22,23,21,24,14,15,13,16,18,19,17,20 ],
[ 11,10,12,9,3,2,4,1,7,6,8,5,23,22,24,21,15,14,16,13,19,18,20,17 ],
[ 5,7,8,6,9,11,12,10,1,3,4,2,17,19,20,18,21,23,24,22,13,15,16,14 ],
[ 7,5,6,8,11,9,10,12,3,1,2,4,19,17,18,20,23,21,22,24,15,13,14,16 ],
[ 8,6,5,7,12,10,9,11,4,2,1,3,20,18,17,19,24,22,21,23,16,14,13,15 ],
[ 6,8,7,5,10,12,11,9,2,4,3,1,18,20,19,17,22,24,23,21,14,16,15,13 ],
[ 13,14,15,16,17,18,19,20,21,22,23,24,1,2,3,4,5,6,7,8,9,10,11,12 ],
[ 14,13,16,15,18,17,20,19,22,21,24,23,2,1,4,3,6,5,8,7,10,9,12,11 ],
[ 15,16,13,14,19,20,17,18,23,24,21,22,3,4,1,2,7,8,5,6,11,12,9,10 ],
[ 16,15,14,13,20,19,18,17,24,23,22,21,4,3,2,1,8,7,6,5,12,11,10,9 ],
[ 21,24,22,23,13,16,14,15,17,20,18,19,9,12,10,11,1,4,2,3,5,8,6,7 ],
[ 24,21,23,22,16,13,15,14,20,17,19,18,12,9,11,10,4,1,3,2,8,5,7,6 ],
[ 22,23,21,24,14,15,13,16,18,19,17,20,10,11,9,12,2,3,1,4,6,7,5,8 ],
[ 23,22,24,21,15,14,16,13,19,18,20,17,11,10,12,9,3,2,4,1,7,6,8,5 ],
[ 17,19,20,18,21,23,24,22,13,15,16,14,5,7,8,6,9,11,12,10,1,3,4,2 ],
[ 19,17,18,20,23,21,22,24,15,13,14,16,7,5,6,8,11,9,10,12,3,1,2,4 ],
[ 20,18,17,19,24,22,21,23,16,14,13,15,8,6,5,7,12,10,9,11,4,2,1,3 ],
[ 18,20,19,17,22,24,23,21,14,16,15,13,6,8,7,5,10,12,11,9,2,4,3,1 ] ]
```

З допомогою подальшого коду з'ясовуємо, коли матриця $\sigma(v)$ буде симетрична ($\sigma(v) = \sigma(v)^T$).

```
gap> SymSg:=List([1..24],i->List([1..24],j->Sg[i][j]));;
gap> for i in [1..24] do
> for j in [1..24] do
> if Sg[i][j]>Sg[j][i] then
> dat:=true;
> for ki in [1..24] do
> for kj in [1..24] do
> if SymSg[ki][kj]=Sg[i][j] then
> if dat then Print("a",Sg[i][j],"=a",Sg[j][i]," ", " "); fi;
> dat:=false;
> SymSg[ki][kj]:=Sg[j][i];
> fi;
```

```

> od;od;
> fi;
> od;od;
a9=a5, a10=a7, a11=a8, a12=a6, a21=a17, a22=a19, a23=a20, a24=a18,
gap> SymSg;
[ [ 1,2,3,4,5,6,7,8,5,7,8,6,13,14,15,16,17,18,19,20,17,19,20,18 ],
  [ 2,1,4,3,6,5,8,7,7,5,6,8,14,13,16,15,18,17,20,19,19,17,18,20 ],
  [ 3,4,1,2,7,8,5,6,8,6,5,7,15,16,13,14,19,20,17,18,20,18,17,19 ],
  [ 4,3,2,1,8,7,6,5,6,8,7,5,16,15,14,13,20,19,18,17,18,20,19,17 ],
  [ 5,6,7,8,1,4,2,3,5,8,6,7,17,18,19,20,13,16,14,15,17,20,18,19 ],
  [ 6,5,8,7,4,1,3,2,8,5,7,6,18,17,20,19,16,13,15,14,20,17,19,18 ],
  [ 7,8,5,6,2,3,1,4,6,7,5,8,19,20,17,18,14,15,13,16,18,19,17,20 ],
  [ 8,7,6,5,3,2,4,1,7,6,8,5,20,19,18,17,15,14,16,13,19,18,20,17 ],
  [ 5,7,8,6,5,8,6,7,1,3,4,2,17,19,20,18,17,20,18,19,13,15,16,14 ],
  [ 7,5,6,8,8,5,7,6,3,1,2,4,19,17,18,20,20,17,19,18,15,13,14,16 ],
  [ 8,6,5,7,6,7,5,8,4,2,1,3,20,18,17,19,18,19,17,20,16,14,13,15 ],
  [ 6,8,7,5,7,6,8,5,2,4,3,1,18,20,19,17,19,18,20,17,14,16,15,13 ],
  [ 13,14,15,16,17,18,19,20,17,19,20,18,1,2,3,4,5,6,7,8,5,7,8,6 ],
  [ 14,13,16,15,18,17,20,19,19,17,18,20,2,1,4,3,6,5,8,7,7,5,6,8 ],
  [ 15,16,13,14,19,20,17,18,20,18,17,19,3,4,1,2,7,8,5,6,8,6,5,7 ],
  [ 16,15,14,13,20,19,18,17,18,20,19,17,4,3,2,1,8,7,6,5,6,8,7,5 ],
  [ 17,18,19,20,13,16,14,15,17,20,18,19,5,6,7,8,1,4,2,3,5,8,6,7 ],
  [ 18,17,20,19,16,13,15,14,20,17,19,18,6,5,8,7,4,1,3,2,8,5,7,6 ],
  [ 19,20,17,18,14,15,13,16,18,19,17,20,7,8,5,6,2,3,1,4,6,7,5,8 ],
  [ 20,19,18,17,15,14,16,13,19,18,20,17,8,7,6,5,3,2,4,1,7,6,8,5 ],
  [ 17,19,20,18,17,20,18,19,13,15,16,14,5,7,8,6,5,8,6,7,1,3,4,2 ],
  [ 19,17,18,20,20,17,19,18,15,13,14,16,7,5,6,8,8,5,7,6,3,1,2,4 ],
  [ 20,18,17,19,18,19,17,20,16,14,13,15,8,6,5,7,6,7,5,8,4,2,1,3 ],
  [ 18,20,19,17,19,18,20,17,14,16,15,13,6,8,7,5,7,6,8,5,2,4,3,1 ] ]

```

Остання матриця вказує вигляд індексів у симетричній матриці $\sigma(v)$ після замін: $\alpha_9 = \alpha_5$, $\alpha_{10} = \alpha_7$, $\alpha_{11} = \alpha_8$, $\alpha_{12} = \alpha_6$, $\alpha_{21} = \alpha_{17}$, $\alpha_{22} = \alpha_{19}$, $\alpha_{23} = \alpha_{20}$, $\alpha_{24} = \alpha_{18}$.

Наступний код шукатиме всі лінійні коди породженні $\sigma(v)$, що $\sigma(\alpha) =$

$\sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$ та обчисленнями командами пакету GUAVA шукатиме їх мінімальну відстань. Додатково врахуємо, що $\sigma(\alpha)^2 = 0_{24 \times 24}$, тільки коли

$$\begin{cases} \alpha_{16} = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_{13} + \alpha_{14} + \alpha_{15}, \\ \alpha_{20} = \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8 + \alpha_{17} + \alpha_{18} + \alpha_{19}. \end{cases}$$

як це показано в підрозділі 7.2.5 формула (7.9).

```
gap> i:=0;;DistList:=[];;
> for a1 in F do
> for a2 in F do
> for a3 in F do
> for a4 in F do
> for a5 in F do
> for a6 in F do
> for a7 in F do
> for a8 in F do
> for a13 in F do
> for a14 in F do
> for a15 in F do
> for a17 in F do
> for a18 in F do
> for a19 in F do
> a16:=a1+a2+a3+a4+a13+a14+a15;
> a20:=a5+a6+a7+a8+a17+a18+a19;
> SgM:=
> [a1,a2,a3,a4,a5,a6,a7,a8,a5,a7,a8,a6,
      a13,a14,a15,a16,a17,a18,a19,a20,a17,a19,a20,a18],
> [a2,a1,a4,a3,a6,a5,a8,a7,a7,a5,a6,a8,
      a14,a13,a16,a15,a18,a17,a20,a19,a19,a17,a18,a20],
> [a3,a4,a1,a2,a7,a8,a5,a6,a8,a6,a5,a7,
      a15,a16,a13,a14,a19,a20,a17,a18,a20,a18,a17,a19],
> [a4,a3,a2,a1,a8,a7,a6,a5,a6,a8,a7,a5,
      a16,a15,a14,a13,a20,a19,a18,a17,a18,a20,a19,a17],
> [a5,a6,a7,a8,a1,a4,a2,a3,a5,a8,a6,a7,
```

```

a17,a18,a19,a20,a13,a16,a14,a15,a17,a20,a18,a19],
> [a6,a5,a8,a7,a4,a1,a3,a2,a8,a5,a7,a6,
a18,a17,a20,a19,a16,a13,a15,a14,a20,a17,a19,a18],
> [a7,a8,a5,a6,a2,a3,a1,a4,a6,a7,a5,a8,
a19,a20,a17,a18,a14,a15,a13,a16,a18,a19,a17,a20],
> [a8,a7,a6,a5,a3,a2,a4,a1,a7,a6,a8,a5,
a20,a19,a18,a17,a15,a14,a16,a13,a19,a18,a20,a17],
> [a5,a7,a8,a6,a5,a8,a6,a7,a1,a3,a4,a2,
a17,a19,a20,a18,a17,a20,a18,a19,a13,a15,a16,a14],
> [a7,a5,a6,a8,a8,a5,a7,a6,a3,a1,a2,a4,
a19,a17,a18,a20,a20,a17,a19,a18,a15,a13,a14,a16],
> [a8,a6,a5,a7,a6,a7,a5,a8,a4,a2,a1,a3,
a20,a18,a17,a19,a18,a19,a17,a20,a16,a14,a13,a15],
> [a6,a8,a7,a5,a7,a6,a8,a5,a2,a4,a3,a1,
a18,a20,a19,a17,a19,a18,a20,a17,a14,a16,a15,a13],
> [a13,a14,a15,a16,a17,a18,a19,a20,a17,a19,a20,a18,
a1,a2,a3,a4,a5,a6,a7,a8,a5,a7,a8,a6],
> [a14,a13,a16,a15,a18,a17,a20,a19,a19,a17,a18,a20,
a2,a1,a4,a3,a6,a5,a8,a7,a7,a5,a6,a8],
> [a15,a16,a13,a14,a19,a20,a17,a18,a20,a18,a17,a19,
a3,a4,a1,a2,a7,a8,a5,a6,a8,a6,a5,a7],
> [a16,a15,a14,a13,a20,a19,a18,a17,a18,a20,a19,a17,
a4,a3,a2,a1,a8,a7,a6,a5,a6,a8,a7,a5],
> [a17,a18,a19,a20,a13,a16,a14,a15,a17,a20,a18,a19,
a5,a6,a7,a8,a1,a4,a2,a3,a5,a8,a6,a7],
> [a18,a17,a20,a19,a16,a13,a15,a14,a20,a17,a19,a18,
a6,a5,a8,a7,a4,a1,a3,a2,a8,a5,a7,a6],
> [a19,a20,a17,a18,a14,a15,a13,a16,a18,a19,a17,a20,
a7,a8,a5,a6,a2,a3,a1,a4,a6,a7,a5,a8],
> [a20,a19,a18,a17,a15,a14,a16,a13,a19,a18,a20,a17,
a8,a7,a6,a5,a3,a2,a4,a1,a7,a6,a8,a5],
> [a17,a19,a20,a18,a17,a20,a18,a19,a13,a15,a16,a14,
a5,a7,a8,a6,a5,a8,a6,a7,a1,a3,a4,a2],
> [a19,a17,a18,a20,a20,a17,a19,a18,a15,a13,a14,a16,
a7,a5,a6,a8,a8,a5,a7,a6,a3,a1,a2,a4],

```

```

> [a20,a18,a17,a19,a18,a19,a17,a20,a16,a14,a13,a15,
      a8,a6,a5,a7,a6,a7,a5,a8,a4,a2,a1,a3],
> [a18,a20,a19,a17,a19,a18,a20,a17,a14,a16,a15,a13,
      a6,a8,a7,a5,a7,a6,a8,a5,a2,a4,a3,a1]];

> if SgM^2=ZM then
>   if RankMat(SgM)=12 then
>     i:=i+1;C:= GeneratorMatCode( SgM, GF(2) );
>     m:=Minimum(List(AsSSortedList(C){[2..Size(C)]}, WeightCodeword ));
>     Add(DistList,m);
>     Print(i,"-",m,"-",Codeword(SgM[1]),"\n");
> fi;fi;
> od;od;od;od;od;od;od;od;od;od;od;od;od;od;od;od;
1-2-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 ]
2-4-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 0 ]
3-4-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 0 1 1 ]
4-4-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 0 ]
5-4-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1 0 0 1 ]

.....

2556-4-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 ]
2557-4-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 1 0 1 0 0 1 1 ]
2558-4-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 1 0 1 1 0 0 ]
2559-4-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 1 0 0 1 0 0 1 ]
2560-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 1 1 1 1 ]
gap> Collected(DistList);
[ [ 2, 256 ], [ 4, 1536 ], [ 6, 384 ], [ 8, 384 ] ]

```

Таким чином є 2560 елементів $v \in \mathbb{F}_2(C_2 \times A_4)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$, а з лінійних кодів породжених $\sigma(v)$ $[24, 12, 2]$ -кодів є 256, $[24, 12, 4]$ -кодів є 1536, $[24, 12, 6]$ -кодів є 384, $[24, 12, 8]$ -кодів є **384**.

Розглянемо, для прикладу, код, що відповідає послідовності $(\alpha_i) = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$ та визначимо його розмірність простору кодових слів та мінімальну відстань


```

gap> IntSgM:=
> [ 1,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,0,1,0,1,0,0,1,1 ],
> [ 0,1,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,1,0,0,0,1,1 ],
> [ 0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,1,0,1,1,1,0,0 ],
> [ 0,0,0,1,0,0,0,0,0,0,0,0,0,1,1,0,1,1,0,1,0,1,1,0,0 ],
> [ 0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1,1,1,0,1,0,1,1,0 ],
> [ 0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,0,1,1,1,0,1,0,0,1 ],
> [ 0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,1,0,1,1,1,1,0,0,1 ],
> [ 0,0,0,0,0,0,0,1,0,0,0,0,0,1,0,1,0,1,0,1,1,0,1,1,0 ],
> [ 0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,1,0,1,1,0,1,1,1,0 ],
> [ 0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,1,0,1,1,0,1,1,0,1 ],
> [ 0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1,1,0,0,1,1,1,0,1 ],
> [ 0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,0,0,1,0,0,1,1,0,1,1 ],
> [ 0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,1,1,0,0,1,1,1 ],
> [ 1,0,1,1,0,1,0,1,0,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0 ],
> [ 0,1,1,1,1,0,1,0,0,0,1,1,0,1,0,0,0,0,0,0,0,0,0,0 ],
> [ 1,1,1,0,0,1,0,1,1,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0 ],
> [ 1,1,0,1,1,0,1,0,1,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0 ],
> [ 0,1,0,1,1,1,0,1,0,1,1,0,0,0,0,0,0,1,0,0,0,0,0,0 ],
> [ 1,0,1,0,1,1,1,0,1,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0 ],
> [ 0,1,0,1,0,1,1,1,1,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0 ],
> [ 1,0,1,0,1,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,1,0,0,0 ],
> [ 0,0,1,1,0,1,1,0,1,1,1,0,0,0,0,0,0,0,0,0,0,1,0,0 ],
> [ 0,0,1,1,1,0,0,1,1,1,0,1,0,0,0,0,0,0,0,0,0,1,0,0 ],
> [ 1,1,0,0,1,0,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,1,0 ],
> [ 1,1,0,0,0,1,1,0,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,1 ] ];;

gap> C:= GeneratorMatCode( IntSgM, GF(2) );
a linear [24,12,1..8]4 code defined by generator matrix over GF(2)
gap> Codeword( GeneratorMat( StandardFormCode( C ) ));
[ [ 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 0 1 0 1 0 0 1 1 ],
  [ 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 1 0 0 0 1 1 ],
  [ 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 1 0 1 1 1 0 0 ],
  [ 0 0 0 1 0 0 0 0 0 0 0 0 0 1 1 0 1 1 0 1 0 1 1 0 0 ],
  [ 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 1 1 0 1 0 1 1 0 ],
  [ 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0 1 ],
  [ 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 1 0 1 1 1 1 0 0 1 ],

```

```

[ 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 1 0 1 1 0 1 1 0 ],
[ 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 1 1 0 1 1 1 0 ],
[ 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 1 1 0 0 1 1 1 0 1 ],
[ 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 0 0 1 0 0 1 1 0 1 1 ],
[ 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 1 1 0 0 1 1 1 ] ]
gap> Minimum(List(AsSSortedList(C){[2..Size(C)]}, WeightCodeword ));
8

```

Отже, було побудовано $[24,12,8]$ -код за груповим кільцем групи $C_2 \times A_4$.

В.6. Знаходження кодів за групою $C_2 \times C_2 \times S_3$

З'ясуємо інформацію, що стосується побудови розширених бінарних самодуальних кодів Голя за груповим кільцем групи $C_2 \times C_2 \times S_3$. Групу можна визначити як $C_2 \times C_2 \times S_3 = \langle x, y, z, w \mid x^2 = y^2 = z^2 = w^3 = 1, xy = yx, xz = zx, xw = wx, yz = zy, yw = wy, zwzw = 1 \rangle$.

```

gap> G:=SmallGroup(24,14);;StructureDescription(G);
"C2 x C2 x S3"
gap> f:=FreeGroup(4);
<free group on the generators [ f1, f2, f3, f4 ]>
gap> H:=f/[f.1^2,f.2^2,f.3^3,
f.4^2,f.1*f.2*f.1*f.2, f.1*f.3*f.1*f.3^2, f.1*f.4*f.1*f.4,
f.2*f.3*f.2*f.3^2, f.2*f.4*f.2*f.4, f.3*f.4*f.3*f.4];
<fp group on the generators [ f1, f2, f3, f4 ]>
gap> IsomorphismGroups(H,G);
[ f1, f2, f3, f4 ] -> [ f2, f3, f4^2, f1*f2*f4 ]

```

Образами символів x, y, z у S_{24} будуть, наприклад, підстановки

$$x = (1, 2), \quad y = (3, 4), \quad z = (5, 6, 7), \quad z = (5, 6).$$

```

gap> x:=(1,2);;
gap> y:=(3,4);;
gap> z:=(5,6,7);;
gap> w:=(5,6);;
gap> Ie:=();;
gap> x^2=Ie;y^2=Ie;z^3=Ie;w^2=Ie;
true
true
true
true
gap> x*y=y*x;x*z=z*x;x*w=w*x;y*z=z*y;y*w=w*y;z*w*z*w=Ie;
true
true
true
true
true
true
gap> H:=Group(x,y,z,w);
Group([ (1,2), (3,4), (5,6,7), (5,6) ])
gap> IsomorphismGroups(H,G);
[ (1,2), (3,4), (5,6,7), (5,6) ] -> [ f3, f2, f4, f1*f4 ]

```

Задамо порядок елементів на групі $C_2 \times C_2 \times S_3$ порядку 24, та перевіriamo, що вказані елементи при визначені порядку не повторюються.

```

gap> g:=
> Ie, z, z^2,
> x, x*z, x*z^2,
> y, y*z, y*z^2,
> x*y, x*y*z, x*y*z^2,
> w, w*z, w*z^2,
> w*x, w*x*z, w*x*z^2,
> w*y, w*y*z, w*y*z^2,
> w*x*y, w*x*y*z, w*x*y*z^2
> ];;
gap> Length(Set(g));

```

Знайдемо матрицю індексів дії регулярного зображення σ на довільному елементі

$$\begin{aligned} v = & \alpha_1 + \alpha_2 z + \alpha_3 z^2 + \alpha_4 x + \alpha_5 xz + \alpha_6 xz^2 + \\ & \alpha_7 y + \alpha_8 yz + \alpha_9 yz^2 + \alpha_{10} xy + \alpha_{11} xyz + \alpha_{12} xyz^2 + \\ & \alpha_{13} w + \alpha_{14} wz + \alpha_{15} wz^2 + \alpha_{16} wx + \alpha_{17} wxz + \alpha_{18} wxz^2 + \\ & \alpha_{19} wy + \alpha_{20} wyz + \alpha_{21} wyz^2 + \alpha_{22} wxy + \alpha_{23} wxyz + \alpha_{24} wxyz^2 \end{aligned}$$

групового кільця $C_2 \times C_2 \times S_3$, що відповідає порядку обернених елементів до вказаних.

```
gap> Sg:=[];;
gap> for i in g do
> A:=[];
> for j in g do
> Add(A,Position(g,i^(-1)*j));od;
> Add(Sg,A);od;
gap> Sg;
[ [ 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 ],
  [ 3,1,2,6,4,5,9,7,8,12,10,11,14,15,13,17,18,16,20,21,19,23,24,22 ],
  [ 2,3,1,5,6,4,8,9,7,11,12,10,15,13,14,18,16,17,21,19,20,24,22,23 ],
  [ 4,5,6,1,2,3,10,11,12,7,8,9,16,17,18,13,14,15,22,23,24,19,20,21 ],
  [ 6,4,5,3,1,2,12,10,11,9,7,8,17,18,16,14,15,13,23,24,22,20,21,19 ],
  [ 5,6,4,2,3,1,11,12,10,8,9,7,18,16,17,15,13,14,24,22,23,21,19,20 ],
  [ 7,8,9,10,11,12,1,2,3,4,5,6,19,20,21,22,23,24,13,14,15,16,17,18 ],
  [ 9,7,8,12,10,11,3,1,2,6,4,5,20,21,19,23,24,22,14,15,13,17,18,16 ],
  [ 8,9,7,11,12,10,2,3,1,5,6,4,21,19,20,24,22,23,15,13,14,18,16,17 ],
  [ 10,11,12,7,8,9,4,5,6,1,2,3,22,23,24,19,20,21,16,17,18,13,14,15 ],
  [ 12,10,11,9,7,8,6,4,5,3,1,2,23,24,22,20,21,19,17,18,16,14,15,13 ],
  [ 11,12,10,8,9,7,5,6,4,2,3,1,24,22,23,21,19,20,18,16,17,15,13,14 ],
  [ 13,14,15,16,17,18,19,20,21,22,23,24,1,2,3,4,5,6,7,8,9,10,11,12 ],
  [ 14,15,13,17,18,16,20,21,19,23,24,22,3,1,2,6,4,5,9,7,8,12,10,11 ],
```

```
[ 15,13,14,18,16,17,21,19,20,24,22,23,2,3,1,5,6,4,8,9,7,11,12,10 ],
[ 16,17,18,13,14,15,22,23,24,19,20,21,4,5,6,1,2,3,10,11,12,7,8,9 ],
[ 17,18,16,14,15,13,23,24,22,20,21,19,6,4,5,3,1,2,12,10,11,9,7,8 ],
[ 18,16,17,15,13,14,24,22,23,21,19,20,5,6,4,2,3,1,11,12,10,8,9,7 ],
[ 19,20,21,22,23,24,13,14,15,16,17,18,7,8,9,10,11,12,1,2,3,4,5,6 ],
[ 20,21,19,23,24,22,14,15,13,17,18,16,9,7,8,12,10,11,3,1,2,6,4,5 ],
[ 21,19,20,24,22,23,15,13,14,18,16,17,8,9,7,11,12,10,2,3,1,5,6,4 ],
[ 22,23,24,19,20,21,16,17,18,13,14,15,10,11,12,7,8,9,4,5,6,1,2,3 ],
[ 23,24,22,20,21,19,17,18,16,14,15,13,12,10,11,9,7,8,6,4,5,3,1,2 ],
[ 24,22,23,21,19,20,18,16,17,15,13,14,11,12,10,8,9,7,5,6,4,2,3,1 ] ]
```

З допомогою подальшого коду з'ясуємо, коли матриця $\sigma(v)$ буде симетрична ($\sigma(v) = \sigma(v)^T$).

```
gap> SymSg:=List([1..24],i->List([1..24],j->Sg[i][j]));;
gap> for i in [1..24] do
> for j in [1..24] do
> if Sg[i][j]>Sg[j][i] then
> dat:=true;
> for ki in [1..24] do
> for kj in [1..24] do
> if SymSg[ki][kj]=Sg[i][j] then
> if dat then Print("a",Sg[i][j],"=a",Sg[j][i]," "); fi;
> dat:=false;
> SymSg[ki][kj]:=Sg[j][i];
> fi;
> od;od;
> fi;
> od;od;
a3=a2, a6=a5, a9=a8, a12=a11,
gap> SymSg;
[ [ 1,2,2,4,5,5,7,8,8,10,11,11,13,14,15,16,17,18,19,20,21,22,23,24 ],
[ 2,1,2,5,4,5,8,7,8,11,10,11,14,15,13,17,18,16,20,21,19,23,24,22 ],
[ 2,2,1,5,5,4,8,8,7,11,11,10,15,13,14,18,16,17,21,19,20,24,22,23 ],
[ 4,5,5,1,2,2,10,11,11,7,8,8,16,17,18,13,14,15,22,23,24,19,20,21 ],
[ 5,4,5,2,1,2,11,10,11,8,7,8,17,18,16,14,15,13,23,24,22,20,21,19 ],
```

```
[ 5,5,4,2,2,1,11,11,10,8,8,7,18,16,17,15,13,14,24,22,23,21,19,20 ],
[ 7,8,8,10,11,11,1,2,2,4,5,5,19,20,21,22,23,24,13,14,15,16,17,18 ],
[ 8,7,8,11,10,11,2,1,2,5,4,5,20,21,19,23,24,22,14,15,13,17,18,16 ],
[ 8,8,7,11,11,10,2,2,1,5,5,4,21,19,20,24,22,23,15,13,14,18,16,17 ],
[ 10,11,11,7,8,8,4,5,5,1,2,2,22,23,24,19,20,21,16,17,18,13,14,15 ],
[ 11,10,11,8,7,8,5,4,5,2,1,2,23,24,22,20,21,19,17,18,16,14,15,13 ],
[ 11,11,10,8,8,7,5,5,4,2,2,1,24,22,23,21,19,20,18,16,17,15,13,14 ],
[ 13,14,15,16,17,18,19,20,21,22,23,24,1,2,2,4,5,5,7,8,8,10,11,11 ],
[ 14,15,13,17,18,16,20,21,19,23,24,22,2,1,2,5,4,5,8,7,8,11,10,11 ],
[ 15,13,14,18,16,17,21,19,20,24,22,23,2,2,1,5,5,4,8,8,7,11,11,10 ],
[ 16,17,18,13,14,15,22,23,24,19,20,21,4,5,5,1,2,2,10,11,11,7,8,8 ],
[ 17,18,16,14,15,13,23,24,22,20,21,19,5,4,5,2,1,2,11,10,11,8,7,8 ],
[ 18,16,17,15,13,14,24,22,23,21,19,20,5,5,4,2,2,1,11,11,10,8,8,7 ],
[ 19,20,21,22,23,24,13,14,15,16,17,18,7,8,8,10,11,11,1,2,2,4,5,5 ],
[ 20,21,19,23,24,22,14,15,13,17,18,16,8,7,8,11,10,11,2,1,2,5,4,5 ],
[ 21,19,20,24,22,23,15,13,14,18,16,17,8,8,7,11,11,10,2,2,1,5,5,4 ],
[ 22,23,24,19,20,21,16,17,18,13,14,15,10,11,11,7,8,8,4,5,5,1,2,2 ],
[ 23,24,22,20,21,19,17,18,16,14,15,13,11,10,11,8,7,8,5,4,5,2,1,2 ],
[ 24,22,23,21,19,20,18,16,17,15,13,14,11,11,10,8,8,7,5,5,4,2,2,1 ] ]
```

Остання матриця вказує вигляд індексів у симетричній матриці $\sigma(v)$ після заміни: $\alpha_3 = \alpha_2$, $\alpha_6 = \alpha_5$, $\alpha_9 = \alpha_8$, $\alpha_{12} = \alpha_{11}$.

Наступний код шукатиме всі лінійні коди породженні $\sigma(v)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$ та обчисленнями командами пакету GUAVA шукатиме їх мінімальну відстань.

```
par> i:=0;;DistList:=[];;
> for a1 in F do
> for a2 in F do
> for a4 in F do
> for a5 in F do
> for a7 in F do
> for a8 in F do
> for a10 in F do
> for a13 in F do
```

```

> for a14 in F do
> for a15 in F do
> for a16 in F do
> for a17 in F do
> for a18 in F do
> for a19 in F do
> for a20 in F do
> for a21 in F do
> for a22 in F do
> for a23 in F do
> a24:=a1+a4+a7+a10+a13+a14+a15+a16+a17+a18+a19+a20+a21+a22+a23;
> a11:=a2+a5+a8+a13*a14+a13*a15+a14*a15+a16*a17+a16*a18+a17*a18+a19*a20+
      a19*a21+a20*a21+a22*a23+a22*a24+a23*a24;
> SgM:=[
> [a1,a2,a2,a4,a5,a5,a7,a8,a8,a10,a11,a11,
      a13,a14,a15,a16,a17,a18,a19,a20,a21,a22,a23,a24],
> [a2,a1,a2,a5,a4,a5,a8,a7,a8,a11,a10,a11,
      a14,a15,a13,a17,a18,a16,a20,a21,a19,a23,a24,a22],
> [a2,a2,a1,a5,a5,a4,a8,a8,a7,a11,a11,a10,
      a15,a13,a14,a18,a16,a17,a21,a19,a20,a24,a22,a23],
> [a4,a5,a5,a1,a2,a2,a10,a11,a11,a7,a8,a8,
      a16,a17,a18,a13,a14,a15,a22,a23,a24,a19,a20,a21],
> [a5,a4,a5,a2,a1,a2,a11,a10,a11,a8,a7,a8,
      a17,a18,a16,a14,a15,a13,a23,a24,a22,a20,a21,a19],
> [a5,a5,a4,a2,a2,a1,a11,a11,a10,a8,a8,a7,
      a18,a16,a17,a15,a13,a14,a24,a22,a23,a21,a19,a20],
> [a7,a8,a8,a10,a11,a11,a1,a2,a2,a4,a5,a5,
      a19,a20,a21,a22,a23,a24,a13,a14,a15,a16,a17,a18],
> [a8,a7,a8,a11,a10,a11,a2,a1,a2,a5,a4,a5,
      a20,a21,a19,a23,a24,a22,a14,a15,a13,a17,a18,a16],
> [a8,a8,a7,a11,a11,a10,a2,a2,a1,a5,a5,a4,
      a21,a19,a20,a24,a22,a23,a15,a13,a14,a18,a16,a17],
> [a10,a11,a11,a7,a8,a8,a4,a5,a5,a1,a2,a2,
      a22,a23,a24,a19,a20,a21,a16,a17,a18,a13,a14,a15],
> [a11,a10,a11,a8,a7,a8,a5,a4,a5,a2,a1,a2,

```



```

1-2-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 ]
2-4-[ 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 1 1 1 ]
3-2-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 ]
4-4-[ 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 1 1 1 ]
5-2-[ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 ]

.....

48380-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 ]
48381-4-[ 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 1 1 1 0 1 0 0 0 ]
48382-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 1 ]
48383-4-[ 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 1 1 1 1 0 0 0 0 ]
48384-2-[ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 ]
gap> Collected(DistList);
[ [ 2, 1536 ], [ 4, 46848 ] ]

```

Таким чином є 48384 елементів $v \in \mathbb{F}_2(C_2 \times C_2 \times S_3)$, що $\sigma(\alpha) = \sigma(\alpha)^T$, $\sigma(\alpha)^2 = 0_{24 \times 24}$, $\text{Rank}(\sigma(\alpha)) = 12$ а з лінійних кодів породжених $\sigma(v)$ $[24, 12, 2]$ -кодів є 1536, $[24, 12, 4]$ -кодів є 46848 і нема **жодного** $[24, 12, 8]$ -коду.

ДОДАТОК Г. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Публікації, в яких опубліковано основні наукові
результати дисертації

1. Тилищак О. А. Про незвідні модулярні зображення даного степеня скінченної p -групи над комутативним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2002. Вип. 7. С. 108–114.
2. Тилищак О. А. Про незвідні модулярні зображення даного степеня скінченної p -групи над напівпервісним комутативним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2003. Вип. 8. С. 156–159.
3. Тилищак О. А. Про незвідні модулярні зображення 2-групи даного степеня над напівпервісним локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2004. Вип. 9. С. 103–106.
4. Тилищак О. А. Про модулярні зображення циклічної 2-групи над локальною областю цілісності. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики*. 2005. Вип. 10–11. С. 137–141.
5. Тилищак О. А. Зображення 2-го степеня групи діедра порядку $2p$ над деякими комутативними локальними кільцями. *Наук. вісник*

- Ужгород. ун-ту. Серія математики і інформатики.* 2008. Вип. 16. С. 188–192.
6. Tylyshchak A. A. On maximal unipotent subgroups of the general linear group over commutative rings. *Bulletin of University of Kyiv. Ser.: Phys. & Math.* 2010. Vol. No 3. P. 115–117.
 7. Динис Р. Ф., Тилищак О. А. Про звідність матриць деякого вигляду над комутативними локальними кільцями головних ідеалів. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики.* 2012. Вип. 23, № 1. С. 57–62.
 8. Bondarenko V. M., Bortos M. Yu., Dinis R. F., Tylyshchak A. A. Reducibility and Irreducibility of Monomial Matrices over Commutative Rings. *Algebra Discret Math.* 2013. Vol. 16, No 2. P. 171–187.
 9. Бортош М. Ю., Тилищак О. А. Приводимость некоторых мономиальных матриц над коммутативными локальными кольцами. *Науковий часопис НПУ ім. М. П. Драгоманова. Серія 1. Фіз.-мат. науки.* Київ. : НПУ ім. М. П. Драгоманова. 2013. № 14. С. 68–78.
 10. Bondarenko V. M., Tylyshchak A. A., Stoika M. V. On the equivalence of matrices over commutative rings modulo ideals. *Algebra and Discrete Math.* 2014. Vol. 17, No 1. P. 12–19.
 11. Динис Р., Тилищак О. Про звідність деяких мономіальних матриць над комутативними кільцями. *Вісник Київ. нац. ун-ту ім. Т. Шевченка. Серія: математики і механіки.* 2014. Вип. 2 (32). С. 20–23.
 12. Gildea J., Tylyshchak A. Torsion units in the integral group ring of $PSL(3, 4)$. *J. Algebra Appl.* 2016. Vol. 15, No 1, 1650013. 9 p.

13. Bondarenko V. M., Bortos M. Yu., Dinis R. F., Tylyshchak A. A. Indecomposable and irreducible t -monomial matrices over commutative rings. *Algebra and Discrete Math.* 2016. Vol. 22, No 1. P. 11–20.
14. Dougherty S. T., Gildea J., Taylor R., Tylyshchak A. Group rings, G -codes and constructions of self-dual and formally self-dual codes. *Designs, Codes and Cryptography.* 2018. Vol. 86, Is. 9. P. 2115–2138.
15. Тилищак О. А. Про число нерозкладних модулярних зображень циклічної p -групи над скінченним локальним кільцем. *Прикл. проблеми механіки і математики.* 2018. Вип. 16. С. 19–29.
16. Тилищак О. А. Про незвідність мономіальних матриць 7-го порядку над локальними кільцями. *Вісник Київ. нац. ун-ту ім. Т. Шевченка. Серія: фіз.-мат. науки.* 2018. Вип. № 3. С. 37–44.
17. Bondarenko V. M., Gildea J., Tylyshchak A. A., Yurchenko N. V. On hereditary reducibility of 2-monomial matrices over commutative rings. *Algebra and Discrete Math.* 2019. Vol. 27, No 1. P. 1–11.
18. Dougherty S., Gildea J., Korban A., Kaya A., Tylyshchak A., Yildiz B. Bordered Constructions of Self-Dual Codes from Group Rings and New Extremal Binary Self-Dual Codes. *Finite Fields and Their Applications.* 2019. Vol. 57. P. 108–127.
19. Тилищак О. А. Про максимальні уніпотентні підгрупи спеціальної лінійної групи над комутативним кільцем. *Укр. мат. журн.* 2019. Т. 71, № 8. С. 1150–1156.
20. Тилищак О. А. Про спадково незвідні унімономіальні зображення циклічних p -груп над локальними кільцями характеристики p .

Наук. вісник Ужгород. ун-ту. Серія математики і інформатики. 2019. Вип. № 1 (34). С. 52–59.

21. Тилищак О. А. Про число нерозкладних модулярних зображень циклічної p -групи над локальним кільцем скінченної довжини. *Мат. методи та фіз.-мех. поля.* 2019. Вип. 62, № 1. С. 74–82.

Публікації, які додатково відображають наукові результати дисертації

22. Тилищак О. А., Юрченко Н. В., Цімболинець Р. Ф. Нерозкладність однієї матриці довільного порядку над локальним кільцем. *Наук. вісник Ужгород. ун-ту. Серія математики і інформатики.* 2016. Вип. № 1 (28). С. 135–139.
23. Dougherty St., Gildea J., Taylor R., Tylyshchak A. Constructions of Self-Dual and Formally Self-Dual Codes from Group Rings. ArXiv preprint arXiv:1604.07863v1, 2016. 20 p. URL: <https://arxiv.org/abs/1604.07863v1> (date of appeal: 28.03.2020).

Публікації, які засвідчують апробацію матеріалів дисертації

24. Tylyshchak O. Irreducible modular representation of the given degree of finite p -group over commutative local ring of characteristic p^s . *IV International Algebraic Conference in Ukraine : abstracts*, L'viv, August 4–9, 2003. L'viv : Ivan Franko National University of L'viv, 2003. P. 222–223.
25. Tylyshchak A. On maximal unipotent subgroups of the general linear group over commutative ring. *XI International Mathematical Kravchuk*

- Conference* : conference materials, Kyiv, May 18–20, 2006. Kyiv. : TOV «Zadruha», 2006. P. 616.
26. Tylyshchak A. A. On Irreducible Modular Representations of Given Degree of Finite Group over Commutative Local Ring. *International Conference of Humboldt-Kolleg Series in Kyiv «Humboldt Cosmos: Science and Society», Kyiv, November 19–22, 2009* : abstracts, Kyiv, November 19–22, 2009. Kyiv : Embassy of the Federal Republic of Germany Kyiv, 2009. P. 45.
 27. Динис Р. Ф., Тилищак О. А. Про еквівалентність матриць деякого вигляду над локальними областями головних ідеалів. *Десята наукова відкрита конф. інституту прикладної математики та фундаментальних наук ІМФН* : зб. матеріалів та програма конф. [«PSC-IMFS-10»] (Львів, 17–18 травня 2012 р.). Львів : Видавництво Львівської політехніки, 2012. С. А31.
 28. Tylyshchak A., Bortosh M. On Reducibility of Monomial Matrixes over Commutative Local Rings. *IX International Algebraic Conference in Ukraine* : abstracts of reports, L'viv, July 8–13, 2013. L'viv : Ivan Franko National University of L'viv, 2013. P. 201.
 29. Bondarenko V., Dinis R., Tylyshchak A. On irreducibility of some matrices over p -adic integers. *Fifth International Conference on Analytic Number Theory and Spatial Tessellations* : abstracts, Kiev, September 16–20, 2013. Kyiv : Institute of Mathematics of NAS of Ukraine, 2013. P. 6.
 30. Dinis R. F., Tylyshchak A. A., Yurchenko N. V. On indecomposability of some monomial matrices over local rings. *X International*

Algebraic Conference in Ukraine dedicated to the 70th anniversary of Yu. A. Drozd : abstracts, Odessa, August 20–27, 2015. Odessa : TES, 2015. P. 32.

31. Stoika M. V., Tylyshchak A. A. On classifying the matrices over commutative rings up to equivalence. *International Conference of Young Mathematicians* : book of abstracts, Kyiv, June 3–6, 2015. Kyiv : Institute of Mathematics of NAS of Ukraine, 2015. P. 23.
32. Динис Р. Ф., Тилищак О. А., Юрченко Н. В. Про нерозкладність мономіальних матриць спеціального вигляду над локальними кільцями. *Міжнар. мат. конф. «Методика викладання та методи досліджень в математиці»* : матеріали конф., Берегове, 21–23 квітня 2016. Ужгород : ТОВ «PIK-Y», 2016. С. 28.
33. Tylyshchak A. A. On the estimation of the number of indecomposable representations of given degree of a cyclic group. *XI International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V. V. Kirichenko* : abstracts, Kyiv, July 3–7, 2017. Kyiv : Institute of Mathematics of NAS of Ukraine, 2017. P. 137.
34. Bondarenko V., Gildea J., Salim M., Tylyshchak A. On the number of indecomposable representations of given degree of a cyclic group over local rings of finite length. *The Second International Conference on Groups, Group Rings and Related Topics* : abstracts [electronic resource], Khorfakkan (UAE), November 19–22, 2017. Khorfakkan (UAE), 2017. P. 10. URL: https://conferences.uaeu.ac.ae/ggrrt2017/en/abstracts_ggrrt.pdf (date of appeal: 28.03.2020).

35. Тилищак О. Деякі нерозкладні модулярні зображення циклічної p -групи над локальним кільцем скінченної довжини. *Між-нар. наукова конф. «Сучасні проблеми механіки та математики»* : збірник наукових праць : у 3-х т. / за заг. ред. А. М. Самойленка та Р. М. Кушніра [Електронний ресурс] (Львів, 22–25 травня 2018). Львів, 2018. Т. 3. С. 237. URL: http://www.iapmm.lviv.ua/mpmm2018/Volume_3.pdf (дата звернення 28.03.2020).
36. Tylyshchak A. A. On irreducibility of monomial matrices of order 7 over local rings. *XII International Algebraic Conference in Ukraine dedicated to the 215th anniversary of V. Bunyakovsky* : abstracts, 2019, July 02-06, Vinnytsia, Ukraine. Vinnytsia : Vasyl' Stus Donetsk National University, 2019. P. 117–118.

ДОДАТОК Д. АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

- 1) Четверта міжнародна алгебраїчна конференція в Україні (Львів, 4–9 серпня 2003р.).
- 2) Одинадцята міжнародна наукова конференція імені академіка Михайла Кравчука (Київ, 18–20 травня 2006 р.).
- 3) Міжнародна конференція Humboldt-Kolleg Series in Kyiv (Київ, 19–22 листопада 2009).
- 4) Десята відкрита науковій конференція інституту прикладної математики та фундаментальних наук (Львів, 17–18 травня 2012 р.).
- 5) Дев'ята міжнародна алгебраїчна конференція в Україні (Львів, 8–13 липня 2013 р.).
- 6) П'ята міжнародна конференція з аналітичної теорії чисел та просторових мозаїк (Київ, 16–20 вересня 2013 р.)
- 7) Десята міжнародна алгебраїчна конференція в Україні, присвячена 70-річчю Ю. А. Дрозда (Одеса, 20–27 серпня 2015 р.).
- 8) П'ятнадцята міжнародна науковій конференція імені академіка Михайла Кравчука (Київ, 15–17 травня 2014 р.).
- 9) Міжнародна алгебраїчна конференції, присвячена 100-річчю від дня народження Л. А. Калужніна (Київ, 7–12 липня 2014 р.).
- 10) Міжнародна мат. конференція «Методика викладання та методи досліджень в математиці» (Берегове, 21–23 квітня 2016 р.).

- 11) Одинадцята міжнародна алгебраїчна конференція в Україні, присвячена 75-річчю В. В. Кириченка (Київ, 3–7 липня 2017 р.).
- 12) Друга міжнародна конференція про групи, групові кільця і пов'язані теми (Хорфаккан (ОАЕ), 19–22 листопада 2017 р.).
- 13) Міжнародна наукова конференція «Сучасні проблеми механіки та математики» (Львів, 22–25 травня 2018 р.)
- 14) Дванадцята міжнародна алгебраїчна конференція в Україні, присвячена 215-й річниці з дня народження В. Буняковського (Вінниця, 2–6 липня 2019 р.).
- 15) Семінари кафедри алгебри Ужгородського національного університету (Ужгород, 2003–2019).
- 16) Алгебраїчний семінар Інституту математики ім. А. Ренні Угорської академії наук (Будапешт (Угорщина), 2005).
- 17) Науковий семінар відділення інженерії факультету механіки та електронної інженерії Технологічного інституту Сліго (Сліго (Ірландія), 2012).
- 18) Наукові семінари відділення комп'ютерних наук та математики Університету Честер (Честер (Великобританія), 2013, 2019).
- 19) Алгебраїчні семінари Інституту математики Кошицького університету ім. П. Й. Шафарика (Кошице (Словаччина), 2019).
- 20) Алгебраїчний семінар Інституту математики НАН України (Київ, 2019).
- 21) Підсумковий семінар кафедри алгебри та мат. логіки Київського національного університету ім. Т. Шевченка (Київ, 2020).