Міністерство освіти і науки, молоді та спорту України

Державний вищий навчальний заклад
«Ужгородський національний університет»

П. М. Гудивок, В. П. Рудько, О. А. Тилищак, Н. В. Юрченко

ЛІНІЙНІ ГРУПИ

Ужгород 2011

УДК 512.8

Лінійні групи / Гудивок П. М., Рудько В. П., Тилищак О. А., Юрченко Н. В. – Ужгород: , 2011. — 84 с.

В посібнику викладено елементи теорії матричних груп над тілами, полями та деякими комутативними кільцями.

Рецензенти:

Доктор фізико-математичних наук, професор *В. М. Бондаренко*

Кандидат фізико-математичних наук, доцент *І. В. Шапочка*

Рекомендовано до друку Вченою радою математичного факультету Державного вищого навчального закладу «Ужгородський національний університет», протокол № 10 від 24 червня 2011 р.

ЗМІСТ

Вступ

В книзі вивчаються властивості матричних груп над полями і над кільцями.

В першому розділі розглядуються групи матриць над полями. Тут вивчається нормальна будова групи $GL(n,T)$ (T — тіло), викладено результати Дж. Діксона і В. П. Платонова про умови цілковитої звідності матричних груп, теорема Бернсайда про скінченність матричної групи, теорема Шура про локальну скінченність періодичної матричної групи, теорема Кліффорда про нормальні підгрупи матричної групи, теорема Супруненка про примітивні розв'язні матричні групи, теорема Колчіна, Мальцева про розв'язні групи матриць над алгебраїчно замкненим полем. Відмітимо, що матеріал цього розділу тісно пов'язаний з відповідним матеріалом книги Д. О. Супруненка «Группы матриц» [1]. Цей розділ є основою курсу за вибором «Лінійні групи» для студентів 5-го курсу математичного факультету.

В другому розділі викладено теорію силовських p-підгруп повної лінійної групи $GL(n,T)$ над полем T, засновану на теорії зображень скінченних груп над полями. У випадку алгебраїчно замкнутого поля T, $\operatorname{char} T \neq p$ силовські p-підгрупи в $GL(n,T)$ вивчив Д. О. Супруненко [2]. Якщо T довільне поле характеристики нуль, задачу описання силовських p-підгруп групи $GL(n,T)$ розв'язали Р. Т. Вольвачев [3] і В. С. Конюх [4] (випадок $p = 2$ див. також [5]). Відмітимо, що В. М. Петечук [6] запропорнував свій підхід до вивчення силовських p-підгруп групи $GL(n,T)$.

В третьому розділі розглянуто результати Г. Мінковського про періодичні підгрупи групи $GL(n,\mathbb{Z})$, викладено теорію І. Менніке [7] конгруенц-підгруп групи $GL(n,\mathbb{Z})$ і приводяться результати П. М. Гудивка і В. П. Рудька [8–9] про силовські p-підгрупи групи $GL(n,\mathbb{Z})$ та результати О. А. Тилищака [10] про силовські p-підгруп повної лінійної групи $GL(n,K)$ над кільцем K характеристики p^s.

Останні два розділи можуть бути корисними для майбутніх магістрів і аспірантів.

РОЗДІЛ 1. ПІДГРУПИ ПОВНОЇ ЛІНІЙНОЇ ГРУПИ

§1. Повна лінійна група

Нехай K — асоціативне кільце з одиницею, $M(n,K)$ — кільце всіх квадратних матриць порядку n над кільцем K,

$$GL(n,K) = (M(n,K))^*$$

— мультиплікативна група кільця $M(n,K)$. Група $GL(n,K)$ складається з усіх оборотних квадратних матриць порядку n над кільцем K і називається *повною лінійною групою* степеня n над кільцем K. Кільце $M(n,K)$ є лівим модулем над кільцем K. Нагадаємо, якщо $A = (\alpha_{ij})$, $B = (\beta_{ij})$ — матриці з кільця $M(n,K)$, то

$$A + B = (\alpha_{ij} + \beta_{ij}), \quad AB = (\gamma_{ij}) \quad (\gamma_{ij} = \sum_{k=1}^{n} \alpha_{ik}\beta_{kj}).$$

Позначимо через e_{ij} — матрицю із кільця $M(n,K)$, всі елементи якої рівні нулю, за винятком елемента i-ого рядка та j-го стовпчика, що рівний одиниці. Матриці e_{ij} $(1 \leqslant i,j \leqslant n)$ називаються *матричними одиницями*. Має місце закон множення:

$$e_{ij} \cdot e_{rs} = \begin{cases} 0, & j \neq r; \\ e_{is}, & j = r. \end{cases}$$

Нехай $A = (\alpha_{ij})$. Тоді

$$A = \sum_{i,j} \alpha_{ij} e_{ij} = \sum_{i,j} e_{ij} \alpha_{ij}.$$

Нехай $i \neq j$ і $\lambda \in K$. Матриці

$$t_{ij}(\lambda) = E + \lambda e_{ij}$$

(E — одинична матриця) називаються *елементарними матрицями*. Відмітимо, що

$$t_{ij}(\alpha)t_{ij}(\beta) = t_{ij}(\alpha + \beta).$$

Матриці

$$d_i(\lambda) = \mathrm{diag}[1, \ldots, 1, \lambda, 1, \ldots, 1]$$

(i-тове місце діагоналі зайняте елементом λ кільця K) називаються *d-матрицями*.

Лема 1.1. *Добуток $t_{jk}(\lambda) \cdot A$ є матриця, що одержується з матриці A, якщо до j-го рядка додати k-ий, домножений зліва на λ. Добуток $A \cdot t_{jk}(\lambda)$ є матриця, що одержується з матриці A, якщо до k-го стовпчика додати j-ий, домножений справа на λ. Добуток $d_i(\lambda) \cdot A$ є матриця, що одержується з матриці A множенням зліва i-го рядка на λ. Аналогічно, $A \cdot d_i(\lambda)$ одержується множенням справа на λ i-го стовпчика в A.*

Перші дві дії над матрицями, що вказані в лемі, називаються *елементарними перетвореннями матриць*. Таким чином, елементарне перетворення матриці — це множення її зліва або справа на елементарну матрицю.

Так як $t_{jk}(\lambda)t_{jk}(-\lambda) = E$, то

$$t_{jk}(\lambda) \in GL(n,K) \quad \text{і} \quad t_{jk}(\lambda)^{-1} = t_{jk}(-\lambda).$$

Через $[a,b]$ позначається *комутатор* елементів a, b групи G :

$$[a,b] = a^{-1}b^{-1}ab.$$

Лема 1.2 (Лема Басса; [2]). *Нехай $n > 2$ та i, j, k — три різних індекси. Тоді*

$$[t_{ik}(\lambda), t_{kj}(\mu)] = t_{ij}(\lambda\mu).$$

Доведення.

$$[t_{ik}(\lambda), t_{kj}(\mu)] = (E - \lambda e_{ik})(E - \mu e_{kj})(E + \lambda e_{ik})(E + \mu e_{kj}) = E + \lambda\mu e_{ij}.$$

Всі елементарні матриці $t_{jk}(\lambda)$ породжують підгрупу $SL(n,\, K) \subset GL(n, K)$, що називається *спеціальною лінійною групою* степеня n над кільцем K.

Лема 1.3. *Нехай α, β — ненульові елементи тіла T. Елементарними перетвореннями над рядками матрицю*

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

можна звести до кожного з виглядів:

$$\begin{pmatrix} 1 & 0 \\ 0 & \alpha\beta \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & \beta\alpha \end{pmatrix}.$$

Доведення. За допомогою елементарних перетворень над рядками одержимо:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \to \begin{pmatrix} \alpha & 0 \\ 1 & \beta \end{pmatrix} \to \begin{pmatrix} 0 & -\alpha\beta \\ 1 & \beta \end{pmatrix} \to \begin{pmatrix} 0 & -\alpha\beta \\ 1 & \alpha\beta \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 0 \\ 1 & \alpha\beta \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & \alpha\beta \end{pmatrix};$$
$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \to \begin{pmatrix} \alpha & 1 \\ 0 & \beta \end{pmatrix} \to \begin{pmatrix} \alpha & 1 \\ -\beta\alpha & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ -\beta\alpha & 0 \end{pmatrix} \to$$
$$\to \begin{pmatrix} 1 & 1 \\ 0 & \beta\alpha \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & \beta\alpha \end{pmatrix}.$$

Теорема 1.1. *Нехай $K = T$ — тіло. Тоді кожний елемент групи $GL(n, T)$ можна представити у вигляді добутку $s \cdot d(\lambda)$, де $s \in SL(n, T)$, $d(\lambda) = d_n(\lambda)$, λ — ненульовий елемент тіла T.*

Доведення. В зв'язку з лемою 1.1, рядки матриць потрібно розглядати як елементи лівого лінійного простору над тілом T, а стовпці — як елементи правого лінійного простору над цим тілом. Матриця A порядку n над тілом T належить групі $GL(n, T)$ тоді і тільки тоді, коли система рядків (система стовпчиків) цієї матриці буде лінійно незалежною над тілом T (інакше кажучи, ця система буде базисом відповідного простору). Нехай $A \in GL(n, T)$ і нехай ненульовий елемент α першого стовпчика знаходиться в i-му рядку. Помноживши i-й рядок на $x\alpha^{-1}$ і послідовно додаючи до інших рядків, одержимо матрицю A_1, в якій, окрім α, всі елементи 1-го стовпчика будуть нульовими. Очевидно $A_1 = SA$, де $S \in SL(n, T)$. Якщо $i \neq 1$, то в матриці A_1 до першого рядка додамо i-й рядок, а потім результат віднімемо від i-го рядка. В результаті одержимо матрицю

$$A_2 = \begin{pmatrix} \alpha & * \\ 0 & B \end{pmatrix},$$

де $B \in GL(n-1, T)$. При $i = 1$ позначаємо через A_2 матрицю A_1, яка вже має вказаний вигляд. Це дає можливість провести індукцію за n. Нехай матриця B елементарними перетвореннями над рядками приводиться до матриці $d_{n-1}(\beta)$. Тоді послідовні елементарні перетворення рядків

$$A_2 \to \begin{pmatrix} \alpha & * \\ 0 & d_{n-1}(\beta) \end{pmatrix} \to \begin{pmatrix} \alpha & 0 \\ 0 & d_{n-1}(\beta) \end{pmatrix} \to d_n(\alpha\beta)$$

приведуть до d-матриці.

Наслідок 1.1. *Група $SL(n,T)$ буде нормальною підгрупою в групі $GL(n,T)$.*

Доведення. Нехай $i,\ j < n$; $\alpha,\ \lambda \in T,\ \lambda \neq 0$. Тоді $d^{-1}(\lambda)t_{ij}(\alpha)d(\lambda) = t_{ij}(\alpha)$. Крім цього, $d^{-1}(\lambda)t_{nj}(\alpha)d(\lambda) = t_{nj}(\lambda^{-1}\alpha)$; $d^{-1}(\lambda)t_{in}(\alpha)d(\lambda) = t_{in}(\alpha\lambda)$, що доводить наслідок.

Нехай T^* — мультиплікативна група тіла $T, (T^*)'$ — комутант групи T^*, $\overline{T} = T^*/(T^*)'$ — фактор-група групи T^* за її комутантом $(T^*)'$. Образ елемента λ групи T^* в групі $\overline{T}$ будемо позначати через $\overline{\lambda}$.

Теорема 1.2 (Теорема Д'єдонне; [2]). *Існує функція* $\det : GL(n,T) \to T^*$, $\det : A \to |A|$ *така, що*
1) $|AB| = |A| \cdot |B|$ $(A,\ B \in GL(n,T))$;
2) $|C| = \overline{1}$ $(C \in SL(n,T))$;
3) $|d(\alpha)| = \overline{\alpha}$ $(\alpha \in T^*,\ d(\alpha) = \operatorname{diag}[1,\ \ldots,\ 1,\ \alpha])$.

Значення $|A|$ функції det названо *детермінантом Д'єдонне* матриці A над тілом T. Якщо T — поле, то детермінант Д'єдонне такий же, як і звичайний детермінант.

Якщо $A \in GL(n,T)$, і $A = C \cdot d(\alpha)$ $(C \in SL(n,T), \alpha \in T^*)$, то

$$|A| = |d(\alpha)| = \overline{\alpha}.$$

Відображення детермінант є гомоморфізм групи $GL(n,T)$ в групу $\overline{T}$, ядро якого містить спеціальну групу $SL(n,T)$ і всі діагональні матриці $d(\lambda)$, $\lambda \in (T^*)'$. Із леми 1.3 випливає, що $|\operatorname{diag}[\alpha_1,\ \ldots,\ \alpha_n]| = \overline{1}$, якщо $\alpha_1 \cdots \alpha_n \in (T^*)'$.

Теорема 1.3. *Нехай T — тіло і $n \geq 2$ Тоді*

$$SL(n,T) = \{A \in GL(n,T) \mid |A| = \overline{1}\}.$$

Доведення. Нехай

$$A \in GL(n,T), \quad A = S \cdot d(\lambda) \quad (S \in SL(n,T),\ \lambda \in T^*)$$

і $|A| = \overline{1}$. Тоді λ належить комутанту $T^{*\prime}$ групи T^*. Досить обмежитись випадком, коли $\lambda = [\alpha,\beta]$ — комутатор. З леми 1.3 випливає існування такої матриці $C \in SL(n,T)$, що $Cd(\beta^{-1}\alpha^{-1}) = C\operatorname{diag}[1,\ \ldots,\ 1,\beta^{-1}\alpha^{-1}] = \operatorname{diag}[1,\ \ldots,\ 1,\alpha^{-1}\beta^{-1}] = d(\alpha^{-1}\beta^{-1})$. Тоді $d(\lambda) = d(\alpha^{-1}\beta^{-1}\alpha\beta) = d(\alpha^{-1}\beta^{-1})d(\alpha\beta) = Cd(\beta^{-1}\alpha^{-1})d(\alpha\beta) = Cd(\beta^{-1}\alpha^{-1}\alpha\beta) = C \in \in SL(n,T)$ і тоді $A \in SL(n,T)$, що доводить теорему.

Наслідок 1.2. *Відображення* $\det : GL(n,T) \to \overline{T}$ *буде гомоморфізмом груп і* $\ker\det = SL(n,T)$.

Наслідок 1.3. *Нехай T — поле. Тоді*

$$SL(n,T) = \{A \in GL(n,T) |\ |A| = 1\}.$$

Наслідок 1.4. *Нехай $n \geq 2$ і T — тіло. Тоді $SL(n,T)$ — нормальна підгрупа групи $GL(n,T)$, фактор-група за якою є ізоморфна абелевій групі $\overline{T} = T^*/(T^*)'$.*

Наслідок 1.5. *Нехай T — тіло і $n \geq 2$. Всяка підгрупа в $GL(n,T)$, що містить $SL(n,T)$, буде нормальною підгрупою.*

Лема 1.4. *Нехай тіло T містить більше двох елементів. Тоді кожна елементарна матриця в групі $GL(2,T)$ буде комутатором в цій групі.*

Доведення. Нехай $\alpha \in T, \alpha \neq 0, \alpha \neq 1$. Тоді

$$\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (1-\alpha^{-1})\beta \\ 0 & 1 \end{pmatrix} = t_{12}(\gamma),$$

де $\gamma = (1-\alpha^{-1})\beta$ може бути довільним елементом з T. Звідси слідує доведення.

Теорема 1.4. *Нехай $n > 2$. Тоді комутант групи $SL(n,T)$ і комутант групи $GL(n,T)$ співпадають з групою $SL(n,T)$. Якщо тіло T не буде полем з двох елементів, то група $SL(2,T)$ також буде комутантом групи $GL(2,T)$.*

Доведення. З наслідку 1.4 випливає, що комутант групи $GL(n,T)$ міститься в групі $SL(n,T)$. Тоді для $n > 2$ теорема випливає з леми 1.2 Басса. Інший випадок слідує з леми 1.4.

Можна показати, що, якщо $n = 2$ і $|T| > 3$, то комутанти груп $GL(2,T), SL(2,T)$ співпадають з $SL(2,T)$.

Контрприклад. Нехай $\mathbb{Z}_2$ — поле із двох елементів. Тоді $GL(n,\mathbb{Z}_2) = SL(n,\mathbb{Z}_2)$ і матриці

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

породжують групу $GL(2,\mathbb{Z}_2)$. Комутант цієї групи суміщається з $\langle a \rangle \neq SL(2,\mathbb{Z}_2)$.

Контрприклад. Нехай $T = \mathbb{Z}_3$ — поле з трьох елементів. Група $GL(2,\mathbb{Z}_3)$ породжується матрицями:

$$a = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, c = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$(-a^2 = -b^2 = c^3 = d^2 = E, b^{-1}ab = a^{-1}, c^{-1}ac = b^{-1},$$

$$c^{-1}bc = (ba)^{-1}, d^{-1}ad = (ba)^{-1}, d^{-1}bd = b^{-1}, d^{-1}cd = (bac)^{-1}).$$

Матриці a, b, c породжують групу $SL(2,T)$, яка є комутантом групи $GL(2,T)$. Але комутант групи $SL(2,T)$ суміщається з групою $\langle a, b \rangle \neq SL(2,T)$.

Нехай, далі, $q = p^t$ — степінь простого числа p, P — поле із q елементів і $GL_n(q)$ — повна лінійна група матриць порядку n над полем P і $|GL_n(q)|$ — порядок групи $GL_n(q)$.

Теорема 1.5. $|GL_n(q)| = \prod_{i=0}^{n-1} (q^n - q^i)$.

Доведення. Нехай A — довільна матриця порядку n над полем P і a_1, a_2, ..., a_n — система рядків матриці A. Для того, щоб матриця A належала групі $GL_n(q)$ необхідно, щоб перший рядок a_1 був одним із $(q^n - 1)$ ненульових n-вимірних векторів над полем P. Якщо перший рядок a_1 уже вибраний, то другий рядок a_2 може бути будь-яким, окрім λa_1 (тобто не пропорційний першому). Таких рядків є $(q^n - q)$. Таким чином, існує $(q^n - 1) \cdot (q^n - q)$ можливостей для пари (a_1, a_2) рядків невиродженої матриці A. Якщо пара (a_1, a_2) перших двох рядків уже вибрана, то 3-ій рядок a_3 може бути будь-яким, окрім вектора

$$\lambda_1 a_1 + \lambda_2 a_2 \quad (\lambda_1, \lambda_2 \in P),$$

тобто 3-ій рядок може бути одним із $(q^n - q^2)$ векторів (при вибраних перших двох рядках). Продовжуючи міркування прийдемо до формули для порядку групи $GL_n(q)$. Теорема доведена.

Наслідок 1.6. $|SL(n,P)| = \frac{1}{q-1} \prod_{j=0}^{n-1} (q^n - q^j)$.

§2. Нормальна будова повної лінійної групи

Через $\mathfrak{Z}(G)$ будемо позначати *центр* групи G :

$$\mathfrak{Z}(G) = \{z \in G \mid zx = xz,\ x \in G\}.$$

Лема 2.1. *Нехай T — тіло. Тоді*

$$\mathfrak{Z}(GL(n,T)) = \{\lambda E | \lambda \in \mathfrak{Z}(T^*)\}.$$

Доведення. Нехай $A = (\alpha_{ij}) \in \mathfrak{Z}(GL(n,T))$ $(\alpha_{ij} \in T)$. Так як $t_{ij}(1)A = At_{ij}(1)$, то $e_{ij}A = Ae_{ij}$ і $\alpha_{ji} = 0$ $(j \neq i)$, $\alpha_{jj} = \alpha_{ii} = \lambda$. Тоді $A = \lambda E$. Так як $\alpha EA = A\alpha E$ $(\alpha \in T^*)$, то $\lambda \in \mathfrak{Z}(T^*)$. Лема доведена.

Наслідок 2.1. *Нехай T — тіло. Тоді*

$$\mathfrak{Z}(SL(n,T)) = SL(n,T) \cap \mathfrak{Z}(GL(n,T)).$$

Доведення. При $n = 1$ твердження наслідку очевидне. Нехай $n > 1$. Зрозуміло, що $SL(n,T) \cap \mathfrak{Z}(GL(n,T)) \subset \mathfrak{Z}(SL(n,T))$. Нехай $A \in \mathfrak{Z}(SL(n,T))$. З доведення леми 2.1 одержимо $A = \lambda E$ $(\lambda \in T^*)$. Так як $\operatorname{diag}[\alpha_1, \ldots, \alpha_n]A = A\operatorname{diag}[\alpha_1, \ldots, \alpha_n]$ $(\alpha_i \in T^*, \alpha_1 \ldots \alpha_n = 1)$, то $\lambda\alpha_i = \alpha_i\lambda$. Якщо $\alpha_1, \ldots, \alpha_{n-1}$ — довільні елементи із T^*, то для $\alpha_n = \alpha_{n-1}^{-1}, \ldots, \alpha_1^{-1}\,\alpha_1 \ldots \alpha_{n-1}\alpha_n = 1$ і, отже, $\lambda \in \mathfrak{Z}(T^*)$. Тому $A \in \mathfrak{Z}(GL(n,T))$. Наслідок доведено.

Підгрупу групи $GL(n,T)$, яка міститься в центрі цієї групи, будемо називати *центральною підгрупою*. Очевидно, центральна підгрупа є нормальною підгрупою. Розглянемо нормальні нецентральні підгрупи групи $GL(n,T)$.

Лема 2.2. *Нехай $n > 2$ і підгрупа H групи $GL(n,T)$ нормалізується спеціальною лінійною групою $SL(n,T)$. Якщо підгрупа H містить хоча б одну елементарну матрицю, то ця підгрупа містить всю групу $SL(n,T)$.*

Доведення. Якщо $h \in H$, $g \in SL(n,T)$, то обидва комутатори $[h,g] = h^{-1}g^{-1}hg$, $[g,h]$ належать підгрупі H. Нехай деяка елементарна матриця $t_{ij}(\alpha)$ належить нормальній підгрупі H групи $GL(n,T)$ $(n > 2)$. Скористаємось лемою Басса. Маємо

$$[t_{ij}(\alpha), t_{jk}(\beta)] = t_{ik}(\alpha\beta) \in H,$$

$$[t_{ri}(\gamma), t_{ik}(\alpha\beta)] = t_{rk}(\gamma\alpha\beta) \in H.$$

Звідси слідує, що група H містить всі елементарні матриці. Тоді H містить всю спеціальну лінійну групу. Лема доведена.

Лема 2.3. *Нехай тіло T не буде полем характеристики 2 або T — тіло характеристики 2, що не містить трансцендентних відносно свого простого підполя елементів. Нехай $S(T)$ — підгрупа адитивної групи тіла T, що породжується добутками квадратів елементів із T. Тоді $T = S(T)$.*

Доведення. Нехай T — некомутативне тіло. Тоді $T_1 = T \setminus \mathfrak{Z}(T)$ — непорожня множина і нехай α — довільний елемент цієї множини. Знайдеться елемент $\beta \in T$ такий, що

$$\gamma = \alpha\beta + \beta\alpha \neq 0$$

(якщо $\gamma = 0$ для всіх $\beta \in T$, то $2\alpha^2 = 0, \operatorname{char} T = 2, \alpha\beta = \beta\alpha$ і $\alpha \in \mathfrak{Z}(T)$).

Так як $\gamma = (\alpha+\beta)^2 - \alpha^2 - \beta^2$, то $\gamma \in S(T)$. Відмітимо, що адитивна група $S(T)$ замкнута відносно дії множення в T. Тоді $\gamma^{-1} = \gamma\gamma^{-2} \in S(T)$. Далі,

$$\gamma\alpha = \alpha\beta\alpha + \beta\alpha\alpha = \alpha(\beta\alpha) + (\beta\alpha)\alpha \in S(T).$$

Звідси випливає, що $\alpha \in S(T)$ і, отже, $T_1 \subset S(T)$. Якщо $\delta \in \mathfrak{Z}(T)$, то

$$\gamma\delta = \alpha\beta\delta + \beta\alpha\delta = \alpha\beta\delta + \beta\delta\alpha = \alpha(\beta\delta) + (\beta\delta)\alpha \in S(T).$$

Тоді $\delta \in S(T)$ і, отже, $\mathfrak{Z}(T) \subset S(T), T \subseteq S(T)$. Нехай T — поле. Якщо $\operatorname{char} T \neq 2$ і $\alpha \in T$, то

$$\alpha = \left(\frac{\alpha+1}{2}\right)^2 - \left(\frac{\alpha-1}{2}\right)^2 \in S(T),$$

тобто $T = S(T)$. Нехай тепер T — поле характеристики 2, яке алгебраїчне над своїм простим підполем $\mathbb{Z}_2 = \{0, 1\}$, і α — ненульовий елемент поля T. Тоді α належить мультиплікативній групі F^* деякого скінченного розширення F поля $\mathbb{Z}_2$. Так як порядок $n = |F^*|$ — непарне число, то

$$\alpha = \alpha^{n+1} = \left(\alpha^{\frac{n+1}{2}}\right)^2 \in S(T)$$

і, отже, $T = S(T)$. Лема доведена.

Зауваження. *Якщо $T = \mathbb{Z}_2(x)$ — поле дробово-раціональних функцій від невідомої x над полем $\mathbb{Z}_2$, то $S(T) = \mathbb{Z}_2(x^2) \neq T$.*

Теорема 2.1. *Нехай $n > 1$, T — тіло і H — така нецентральна підгрупа групи $GL(n, T)$, що H нормалізується спеціальною групою $SL(n, T)$. Тоді підгрупа H містить групу $SL(n, T)$. Виключення складають лише випадки, коли $n = 2$, а тіло T є полем із 2-х або 3-х елементів.*

Доведення. Якщо H нормалізується $SL(n, T)$, то для будь-якого $g \in GL(n, T)$ група $H_1 = g^{-1}Hg$ також нормалізується $SL(n, T)$. Якщо H_1 містить групу $SL(n, T)$, то H також містить цю групу. Це дає можливість заміняти підгрупу H на спряжену з нею підгрупу H_1. Будемо розглядати групу $GL(n, T)$ як групу лівих лінійних операторів правого n-вимірного векторного простору L над тілом T. Так як H — нецентральна, то H містить нескалярну матрицю A. Тоді в просторі L існує такий вектор u_1, що вектори $u_1, u_2 = Au_1$ непропорційні і тоді їх можна включити в новий T-базис простору L. В новому базисі перший стовпчик матриці оператора A буде мати вигляд $(0\ 1\ 0\ \ldots\ 0)$. Будемо вважати, що сама матриця A має такий перший стовпчик.

Розіб'ємо доведення на два випадки.

1-*й випадок*: $n > 2$. Для доведення теореми досить довести існування в H деякої елементарної матриці t_{ij} $(i \neq j)$ (див. лему 2.2). Розглянемо комутатор

$$B = [t_{12}(1), A^{-1}] = (E - e_{12})A(E + e_{12})A^{-1} = (E - e_{12})(E + Ae_{12}A^{-1}).$$

Очевидно $B \in H$. Враховуючи, що $Ae_{12} = e_{22}$, неважко показати, що

$$B = E - e_{12} + (E - e_{12})e_{22}A^{-1} = E - e_{12} + (e_{22} - e_{12})A^{-1} = E - e_{12} + \sum_j (e_{2j} - e_{1j})\beta_{2j},$$

де β_{ij} — елементи матриці A^{-1}. Відмітимо, що $\beta_{22} = 0$. Нехай $C = [t_{13}(1), B^{-1}]$. Неважко перевірити, що

$$C = (E - e_{13})(E + Be_{13}B^{-1}) = (E - e_{13})(E + (e_{13} - e_{13}\beta_{21} + e_{23}\beta_{21})B^{-1}) =$$

$$= (E - e_{13})(E + e_{13} - e_{13}\beta_{21} + e_{23}\beta_{21}) = E + \beta_{21}(e_{23} - e_{13}).$$

Якщо $\beta_{21} \neq 0$, то $t_{23}(\beta_{21}) = t_{12}(1)Ct_{12}(-1) \in H$. Нехай $\beta_{21} = 0$. Тоді $[t_{23}(1), B^{-1}] = (E - e_{23})(E + Be_{23}B^{-1}) = (E - e_{23})(E + (-e_{13} + e_{23})B^{-1}) = (E - e_{23})(E - e_{13} + e_{23}) = t_{13}(-1)$,

отже, $t_{13}(-1) \in H$. Таким чином, у випадку $n > 2$ група H містить елементарну матрицю, що доводить теорему для цього випадку.

2-*й випадок*: $n = 2$, $|T| > 3$. Нехай H — нецентральна підгрупа групи $GL(2,T)$, яка нормалізується групою $SL(2,T)$. Покажемо, що $SL(2,T) \subseteq H$. Для цього досить довести, що H містить всі елементарні матриці. Покажемо спочатку існування в H однієї елементарної матриці. Нехай

$$A = \begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix} \in H.$$

Тоді

$$A^{-1} = \begin{pmatrix} \beta\alpha^{-1} & 1 \\ -\alpha^{-1} & 0 \end{pmatrix}$$

і

$$B = [t_{12}(1), A^{-1}] = (E - e_{12})(E + Ae_{12}A^{-1}) = (E - e_{12})(E + e_{22}A^{-1}) =$$
$$= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha^{-1} & 1 \end{pmatrix} = \begin{pmatrix} 1 - \alpha^{-1} & -1 \\ \alpha^{-1} & 1 \end{pmatrix} \in H.$$

Всі елементи матриці B належать полю $F(\alpha)$, де F — центр тіла T. Над цим полем матриця B подібна матриці

$$B_1 = t_{12}(-2 + \alpha^{-1})t_{21}(1) \begin{pmatrix} 1 - \alpha^{-1} & -1 \\ \alpha^{-1} & 1 \end{pmatrix} t_{21}(-1)t_{12}(2 - \alpha^{-1}) =$$

$$= t_{12}(-2 + \alpha^{-1}) \begin{pmatrix} 2 - \alpha^{-1} & -1 \\ 1 & 0 \end{pmatrix} t_{12}(2 - \alpha^{-1}) = \begin{pmatrix} 0 & -1 \\ 1 & \beta_1 \end{pmatrix},$$

де $\beta_1 = 2 - \alpha^{-1} \in F(\alpha)$. Зрозуміло, що $B_1 \in H$. Нехай γ — ненульовий елемент тіла T, який комутує з α, $d = \mathrm{diag}[\gamma, \gamma^{-1}]$ і

$$B_2 = [d, B_1] = \mathrm{diag}[\gamma^{-1}, \gamma] \begin{pmatrix} \beta_1 & 1 \\ -1 & 0 \end{pmatrix} \mathrm{diag}[\gamma, \gamma^{-1}] \begin{pmatrix} 0 & -1 \\ 1 & \beta_1 \end{pmatrix} = \begin{pmatrix} \gamma^{-2} & (\gamma^{-2} - 1)\beta_1 \\ 0 & \gamma^2 \end{pmatrix}.$$

Так як $d \in SL(2,T)$, то $B_2 \in H$. Комутатор

$$[t_{12}(1), B_2] = (E - e_{12})(E + B_2^{-1}e_{12}B_2) = (E - e_{12})(E + \gamma^2 e_{12}B_2) = (E - e_{12})(E + \gamma^4 e_{12}) =$$
$$= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma^4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \gamma^4 - 1 \\ 0 & 1 \end{pmatrix}$$

буде елементарною матрицею, якщо $\gamma^4 \neq 1$.

Дослідимо існування такого ненульового елемента γ в T, який комутує з α і $\gamma^4 \neq 1$.

Нехай $|F| > 5$. Тоді в полі F крім нуля та до 4-х коренів 4-го степеня з одиниці існують інші елементи. Звідси стає зрозумілим існування елемента γ.

Нехай $|F| \leqslant 5$, $F(\alpha) \neq F$. Зрозуміло, що $|F(\alpha)| \geq 4$. Для $|F(\alpha)| = 4$, $|F(\alpha)^*| = 3$ і $\alpha \neq 0$, $\alpha^3 = 1$, $\alpha^4 = \alpha \neq 1$. Тоді $\gamma = \alpha$ — шуканий елемент. Для $|F(\alpha)| = 5$, $F(\alpha) \cong \mathbb{Z}_5$ і $F(\alpha) = F$, що неможливо. Випадок $|F(\alpha)| > 5$ аналогічний до випадку $|F| > 5$.

Нехай $|F| \leqslant 5$, $F(\alpha) = F \neq T$. Очевидно, існує елемент $\theta \in T \setminus F$. Тоді довільний елемент з $T(\theta)$ комутує з α. Зрозуміло, що $F(\theta) \neq F$ і $F(\theta)$ аналогічно як і $F(\alpha)$ в розглянутому раніше випадку містить елемента γ.

Нехай $3 < |F| \leqslant 5$, $F(\alpha) = F = T$. Випадок $|F| = 4$ аналогічний до випадку $|F(\alpha)| = 4$. Випадок $|F| = 5$ означає, що $T \cong \mathbb{Z}_5$ — поле з 5-ти елементів і розглядається як приклад. Отже, ми показали існування в H елементарної матриці $t_{12}(\delta)$, $(\delta \in T, \delta \neq 0.)$ Замінимо підгрупу H на спряжену підгрупу

$$H_1 = \mathrm{diag}[\delta, 1]^{-1} H (\mathrm{diag}[\delta, 1]).$$

Якщо H_1 містить $SL(2,T)$, то H також містить $SL(2,T)$. Отже, можна вважати, що

$$t_{12}(1) = \mathrm{diag}[\delta, 1]^{-1} t_{12}(\delta)(\mathrm{diag}[\delta, 1]) \in H.$$

Нехай λ — будь-який ненульовий елемент тіла T. Так як $\sigma(\lambda) = \mathrm{diag}[\lambda^{-1}, \lambda] \in$ $\in SL(2,T)$, то $t_{12}(\lambda^2) = \sigma(\lambda)^{-1} t_{21}(1)\sigma(\lambda) \in H$. Неважко тепер бачити, що всі матриці вигляду

$$t_{12}(\mu) \quad (\mu \in S(T))$$

належать групі H. Нехай тіло T задовольняє умовам леми 2.3. Тоді $S(T) = T$ і, отже, група H містить всі елементарні матриці $t_{21}(\lambda)$. Нехай тепер T — поле характеристики 2, що містить трансцендентний над $\mathbb{Z}_2$ елемент ϱ. Нехай

$$D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 0 & \varrho \\ \varrho^{-1} & 0 \end{pmatrix}.$$

Очевидно, $R \in SL(2,T)$ і матриця $t_{12}(1) = t_{21}(1) D t_{21}(1)$ подібна матриці D. Неважко бачити, що $[D, R] = \mathrm{diag}[\varrho^2, \varrho^{-2}]$,

$$[t_{12}(\lambda), [D, R]] = (E + \lambda e_{12})(E + \lambda\, \mathrm{diag}[\varrho^2, \varrho^{-2}] e_{12}\, \mathrm{diag}[\varrho^{-2}, \varrho^2]) = (E + \lambda e_{12})(E + \lambda \varrho^4 e_{12}) =$$

$$= \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \lambda\varrho^4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda(1+\varrho^4) \\ 0 & 1 \end{pmatrix} = t_{12}(\lambda(1+\varrho^4)).$$

Так як $1 + \varrho^4 \neq 0$, то група H містить всі елементарні матриці $t_{12}(\lambda)$. Нарешті відмітимо, що матриця $t_{12}(\lambda)$ спряжена в $SL(2,T)$ з матрицею $t_{21}(-\lambda)$. Це завершує доведення теореми.

Контрприклад (див. контрприклад § 1). Підгрупа $H = \langle a, b \rangle$ в групі $GL(2, \mathbb{Z}_3)$ буде нормальною в цій групі, але вона не містить групу $SL(2, \mathbb{Z}_3) = \langle a, b, c \rangle$.

Наслідок 2.2. *Нехай $n > 1$ і при $n = 2$ тіло T містить більше ніж три елементи. Якщо H — нецентральна нормальна підгрупа в групі $SL(n,T)$, то $H = SL(n,T)$.*

Фактор-групу $PGL(n,T) = GL(n,T)/\mathfrak{Z}(GL(n,T))$ повної лінійної група за її центром називають *повною проективною групою* степеня n над тілом T, а фактор-групу $PSL(n,T) = SL(n,T)/\mathfrak{Z}(SL(n,T))$ спеціальної — *спеціальною проективною групою* степеня n над тілом T.

Наслідок 2.3. *Нехай $n > 1$ і при $n = 2$ тіло T містить більше ніж три елементи. Тоді група $PSL(n,T)$ є простою групою.*

Приклад. Розглянемо випадок групи $GL(2, \mathbb{Z}_5)$. Нехай H — нецентральна підгрупа групи $GL(2, \mathbb{Z}_5)$, яка нормалізується групою $SL(2, \mathbb{Z}_5)$. Зрозуміло, що деяка матриця вигляду

$$A = \begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix} \in H,$$

де $\alpha = \pm 1, \pm 2$. Розглянемо тільки випадок $\alpha = -1$. Тобто

$$B(\beta) = \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix} \in H,$$

де $\beta = 0, \pm 1, \pm 2$. Покажемо, що підгрупа H або спряжена з нею підгрупа містить елементарну матрицю.

1. $\beta = 0$. Матриця $B(0)$ подібна матриці $D = \mathrm{diag}[2, -2]$. Можна вважати, що $D \in H$. Неважко впевнитись в тому, що

$$[t_{12}(1), D] = (E - e_{12})(E + \mathrm{diag}[-2, 2] e_{12}\, \mathrm{diag}[2, -2]) = (E - e_{12})^2 = t_{12}(-1)^2 = t_{12}(-2).$$

2. $\beta = \pm 1$. Неважко впевнитись в тому, що

$$[B(1), D] =$$

$$= \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix},$$

$$[B(-1), D] =$$

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

Тому матриці $[B(1), D]^2$ і $[B(-1), D]^2$ подібні клітці Жордана $J_2(1) = t_{12}(1)$.

3. $\beta = \pm 2$.

$$t_{12}(1)B(2)t_{12}(-1) = t_{12}(1)\begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}t_{12}(-1) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$t_{12}(-1)B(-2)t_{12}(1) = t_{12}(-1)\begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}t_{12}(1) = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}.$$

Тому матриці $B(2)$ і $B(-2)^2$ подібні клітці Жордана $J_2(1) = t_{12}(1)$.

В усіх випадках група H (або спряжена з нею) містить елементарну матрицю.

§3. Основні поняття і дії над матричними групами

Нехай V — лінійний простір розмірності n над полем T, $E(V) = \mathrm{End}_T(V)$ — кільце всіх лінійних операторів простору V, $GL(V)$ — мультиплікативна група кільця $E(V)$. Ця група також називається *повною лінійною групою* (простору V). Нехай

$$\mathbf{u} = (u_1,\ \ldots,\ u_n) \quad (u_i \in V) \tag{1}$$

— базис простору V. Кожному лінійному операторові $\varphi \in E(V)$ поставимо у відповідність його матрицю A_φ в базисі $\mathbf{u}(1)$ (стовпці цієї матриці будуть координатними стовпцями образів базисних векторів). Одержане відображення

$$\tau_{\mathbf{u}} : E(V) \to M(n, T)$$

буде ізоморфізмом кілець, а його обмеження на групу $GL(V)$ буде ізоморфізмом цієї групи на повну лінійну групу $GL(n, T)$.

Нехай $\nu_{\mathbf{u}} = \tau_{\mathbf{u}}^{-1}$. Якщо

$$g = (\alpha_{ij}) \in M(n, T) \quad (\alpha_{ij} \in T),$$

то $\nu_{\mathbf{u}}(g) \in E(V)$ і, як слідує із означень

$$\nu_{\mathbf{u}}(g)(u_j) = \sum_i \alpha_{ij} u_i \quad (j = 1, \ldots, n). \tag{2}$$

Неважко бачити, що матриця g є матрицею лінійного оператора в базисі $\mathbf{u}$ (1). Формула (2) дозволяє будь-яку матричну підгрупу G групи $GL(n, T)$ перетворити в групу лінійних операторів простору V, тобто перетворити простір V в модуль (лівий) над груповою алгеброю TG. Довільна група G, очевидно, діє (зліва) у будь-якому TG-модулі, а будь-який лінійний простір над полем T, в якому діє група G, є TG-модулем. TG-модуль будемо називати ще *G-простором* над полем T, а його TG-підмодулі — *G-підпросторами*. Далі термін група $G \subset GL(n, T)$ *діє* в лінійному просторі над полем T будемо використовувати тільки для n-вимірного лінійного простору V над полем T з дією визначеною формулою (2).

Гомоморфізми $\nu_{\mathbf{u}}, \tau_{\mathbf{u}}$ залежать від вибору базису $\mathbf{u}$ простору V. Нехай в просторі V вибрано ще один базис

$$\mathbf{v} = (v_1, \ \ldots, \ v_n) \quad (v_i \in V). \tag{3}$$

Нехай S — матриця переходу від базису $\mathbf{u}$ (1) до базису $\mathbf{v}$ (3) і ϕ — автоморфізм простору V такий, що $\phi(\mathbf{u}) = \mathbf{v}$, тобто $\phi(u_i) = v_i$ $(i = 1, \ldots, n)$.

Лема 3.1. *Нехай H — підгрупа групи $GL(V)$. Тоді*

$$\tau_{\boldsymbol{v}}(H) = S^{-1}\tau_{\boldsymbol{u}}(H)S. \tag{4}$$

Нехай G — підгрупа групи $GL(n, T)$. Тоді

$$\nu_{\boldsymbol{v}}(G) = \phi\nu_{\boldsymbol{u}}(G)\phi^{-1}. \tag{5}$$

Доведення. (4) слідує із зв'язку матриці одного і того ж лінійного оператора в різних базисах. Нехай $g \in G$. Тоді згідно (2)

$$\phi\nu_{\mathbf{u}}(g)\phi^{-1}(v_j) = \phi\nu_{\mathbf{u}}(g)(u_j) = \phi\left(\sum_j \alpha_{ij}u_i\right) = \sum_j \alpha_{ij}\phi(u_i) = \sum_j \alpha_{ij}v_i = \nu_{\mathbf{v}}(g)(v_j),$$

звідки слідує (5). Лема доведена.

Нагадаємо, підгрупи H_1, H_2 групи G називаються *спряженими*, якщо існує елемент $c \in G$ такий, що $c^{-1}H_1c = H_2$. В розглянутій відповідності між матричними групами із $GL(n, T)$ і групами лінійних операторів простору V дві групи матриць, що відповідають одній групі операторів, будуть спряженими в групі $GL(n, T)$, а дві групи операторів із $GL(V)$, що відповідають одній матричній групі, будуть спряженими в групі $GL(V)$.

Підгрупа G групи $GL(n, T)$ називається *звідною*, якщо вона спряжена з групою матриць вигляду

$$\begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix}, \tag{6}$$

де $g_j \in G_j \subseteq GL(n_j, T)$($G_j$ — підгрупа групи $GL(n_j, T)$, $n_1 + n_2 = n$).

Підгрупа G групи $GL(n, T)$, яка не буде звідною, називається *незвідною* групою.

Нехай підгрупа G групи $GL(n, T)$ буде звідною і спряженою за допомогою матриці $C \in GL(n, T)$ з групою матриць вигляду (6), де $G_j (1 \leqslant j \leqslant 2)$ така група, що для кожного елемента $g_j \in G_j$ знайдеться матриця $g \in G$, що спряжена за допомогою тієї ж матриці C з матрицею (6). Нехай V — лінійний простір над полем T в якому діє група G. Тоді в просторі V існує такий базис

$$u_1, \ldots, u_{n_1}, \quad v_1 = u_{n_1+1}, \ldots, v_{n_2} = u_n, \tag{7}$$

в якому кожний оператор $g \in G$ має матрицю (6). Нехай

$$U = Tu_1 + \cdots + Tu_{n_1}, \quad \overline{V} = V/U = T\overline{v}_1 + \cdots + T\overline{v}_{n_2} \quad (\overline{v}_i = v_i + U)$$

— підпростір в просторові V і відповідний фактор-простір. Так як

$$g(u_i) = g_1(u_i) \in U \quad (i \leqslant n_1),$$

$$g(v_j) = g_2(v_j) + x_j(g) \quad (x_j(g) \in U),$$

то U — G-підпростір. І, окрім цього, фактор-простір $\overline{V}$ перетворюється в G-простір

$$g(v + U) = g_2(v) + U. \tag{8}$$

G-простір V називається *звідним*, якщо в ньому існує власний ненульовий G-підпростір U. G-простір V називається *незвідним*, якщо в ньому нема G-підпросторів, окрім нульового підпростору і всього простору V. Нехай лінійний простір V в якому діє група G є звідним і U — G-підпростір простору V ($U \neq 0$, $U \neq V$). Нехай (7) базис в V, який проходить через базис підпростору U. Тоді матриці всіх операторів із групи G в цьому базисі будуть мати вигляд (6). Отже, група G буде звідною групою. Підсумуємо результат.

Лема 3.2. *Група $G \subseteq GL(n,T)$ буде звідною групою тоді і тільки тоді, коли буде звідним простір V в якому діє група G над полем T.*

Нехай V — лінійний простір над полем T в якому діє група G і

$$0 = U_0 \subset U_1 \subset \cdots \subset U_t = V \tag{9}$$

— композиційний ряд TG-модуля V, де U_j — G-підпростори в V і фактори U_j/U_{j-1} — незвідні TG-модулі (такий ряд існує). Проведемо базис простору V через базиси підпросторів в (9), доповнюючи базис U_j до базису U_{j+1}. В так вибраному базисі матриця кожного оператора буде мати вигляд

$$\begin{pmatrix} g_1 & * & \dots & * \\ 0 & g_2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g_t \end{pmatrix}, \tag{10}$$

де g_j — матриця оператора g в незвідному G-модулі U_j/U_{j-1} (див. (8)) пробігає деяку незвідну матричну групу G_j. Отже, встановлено такий результат.

Теорема 3.1 (Теорема про канонічний вигляд матричної групи)**.** *Будь-яка підгрупа G в групі $GL(n,T)$ спряжена в цій групі з групою матриць вигляду* (10)*, яку називають її канонічним виглядом, де g_j пробігає деяку незвідну підгрупу G_j групи $GL(n_j,T)$ ($j = 1, \ \dots, \ t$), $n_j \geq 1$, $n_1 + \cdots + n_t = n$.*

Нехай

$$\gamma_j : G \to GL(n_j,T) \quad (\gamma_j(g) = g_j \in G_j)$$

— відображення, яке ставить у відповідність кожному елементу g групи G j-ий діагональний блок g_j матриці (10) в канонічному вигляді групи G ($j = 1, \ \dots, \ t$). Тоді γ_j — зображення групи G над полем T і $\gamma_j(G) = G_j$.

Підгрупа G групи $GL(n,T)$ називається *розкладною*, якщо вона спряжена з групою матриць вигляду

$$\operatorname{diag}[g_1, g_2] = \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \quad (g_j \in GL(n_j,T), n_1 + n_2 = n). \tag{11}$$

Група $G \subset GL(n,T)$ є розкладною тоді і тільки тоді, коли лінійний простір V в якому діє група G розкладається в пряму суму

$$V = U_1 \oplus U_2$$

ненульових G-підпросторів U_1, U_2.

Група $G \subset GL(n,T)$ називається *цілком звідною*, якщо вона незвідна або спряжена з групою матриць вигляду

$$\operatorname{diag}[g_1, g_2, \dots, g_t] = \begin{pmatrix} g_1 & 0 & \dots & 0 \\ 0 & g_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g_t \end{pmatrix},$$

де g_j пробігає незвідну підгрупу G_j групи $GL(n_j, T)$ $(n_1 + \cdots + n_t = n)$. Група $G \subset$ $\subset GL(n, T)$ буде цілком звідною тоді і тільки тоді, коли простір V в якому діє група G є *цілком звідний*, тобто є незвідним або розкладається в пряму суму

$$V = U_1 \oplus \cdots \oplus U_t$$

незвідних ненульових G-підпросторів $U_1, \ldots, U_t$ $(t > 1)$.

Нехай G_j підгрупа групи $GL(n_j, T)$ $(j = 1, 2)$. *Прямим добутком* $G_1 \times G_2$ називається група $\mathrm{diag}[G_1, G_2]$ усіх матриць вигляду $\mathrm{diag}[g_1, g_2]$ (див. (11)).

Нехай G_j підгрупа групи $GL(n_j, T)$ $(j = 1, \ldots, t > 2)$. За означенням

$$G_1 \times \cdots \times G_t = (G_1 \times \cdots \times G_{t-1}) \times G_t$$

називається *прямим добутком* груп $G_j (j = 1, \ldots, t)$. Нехай γ_j — проекція прямого добутку $G_1 \times \cdots \times G_t$ на j-ту компоненту G_j.

Підгрупа G прямого добутку $G_1 \times \cdots \times G_t$ називається *підпрямим добутком* груп $G_j (j = 1, \ldots, t)$, якщо $\gamma_j(G) = G_j$ $(j = 1, \ldots, t)$.

Група $G \subset GL(n, T)$ є цілком звідною тоді і тільки тоді, коли вона незвідна або спряжена з підпрямим добутком незвідних матричних груп над полем T.

Нехай $A = (\alpha_{ij})$, $B = (\beta_{ij})$ — матриці над полем T порядків n і m відповідно. Матриця

$$A \otimes B = \begin{pmatrix} \alpha_{11}B & \ldots & \alpha_{1n}B \\ \vdots & \ddots & \vdots \\ \alpha_{n1}B & \ldots & \alpha_{nn}B \end{pmatrix}$$

порядку nm називається *кронекеровим добутком* матриць A та B. Неважко бачити, що

$$\det(A \otimes B) = (\det A)^m \cdot (\det B)^n.$$

Нехай G_j підгрупа групи $GL(n_j, T)$ $(j = 1, 2)$. Група

$$G_1 \otimes G_2 = \{\ A_1 \otimes A_2 \ \mid \ A_j \in G_j \ \}$$

називається *тензорним добутком груп* G_1, G_2. Очевидно, $G_1 \otimes G_2$ є підгрупою групи $GL(nm, T)$. Якщо G_1, G_2 — скінченні групи, то $|G_1 \otimes G_2| = |G_1||G_2|$.

Нехай K — кільце з одиницею. Матриця $A \in M(n, K)$ називається *мономіальною*, якщо кожний рядок і кожний її стовпчик містить не більше одного елемента, відмінного від нуля. Підгрупа групи $GL(n, K)$ називається *мономіальною*, якщо вона спряжена з підгрупою групи $GL(n, K)$ всі матриці якої мономіальні. Нехай σ — підстановка степеня n. *Підстановочною* матрицею $\widetilde{\sigma} \in GL(n, K)$, відповідною підстановці σ називається мономіальна матриця, яка в j-стовпчику містить одиницю на $\sigma(j)$-му місці $(j = 1, \ldots, n)$. Кожну мономіальну матрицю можна представити у вигляді добутку діагональної матриці на підстановочну матрицю. Матриця $B \otimes A$ подібна матриці $A \otimes B$, причому матриця подібності є підстановочна матриця.

Нехай H — підгрупа групи $GL(n, T)$, A — підгрупа симетричної групи S_t. *Сплетінням* $H \wr A$ цих груп називається підгрупа групи $GL(nt, T)$, яка породжується групою $H^t = H \times \cdots \times H$ і усіма підстановочними матрицями $\widetilde{\sigma}$ над кільцем $K = M(n, T)$, відповідним підстановкам $\sigma \in A$. Якщо H — скінченна група, то $|H \wr A| = |H|^t|A|$.

Група $G \subset GL(n, T)$ над полем T називається *імпримітивною*, якщо для деякого дільника $d > 1$ числа n група G спряжена з групою G_1 мономіальних матриць над кільцем $K = M(s, T)$, де $s = n/d$. Нехай при цьому C така матриця із групи $GL(n, T)$, що $C^{-1}GC = G_1$. Якщо $g \in G$, то

$$C^{-1}gC = \mathrm{diag}[a_1(g), \ldots, a_d(g)]\widetilde{\sigma(g)}, \tag{12}$$

де $a_1(g), \ldots, a_d(g) \in GL(s,T), \widetilde{\sigma(g)}$ — матриця деякої підстановки $\sigma(g)$ на d символах. Відображення $\sigma : G \to S_d$, при якому елемент $g \in G$ переходить у підстановку $\sigma(g) \in S_d$, буде зображенням імпримітивної групи G підстановками (див. (12)). Нехай H — та підгрупа групи $GL(s,T)$, що породжується всіма матрицями $a_j(g)(j = 1, \ldots, d; g \in G$ (див. (12)). Тоді група G_1 буде підгрупою сплетіння $H \wr \sigma(G)$. Отже, імпримітивна матрична група над полем T — це група, що спряжена з підгрупою сплетіння матричної групи і групи підстановок на $d > 1$ символах.

Нагадаємо, що підгрупа A групи S_d називається *транзитивною*, якщо для будь-яких символів i та j $(1 \leqslant i, j \leqslant d)$ в підгрупі A знайдеться такий елемент a, що $a(i) = j$.

Лема 3.3. *Імпримітивна група $G \subset GL(n,T)$ над полем T буде незвідною тоді і тільки тоді, коли незвідною буде підгрупа H в групі $GL(s,T)$ і зображення σ підстановками буде транзитивним (тобто, коли група підстановок $\sigma(G)$ буде транзитивною).*

Лема 3.4. *Нехай L — лінійний простір в якому діє група G. Група G буде імпримітивною тоді і тільки тоді, коли простір L можна представити у вигляді прямої суми*

$$L = L_1 \oplus \cdots \oplus L_d \quad (d > 1)$$

таких підпросторів L_j, що для кожного $g \in G$ і кожного номера j існує номер t такий, що $g(L_j) = L_t$.

Незвідна група називається *примітивною* групою, якщо вона не буде імпримітивною. Будь-яка незвідна група буде примітивною або імпримітивною.

§4. Цілком звідні групи

Лема 4.1. *Нехай V — G-простір над полем T. Подані умови є еквівалентні:*
1) *кожний власний ненульовий G-підпростір U в V має пряме G-доповнення U', тобто $V = U \oplus U'$, де U' — H-підпростір в V;*
2) *простір V є сумою незвідних G-підпросторів;*
3) *простір V є пряма сума незвідних G-підпросторів.*

Теорема 4.1 (Теорема Діксона; [2]). *Нехай G — така група матриць порядку n над полем T, що містить підгрупу H скінченного індекса $s = [G : H]$, який не ділиться на характеристику* $\operatorname{char} T$ *поля T. Група G є цілком звідною тоді і тільки тоді, коли цілком звідна підгрупа H.*

Доведення. Нехай H — цілком звідна група. Покажемо, що група G також цілком звідна. Нехай V — лінійний простір в якому діє група G. Досить показати, що простір V є пряма сума незвідних G-підпросторів. Для цього покажемо що кожний власний ненульовий G-підпростір в V має пряме G-доповнення і скористаємось лемою 4.1. Нехай U — G-підпростір в просторі V і $U \neq 0, U \neq V$. Так як H — цілком звідна група, то H-підпростір U має пряме H-доповнення. Нехай $p : V \to V$,

$$p(u + u') = u \ (u \in U, u' \in U')$$

проектор простору V на прямий доданок U. Тоді

$$p(V) = U, \ p^2 = p, \ h^{-1}ph = p \quad (h \in H). \tag{1}$$

Нехай $g_1, \ldots, g_s$ — система представників усіх суміжних класів групи G за підгрупою H. Покладемо

$$\theta : V \to V, \quad \theta = s^{-1} \sum_{j=1}^{s} g_j^{-1} p g_j.$$

Тоді $\theta(V) = U$. Якщо $u \in U$, то $g_j(u) \in U$ і

$$\theta(u) = s^{-1} \sum_j g_j^{-1}(p(g_j(u))) = s^{-1} \sum_j g_j^{-1} g_j(u) = s^{-1} \sum_j u = s^{-1} \sum_{j=1}^{s} u = u,$$

тобто

$$\theta^2 = \theta. \tag{2}$$

Нехай $g \in G$. Існує підстановка ρ на s символах і такі елементи $h_1, \ldots, h_s$ групи H, що

$$g_j g = h_i g_i, \quad i = \rho(j) \quad (j = 1, \ldots, s).$$

Так як $g_j^{-1} = g g_i^{-1} h_i^{-1}$, то врахувавши (1), будемо мати

$$\theta g = s^{-1} \sum_j g_j^{-1} p g_j g = s^{-1} \sum_{i=\rho(j)} g g_i^{-1} h_i^{-1} p h_i g_i = g\theta \tag{3}$$

для всіх $g \in G$. Із (2) і (3) слідує, що $(I - \theta)(V)$ (I — одиничний оператор) буде G-підпростором в просторі V і

$$\theta(V) \bigcap (I - \theta)(V) = 0. \tag{4}$$

Так як V є сумою $\theta(V) + (I - \theta)(V)$, то в силу (4), ця сума є пряма. Отже, підпростір U має G-доповнення $(I - \theta)(V)$, що доводить теорему.

Наведемо матричний варіант доведення теореми. Нехай G — звідна група. Отже, можна вважати, що ця група суміщається з групою матриць вигляду

$$g = \begin{pmatrix} \Gamma(g) & A(g) \\ 0 & \Delta(g) \end{pmatrix},$$

де Γ, Δ деякі T-зображення групи G степенів n_1, n_2 ($n_1 + n_2 = n$) і $A : G \to T_{n_1 \times n_2}$ — *зв'язуюча функція* для цих зображень. Так як H — цілком звідна група, то можна вважати, що $A(h) = 0$ для всіх елементів $h \in H$. Нехай $g_1, g_2, \ldots, g_s$ — система представників всіх лівих суміжних класів групи G за підгрупою H. Для кожної пари індексів $i, j (1 \leqslant i, j \leqslant s)$ існує єдиний індекс $k (1 \leqslant k \leqslant s)$, такий, що

$$g_i g_j g_k^{-1} \in H.$$

Відмітимо, що коли при даному індексу j індекс i пробігає всі значення від 1 до s, то індекс k також пробігає всі ці значення але, можливо, в іншому порядку. Із рівності

$$A(g_i g_j g_k^{-1}) = 0,$$

використовуючи формули $A(xy) = \Gamma(x)A(y) + A(x)\Delta(y)$ $(x, y \in G)$, $A(g_k^{-1}) = -\Gamma(g_k^{-1}) \times$ $\times A(g_k)\Delta(g_k^{-1})$, маємо

$$\Gamma(g_i g_j) A(g_k^{-1}) + A(g_i g_j)\Delta(g_k^{-1}) = 0,$$

$$-\Gamma(g_i)\Gamma(g_j)\Gamma(g_k^{-1})A(g_k)\Delta(g_k^{-1}) + \Gamma(g_i)A(g_j)\Delta(g_k^{-1}) + A(g_i)\Delta(g_j)\Delta(g_k^{-1}) = 0,$$

$$\Gamma(g_i)\left(-\Gamma(g_j)\Gamma(g_k^{-1})A(g_k) + A(g_j) + \Gamma(g_i^{-1})A(g_i)\Delta(g_j)\right)\Delta(g_k^{-1}) = 0.$$

Звідси одержуємо

$$-\Gamma(g_j)\Gamma(g_k^{-1})A(g_k) + A(g_j) + \Gamma(g_i^{-1})A(g_i)\Delta(g_j) = 0.$$

При даному j просумуємо одержані співвідношення за i від 1 до s (при цьому k буде також змінюватись в межах від 1 до s) і використаємо ту обставину, що $s^{-1} \in T$. Одержимо

$$A(g_j) = \Gamma(g_j)B - B\Delta(g_j), \tag{5}$$

де

$$B = s^{-1} \sum_{i=1}^{s} \Gamma(g_i^{-1})A(g_i).$$

Нехай $h \in H$. Для кожного i існує єдиний j $(1 \leqslant i, j \leqslant s)$ і такий елемент $h' \in H$, що $g_i h = h' g_j$. Враховуючи при цьому, що $A(h) = A(h') = 0$, отримаємо $A(g_i)\Delta(h) = = \Gamma(h')A(g_j)$. Тоді, використавши цю рівність і рівність $g_s^{-1}h' = hg_j^{-1}$, отримаємо

$$\begin{gathered} B\Delta(h) = s^{-1} \sum_{i=1}^{s} \Gamma(g_i^{-1})A(g_i)\Delta(h) = s^{-1} \sum_{i=1}^{s} \Gamma(h)\Gamma(h^{-1}g_i^{-1})\Gamma(h')A(g_j) = \\ = \Gamma(h)s^{-1} \sum_{i=1}^{s} \Gamma(h^{-1}g_i^{-1}h')A(g_j) = \Gamma(h)s^{-1} \sum_{j=1}^{s} \Gamma(g_j^{-1})A(g_j) = \Gamma(h)B. \end{gathered} \tag{6}$$

Нехай

$$C = \begin{pmatrix} E_{n_1} & B \\ 0 & E_{n_2} \end{pmatrix}$$

(E_{n_1}, E_{n_2} — одиничні матриці порядків n_1 та n_2 відповідно). Використовуючи (5), (6) неважко пересвідчитись, що

$$C^{-1}GC = \left\{ \begin{pmatrix} \Gamma(g) & 0 \\ 0 & \Delta(g) \end{pmatrix} \middle| \, g \in G \right\},$$

тобто G — розкладна група. Теорема доведена.

Теорема 4.2 (Теорема Платонова; [2]). *Нехай матрична група G над полем T має таку нормальну підгрупу H, що фактор-група G/H є локально скінченна і порядки її елементів не діляться на* $\operatorname{char} T$. *Якщо група H є цілком звідна, то і група G також цілком звідна.*

Доведення. Перш за все врахуємо наступне зауваження: матрична група є цілком звідною, коли цілком звідна система твірних цієї групи. В кільці $M(n, T)$ будь-яка лінійно незалежна над полем T множина матриць містить не більше ніж n^2 матриць. Нехай

$$g_1, \ \ldots, \ g_t \tag{7}$$

— максимальна лінійно незалежна над T система матриць із групи G і G_1 — підгрупа в G, що породжується $g_1, \ldots, g_t$ і групою H. Із умови теореми слідує, група G_1/H є скінченною підгрупою групи G/H, тобто H має скінченний індекс в групі G_1 і цей індекс не ділиться на $\operatorname{char} T$. Із теореми 4.1 випливає, що G_1 — цілком звідна група. Тоді цілком звідними будуть множина (7) і множина всіх лінійних над полем T комбінацій системи (7), серед яких міститься група G. Отже, група G є цілком звідна. Теорема доведена.

Наслідок 4.1. *Якщо G — локально скінченна підгрупа групи $GL(n, T)$ і порядки її елементів не діляться на* $\operatorname{char} T$, *то група G — цілком звідна.*

Нехай H — підгрупа групи $GL(n, T)$,

$$[H]_T = \left\{ \sum_{h \in H} \lambda_h h | \lambda_h \in T \right\}$$

— множина всіх скінчених лінійних комбінацій над полем T елементів групи H. Ця множина $[H]_T$ є алгеброю над полем T. Ця алгебра називається *лінійною оболонкою* групи H над полем T. Легко бачити, що алгебра $[H]_T$ є гомоморфним образом групової алгебри TH.

Лема 4.2. *Нехай H — незвідна група над полем T. Тоді групова алгебра $[H]_T$ є простою скінченно вимірною алгеброю над полем T.*

Доведення. Нехай V — лінійний простір в якому діє група H. Тоді V — простий A-модуль ($A = [H]_T$). Якщо $x \in A$, $xV = 0$, то $x = 0$. Отже, V — точний A-модуль. Тоді $\operatorname{Rad} A = 0$ і, отже, A — напівпросте артінове кільце. Нехай J — двосторонній ідеал в A. Тоді $J = Ae$, де e — центральний ідемпотент і

$$V = eV + (E - e)V$$

пряма сума A-підмодулів в незвідному A-модулі V. Тоді $e = 0$ або $E - e = 0$, тобто A — просте кільце. Лема доведена.

Централізатором групи $H \subset GL(n, T)$ над полем T називається множина

$$\mathfrak{Z}_T(H) = \{x \in M(n, T) | xh = hx (h \in H)\}$$

всіх матриць x, що комутують з кожним елементом групи H.

Наслідок 4.2. *Нехай виконуються умови леми 4.2. Тоді $\mathfrak{Z}_T(H)$ — скінченно вимірне тіло над полем T, а алгебра $[H]_T$ ізоморфна повному матричному кільцю над тілом D, антиізоморфним тілу $\mathfrak{Z}_T(H)$. Якщо $[H]_T \cong M(s, D)$, то $n = s \cdot (D : T)$.*

Наслідок 4.3. *Нехай G — цілком звідна матрична група над полем T. Тоді її лінійна оболонка $[G]_T$ буде напівпростою скінченно вимірною алгеброю над полем T.*

Доведення. Нехай група G є підпрямим добутком незвідних над полем T матричних груп $G_1, \ldots, G_s$. Нехай $\gamma_j : G \to G_j$ — проекція групи G на групу G_j ($j = 1, \ldots, s$). Гомоморфізм груп γ_j продовжується до гомоморфізму алгебри $[G]_T$ на напівпросту над полем T алгебру $[G_j]_T$. Якщо $x \in [G]_T$, то $x = \operatorname{diag}[\gamma_1(x), \ldots, \gamma_s(x)]$. Якщо $x \in \operatorname{Rad}[G]_T$, то $\gamma_j(x) = 0$ ($j = 1, \ldots, s$). Отже, $\operatorname{Rad}[G]_T = 0$, що завершує доведення.

Нехай T' — алгебраїчне розширення поля T. Будь-яка матриця над полем T буде матрицею над розширенням T'. Постає питання: якщо G — незвідна підгрупа групи $GL(n, T)$, то чи буде група G незвідною в групі $GL(n, T')$? Взагалі кажучи, відповідь негативна. Незвідна матрична група G над полем T називається *абсолютно незвідною*, якщо вона залишається незвідною при будь-якому розширені T' поля T. Якщо поле T — алгебраїчно замкнене, то будь-яка незвідна матрична група над цим полем буде абсолютно незвідною.

Теорема 4.3. *Незвідна підгрупа G групи $GL(n, T)$ буде абсолютно незвідною тоді і тільки тоді, коли виконується одна із еквівалентних умов:*
1) $C(G) = \{\lambda E | \lambda \in T\} \cong T$;
2) $[G]_T = M(n, T)$;
3) *в групі G існує n^2 лінійно незалежних над полем T матриць.*

Поле T називається *сепарабельним*, якщо будь-який незвідний над цим полем T многочлен від невідомої x не має кратних коренів (в алгебраїчному замиканні поля T).

Теорема 4.4. *Нехай поле T — сепарабельне (зокрема $\operatorname{char} T = 0$). Якщо G — незвідна матрична група над полем T, то група G буде цілком звідною над полем T'.*

Доведення. Нехай

$$A = [G]_T, \quad A' = [G]_{T'} = T' \otimes_T A$$

і $K = T(\theta) \cong T[x] / \langle f(x) \rangle$ — центр алгебри A, де θ — корінь незвідного над полем T многочлена $f(x)$. Так як цей многочлен не має кратних коренів, то центр алгебри A'

буде ортогональною сумою деяких скінченних розширень поля T'. Тоді алгебра A' розкладеться в ортогональну суму s повних матричних кілець над деякими тілами, що є скінченно вимірними над полем T'. У відповідності з цим розкладом група G буде спряжена над полем T' з підпрямим добутком незвідних матричних груп над полем, тобто G — цілком звідна над полем T' група. Нехай G — абсолютно незвідна група. Тоді G — незвідна група над полем T'. Звідси слідує, що

$$\mathfrak{Z}_{T'}(G) = T' \otimes_T \mathfrak{Z}_T(G)$$

поле для любого поля $T' \supset T$. Це можливо тільки тоді, коли $\mathfrak{Z}_T(H) = T$. Теорема доведена.

Приклад. Нехай $P = \mathbb{Z}_p(t)$ — поле дробово раціональних функцій від змінної t над полем із p елементів $\mathbb{Z}_p, G$ — циклічна група, що породжена такою матрицею порядку p

$$\widetilde{f(x)} = \begin{pmatrix} 0 & \dots & 0 & t \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix} \tag{8}$$

— супровідною матрицею незвідного над полем P многочлена $f(x) = x^p - t$. Група G — незвідна підгрупа в $GL(p, P)$. Нехай $P' = P(\theta)$, де θ — корінь цього многочлена $f(x)$. Тоді над полем P' матриця (8) подібна клітці Жордана

$$J_p(\theta) = \begin{pmatrix} \theta & 1 & \dots & 0 & 0 \\ 0 & \theta & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \theta & 1 \\ 0 & 0 & \dots & 0 & \theta \end{pmatrix}.$$

Отже група G не буде цілком звідною над полем P'. Відмітимо, що

$$A \cong P', \quad \operatorname{Rad} A' \neq 0, \quad A'/\operatorname{Rad} A' \cong P'$$

(див. позначення теореми 4.4).

Приклад. Нехай

$$K_4 = \langle a, b | a^4 = 1, a^2 = b^2, ab = ba^3 \rangle$$

— група кватерніонів порядку 8,

$$G = \left\langle \tilde{a} = \begin{pmatrix} \tilde{i} & 0 \\ 0 & \tilde{i} \end{pmatrix}, \tilde{b} = \begin{pmatrix} 0 & -E \\ E & 0 \end{pmatrix} \right\rangle \quad \left(\tilde{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

— незвідна підгрупа в $GL(4, \mathbb{Q})$, ізоморфна групі K_4. Над полем $Q' = \mathbb{Q}(i)(i^2 = -1)$ група G буде звідною і спряженою з групою

$$\left\langle \begin{pmatrix} i\Delta & 0 \\ 0 & i\Delta \end{pmatrix}, \begin{pmatrix} \tilde{i} & 0 \\ 0 & \tilde{i} \end{pmatrix} \right\rangle \quad \left(\Delta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right).$$

Окрім того, $\mathfrak{Z}_{\mathbb{Q}}(G)$ і $[G]_{\mathbb{Q}}$ — тіла кватерніонів.

§5. Теореми про скінченність

Теорема 5.1 (Теорема Бернсайда; [2]). *Нехай G — абсолютно незвідна підгрупа групи $GL(n,T)$ (T — поле) така, що множина $\operatorname{tr}(G)$ слідів всіх елементів групи G є скінченою. Тоді G — скінченна група і $|G| \leqslant |\operatorname{tr}(G)|^{n^2}$.*

Доведення. В групі G міститься n^2 лінійно незалежних матриць

$$A_1, \ldots, A_j = (\alpha_{ik}^{(j)}), \ldots, A_{n^2} \quad (1 \leqslant j \leqslant n^2; \alpha_{ik} \in T). \tag{1}$$

Нехай $X = (x_{ik})$ — довільна матриця порядку n^2 і

$$\operatorname{tr}(A_j X) = \beta_j. \tag{2}$$

Якщо $X \in G$, то $\beta_j \in \operatorname{tr}(G)$. Розписуючи (2), одержимо

$$\sum_i \sum_k \alpha_{ik}^{(j)} x_{ki} = \beta_j \quad (j = 1, \ldots, n^2). \tag{3}$$

На (3) можна дивитись як на систему n^2 лінійних рівнянь з невідомими x_{ki}. Коефіцієнти j-го рівняння — це всі рядки матриці A_j і $\beta_j \in \operatorname{tr}(G)$. Так як матриці (1) лінійно незалежні, то рядки матриці системи рівнянь (3) також лінійно незалежні. Отже, при вибраному наборі β_j ($j = 1, \ldots, n^2$) система (3) має єдиний розв'язок. Систем (3) існує $|\operatorname{tr}(G)|^{n^2}$. Розв'язки деяких систем (3) будуть матриці із групи G. Теорема доведена.

Наслідок 5.1. *Якщо порядки елементів періодичної абсолютно незвідної підгрупи G групи $GL(n,T)$ обмежені числом m, то G — скінченна група, порядок якої не перевищує деякого числа, що залежить лише від n і m.*

Доведення. Нехай $A \in G$ і $A^r = E$. Тоді слід $\operatorname{tr} A$ матриці A є сумою n коренів степеня r із одиниці. Так як $r \leqslant m$, то число $|\operatorname{tr}(G)|$ буде скінченне і наслідок випливає із теореми 5.1.

Наслідок 5.2. *Нехай $\operatorname{char} T = p$ і G — абсолютно незвідна p-підгрупа групи $GL(n,T)$. Тоді $n = 1$ і G — одинична група.*

Доведення. Якщо $A \in G$, то $\operatorname{tr} A = n$. Отже, $|\operatorname{tr}(G)| = 1$ і тоді діє теорема 5.1.

Теорема 5.2 (Критерій Бернсайда; [2]). *Нехай G — періодична підгрупа групи $GL(n,T)$ (T — довільне поле), порядки елементів якої не діляться на $\operatorname{char} T$ і обмежені деяким числом m. Тоді G — скінченна група, порядок якої обмежений числом, що залежить лише від n і m.*

Доведення. Нехай T' — алгебраїчне замикання поля T. Над полем T' група G буде спряжена з групою матриць вигляду

$$g \to \begin{pmatrix} g_1 & * & \ldots & * \\ 0 & g_2 & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & g_s \end{pmatrix} \quad (g \in G), \tag{4}$$

де g_j пробігає абсолютно незвідну групу G_j над полем T'($j = 1, \ldots, s$). Згідно наслідку 5.1. G_j — скінченна група. Нехай

$$\gamma : G \to G_1 \times \cdots \times G_s$$

гомоморфізм такий, що $\gamma(g) = \mathrm{diag}[g_1, \ldots, g_s]$ (див. (4)). Тоді $\gamma(G)$ — скінченна група. Ядро гомоморфізму γ складається із унітрикутних матриць. Якщо $\mathrm{char}\, T = 0$, то неодинична унітрикутна матриця над полем T є елемент нескінченного порядку. Отже, в цьому випадку $\mathrm{Ker}\,\gamma$ — одинична група і тоді G — скінченна група. Нехай $\mathrm{char}\, T = p > 0$. Тоді $\mathrm{Ker}\,\gamma$ — p-група. Але в групі G нема елементів порядків p. Отже, і в цьому випадку $\mathrm{Ker}\,\gamma$ — одинична група. Теорема доведена.

Лема 5.1. *Абсолютно незвідна періодична матрична група $G \subset GL(n, T)$ над полем T буде локально скінченною групою.*

Доведення. Нехай M — скінченна множина елементів групи G і G_1 — група породжена множиною M. Потрібно довести, що G_1 — скінченна група. Можна вважати, що M — абсолютно незвідна множина (при необхідності можна приєднати елементи до M). Нехай P — просте підполе в T і P' — розширення поля P з допомогою всіх матричних елементів всіх матриць із множини M. Поле P' — скінченно породжене розширення простого поля P і група G_1 є абсолютно незвідною підгрупою групи $GL(n, P')$. Нехай P'' — алгебраїчне замикання поля P в полі P'. Тоді P'' — скінченне розширення поля P. Кожне власне значення α будь-якої матриці A із групи G_1 є, по-перше, коренем із одиниці а, по-друге, є коренем степеня n над P' характеристичного многочлена матриці A. Степінь алгебраїчності елемента α над полем P'' не перевищує n. Тоді степінь алгебраїчності цього елемента над полем P не перевищує nm, де $m = (P'' : P)$. Існує лише скінченне число таких коренів α із одиниці. Отже, множина $\mathrm{tr}(G_1)$ є скінченною і група G_1 також скінченна. Лема доведена.

Теорема 5.3 (Теорема Шура; [2]). *Періодична матрична група $G \subset GL(n, T)$ над полем T буде локально скінченною групою.*

Доведення. Можна вважати, що поле T — алгебраїчно замкнене. Нехай γ — гомоморфізм, розглянутий при доведені теореми 5.2. Із леми 5.1 слідує, що $\gamma(G)$ — локально скінченна група. Нехай $\mathrm{char}\, T = 0$. Тоді $\mathrm{Ker}\,\gamma = \{E\}$ і $\gamma(G) \cong G$ — локально скінченна група. Нехай $\mathrm{char}\, T = p$. Тоді $\mathrm{Ker}\,\gamma$ — підгрупа локально скінченної унітрикутної групи $UT(n, T)$ і, отже, $\mathrm{Ker}\,\gamma$ — локально скінченна група. Тоді група G є розширення локально скінченної групи з допомогою локально скінченної групи $\gamma(G)$. Це значить, що група G також локально скінченна. Теорема доведена.

Наслідок 5.3. *Силовська p-підгрупа групи $GL(n, T)$ над полем T буде локально скінченною групою.*

Наслідок 5.4. *Нехай $\mathrm{char}\, T \neq p$. Силовська p-підгрупа групи $GL(n, T)$ над полем T буде цілком звідною групою.*

Доведення випливає із наслідку 5.3 і ознаки Платонова цілком звідності груп.

Проблеми Бернсайда.

1. Чи буде скінченною скінченно породжена періодична група (необмежена проблема Бернсайда)?

2. Нехай дано натуральні числа $n > 1$ і $k > 1$. Чи буде скінченною група експоненти n і з числом твірних не більше ніж k (обмежена проблема Бернсайда)?

3. Нехай $B(k, n) = F_k/(F_k)^n$ — фактор-група вільної групи F_k з k твірними за підгрупою, породженою n-ми степенями всіх елементів групи F_k. Питання 2 еквівалентно питанню про скінченність групи $B(k, n)$.

Деякі відповіді. Скінченними є групи:

$$B(k, 2), B(k, 3), B(k, 4), B(k, 6).$$

П. С. Новіков анонсував негативну відповідь на обмежену проблему, а Є. С. Голод довів негативну відповідь на необмежену проблему Бернсайда.

З робіт П. С. Новікова, С. І. Адяна, О. І. Кострикіна випливає існування для досить великих простих p скінченно породженої нескінченної простої p-групи показника[1] p.

О. І. Кострикін довів існування такої константи $r(k,p)$, що порядок любої скінченної p-групи показника p і з k твірними не перевищує цю константу.

§6. Теорема Кліффорда

Нехай G — група, H — нормальна підгрупа групи G і

$$\Delta : H \to GV(d,T)$$

зображення групи H над полем T. Нехай $g \in G$. Тоді відображення

$$\Delta^g : H \to GV(d,T), \quad \Delta^g(h) = \Delta(g^{-1}hg) \quad (h \in H) \tag{1}$$

буде також зображенням групи H над полем T. Воно називається *спряженим* до Δ за допомогою елемента g. Нехай далі G — незвідна група, V — лінійний простір в якому діє група G.

Лема 6.1. *Нехай M — ненульовий незвідний H-підпростір лінійного простору V. Тоді для кожного $g \in G$ підпростір $g(M)$ простору V буде незвідним H-підпростором і $V = \sum\limits_{g\in G} g(M)$ є цілком звідним.*

Доведення. Нехай $h \in H$. Тоді

$$h(g(M)) = hg(M) = g(g^{-1}hg)M = g(M),$$

так як $h' = g^{-1}hg \in H$ і $h'(M) = M$. Отже, $g(M)$ — H-підпростір простору V. Неважко бачити, що це незвідний H-підпростір. Нехай $V_1 = \sum\limits_{g\in G}(g(M))$. Тоді

$$g(V_1) = g\left(\sum_{x\in G}(x(M))\right) = \sum_{x\in G}(gx(M)) = \sum_{y\in G}(y(M)) = V_1,$$

тобто V_1 — G-підпростір незвідного G-простору V. Отже, $V_1 = V$ і H-простір V буде цілком звідними як сума незвідних H-підпросторів $g(M)$ $(g \in G)$. Лема доведена.

Теорема 6.1 (Теорема Кліффорда; [2]). *Нормальна підгрупа H незвідної матричної групи $G \subset GV(n,T)$ над полем T є цілком звідною групою.*

Доведення випливає із леми 6.1.

Нехай виконуються умови леми 6.1. Введемо в розгляд множину $\mathrm{St}(M)$ всіх елементів g групи G таких, що H-підпростір $g(M)$ є ізоморфний H-підпросторові M. Множина $\mathrm{St}(M)$ називається *стабілізатором* H-підпростору M в групі G. Так як $h(M) = M$ $(h \in H)$, то $H \subseteq \mathrm{St}(M)$.

Лема 6.2. *Стабілізатор $\mathrm{St}(M)$ є підгрупою групи G.*

Доведення. Нехай g_1, $g_2 \in \mathrm{St}(M)$ і

$$\varphi_1 : M \to g_1(M), \quad \varphi_2 : M \to g_2(M)$$

ізоморфізми H-просторів. Тоді $\varphi = g_1\varphi_2 g_1^{-1}\varphi_1$ буде відображенням $M \to g_1g_2(M)$. Нехай $h \in H$. Тоді $h^{-1}\varphi h = h^{-1}g_1\varphi_2 g_1^{-1}h\varphi_1 = h^{-1}g_1\varphi_2 h_1 g_1^{-1}\varphi_1 = g_1h_1^{-1}\varphi_2 h_1 g_1^{-1}\varphi_1 = \varphi$.

[1] *Показник* періодичної групи — найменше спільне кратне порядків її елементів.

Звідси слідує, що φ — ізоморфізм H-простору M на H-простір $g_1g_2(M)$. Отже, $g_1g_2 \in$ $\in \mathrm{St}(M)$. Лема доведена.

Введемо простір

$$L = \sum_{x \in \mathrm{St}(M)} x(M).$$

Неважко бачити, що L — $\mathrm{St}(M)$-простір і L — цілком звідний H-простір, причому

$$L \cong M \dot{+} \cdots \dot{+} M.$$

Нехай G/St — множина всіх представників лівих суміжних класів групи G за підгрупою $\mathrm{St}(M)$ (будемо вважати, що одиниця входить в цю множину) і $g \in G/\mathrm{St}$. Тоді $g(L)$ — цілком звідний H-простір і

$$g(L) \cong g(M) \dot{+} \cdots \dot{+} g(M).$$

Відмітимо, що $M \cong g(M)$ (як H-простори) тоді і тільки тоді, коли $g \in \mathrm{St}(M)$. Із сказаного випливає, що коли g_1, g_2 різні елементи із G/St, то сума $g_1(L) + g_2(L)$ буде прямою сумою H-просторів. Нехай

$$V_2 = \sum_{x \in G/St} x(L).$$

Неважко бачити, що V_2 — G–підпростір в V. Отже, $V_2 = V$. Нехай натуральне число t є найбільше таке, що існують елементи $g_1, \ldots, g_t$ ($g_1 = 1$) множини G/St, для яких сума

$$V_3 = g_1(L) + \cdots + g_t(L)$$

буде прямою сумою H-підпросторів. Якщо існує $g \in G/\mathrm{St}$ ($g \neq g_1, \ldots, g \neq g_t$), то незвідні прямі доданки в H-підпросторі $g(L)$ (вони ізоморфні) не будуть ізоморфні незвідним прямим доданками в H-підпросторі V_3. Тоді сума $V_3 + g(L)$ буде прямою сумою H-підпросторів. Це суперечить вибору числа t. Отже, $V_3 = V$, тобто

$$V = g_1(L) \oplus \cdots \oplus g_t(L) \tag{2}$$

— пряма сума H-підпросторів і, окрім цього, $G/\mathrm{St} = \{g_1, \ldots, g_t\}$ та $t = [G : \mathrm{St}(M)]$.

Нехай $g \in G$. Для кожного номера $i \in \{1, \ldots, t\}$ існує єдиний номер $j \in \{1, \ldots, t\}$ такий, що

$$g_j^{-1} g g_i \in \mathrm{St}(M). \tag{3}$$

Тоді

$$g(g_i L) = g_j L. \tag{4}$$

Нехай $L^G = TG \otimes_{\mathrm{St}(M)} L$ — індукований TG-модуль. Із (2)–(4) випливає ізоморфізм G-просторів $V \cong L^G$.

Підсумовуючи сказане, одержуємо деталізацію теореми 6.1.

Теорема 6.2 (Теорема Кліффорда; [2]). *Нехай G — незвідна підгрупа групи $GV(n,T)$ над полем T, H — нормальна підгрупа групи G, V — лінійний простір над полем T, в якому діє група G, M — ненульовий незвідний H-підпростір в просторі V, $\mathrm{St}(M)$ — стабілізатор H-підпростору M в групі G і $L = \sum\limits_{x \in \mathrm{St}(M)} x(M)$. Тоді виконуються умови:*

1) *V — цілком звідний H-простір;*
2) *H-простір L є однорідно цілком звідний, точніше $L \cong M \dot{+} \cdots \dot{+} M$;*
3) *$t = [G : \mathrm{St}(M)] < \infty$;*
4) *$V \cong L^G$;*
5) *$n = (\dim M)st$, де $s = (\dim L)/(\dim M)$ — число прямих доданків M в H-просторі L.*

Наслідок 6.1. *Нехай Δ — незвідне T-зображення групи H, що відповідає просторові M, Γ — T-зображення групи $\mathrm{St}(M)$, що відповідає просторові L. Тоді*

$$\Gamma = \underbrace{\Delta + \cdots + \Delta}_{s}.$$

Група G спряжена з групою $\Gamma^G(G)$, де Γ^G — індуковане зображення групи G. При цьому група H спряжена з групою матриць

$$\{\mathrm{diag}[\Gamma^{g_1}(h), \ldots, \Gamma^{g_t}(h)] | h \in H\}.$$

Наслідок 6.2. *Якщо $t > 1$, то група G — імпримітивна.*

§7. Трикутна і унітрикутна групи

Нехай F — поле, $T(n, F)$ — підгрупа в $GL(n, F)$ всіх верхніх трикутних матриць порядку n над полем T, $UT(n, F)$ — підгрупа в $T(n, F)$ всіх *унітрикутних матриць* (тобто трикутних матриць з одиницями на діагоналі). Групи

$$T(n, T),\ UT(n, F)$$

називаються *трикутною* і відповідно *унітрикутною* групами степеня n над полем F. Неважко бачити, що унітрикутна група $UT(n, F)$ є нормальною підгрупою трикутної групи $T(n, F)$ і

$$T(n, F) = UT(n, F)D(n, F),$$

де $D(n, F)$ підгрупа всіх діагональних матриць степеня n над полем F. Відмітимо, що унітрикутна група $UT(n, F)$ породжується тими елементарними матрицями $t_{ij}(\lambda)(\lambda \in F)$, для яких $j > i$.

Нагадаємо деякі означення. Нехай G — довільна група, A, B — підгрупи групи G. Через $[A, B]$ позначається підгрупа в G, що породжується всіма комутаторами $[a, b]$ $(a \in A, b \in B)$. Ряд

$$G \supset G' \supset \cdots \supset G^{(k)} \quad (G' = [G, G], G^k = [G^{(k-1)}, G^{(k-1)}], k > 1)$$

називається *рядом комутантів* групи G, G' називається *комутантом* групи G. Група G є розв'язною групою тоді і тільки тоді, коли $G^{(k)}$ — одинична підгрупа для деякого k. Якщо G — розв'язна група, то найменше $k = k(G)$ з $G^{(k)} = 1$ називається *довжиною* ряду комутантів групи G. Якщо G — нетривіальна абелева група, то $k(G) = 1$.

Ряд

$$1 \subset Z_1 \subset \ldots \subset Z_{k-1} \subset Z_k \subset \ldots,$$

де $Z_1 = \mathfrak{Z}(G), Z_k$ — така підгрупа в G, що

$$Z_k/Z_{k-1} = \mathfrak{Z}(G/Z_{k-1}) \quad (k > 1),$$

називається *верхнім центральним рядом* групи G. Група G буде нільпотентною групою тоді і тільки тоді, коли її верхній центральний ряд доходить до групи G, тобто $Z_k = G$ для деякого k, при цьому, найменше k називається *степенем нільпотентності* групи G. Нільпотентна група степеня $k = 1$ буде абелевою групою.

Ряд

$$G \supset \Gamma_1 \supset \ldots \supset \Gamma_{k-1} \supset \Gamma_k \supset \ldots,$$

де

$$\Gamma_1 = [G, G], \quad \Gamma_k = [G, \Gamma_{k-1}] \quad (k > 1),$$

називається *нижнім центральним рядом* групи G. Група G є нільпотентною групою степеня k тоді і тільки тоді, коли Γ_k — одинична група і при цьому k — найменше.

Теорема 7.1. *Унітрикутна група $UT(n,F)$ $(n>1)$ є нільпотентна група степеня нільпотентності $n-1$. Довжина ряду комутантів групи $UT(n,F)$ рівна $d=$ $=[\log_2(n-1)]+1$. Трикутна група $T(n,F)$ є розв'язна група з довжиною ряда комутантів $d+1$.*

Доведення. Позначимо через b_j — j-ву бічну діагональ, паралельну головній діагоналі матриць із групи $UT(n,F)$ $(j=1,\ldots,n-1)$. Якщо $A=(\alpha_{ij})$, то

$$b_1(A)=(\alpha_{12},\ldots,\alpha_{n-1n}),$$

$$b_j(A)=(\alpha_{1j+1},\ldots,\alpha_{n-jn}),$$

$$b_{n-1}=(\alpha_{1n}).$$

Знайдемо верхній центральний ряд групи $UT(n,F)$. При цьому скористаємось такою властивістю: матриця

$$t_{ij}^{-1}(1)At_{ij}(1)=t_{ij}(-1)At_{ij}(1)$$

одержується з матриці A, якщо до j-го стовпчика додати i-ий та від i-го рядка відняти j-ий рядок. Поступово упевнюємось в тому, що у верхньому центральному ряді групи $UT(n,F)$ перший член Z_1 складається з тих матриць, у яких всі бічні діагоналі b_j є нульові, окрім діагоналі b_{n-1}; другий член Z_2 складається з матриць, у яких нульовими є всі бічні діагоналі, окрім діагоналей b_{n-2}, b_{n-1}; і т. д. $(n-2)$-ий член Z_{n-2} складається із тих матриць, у яких перша діагональ b_1 є нульова; $Z_{n-1}=UT(n,F)$.

Зокрема, комутант G' групи $G=UT(n,F)$ суміщається з Z_{n-2} і нижній центральний ряд цієї групи суміщається з верхнім, записаному у зворотньому порядку. Таким чином, група $UT(n,F)$ є нільпотентна степеня нільпотентності $n-1$. Другий комутант G'' групи $UT(n,F)$ складається із тих матриць, у яких перші $1+2$ бічні діагоналі є нульові; група G''' складається із тих матриць, у яких перші $1+2+4$ бічні діагоналі є нульові і т. д. Теорема доведена.

Лема 7.1. *Нехай $U=[UT(n,F)]_F$ — лінійна оболонка групи $UT(n,F)$ і $R=$ $=\{A-E|A\in UT(n,T)\}$. Тоді*

$$R=\operatorname{Rad}U,\ R^n=0,\ U/R\cong F.$$

Доведення. Множина R є двостороннім ідеалом алгебри U над полем F. Матричні одиниці $e_{ij}(j>i)$ утворюють базис цього ідеала над полем F. Добуток $e_{ij}\cdots e_{ts}$ упорядкованої множини r цих одиниць тільки тоді може бути відмінний від нуля, коли $s-i\geq r$. Звідси слідує, що добуток n будь-яких елементів із R є нульовий. Це доводить лему.

Наслідок 7.1. *Нехай $T=[T(n,F)]_F$ — лінійна оболонка трикутної групи $T(n,F)$. Тоді*

$$\operatorname{Rad}T=R,\ T/R\cong\underbrace{T\oplus\cdots\oplus T}_{n}.$$

Відмітимо, що будь-яка матриця $A\in UT(n,F)$ буде подібна нормальній формі Жордана:

$$\mathrm{J}(A)=\operatorname{diag}[J_s(1),\ldots,J_t(1)],\qquad(1)$$

де $J_r(1)$ — клітка Жордана порядку r з одиницями на діагоналі.

Лема 7.2.

1) *Нехай* $\operatorname{char}F=p>0$. *Тоді унітрикутна група $UT(n,F)$ буде p-групою. Нехай $A\in UT(n,F)$, r — найбільший із розмірів кліток Жордана в $\mathrm{J}(A)$ (див. (1)). Тоді порядок елемента A дорівнює p^k, де показник k найменший такий, що $p^k\geq r$.*
2) *Нехай* $\operatorname{char}F=0$. *Тоді група $UT(n,F)$ буде групою без кручення.*

Доведення. 1) $(A-E)^r = 0, A^{p^k} - E = (A-E)^{p^k} = 0$ тоді і тільки тоді, коли $p^k \geq r$. Звідси випливає твердження 1). У випадку 2) клітка Жордана $J_r(1)$ — елемент нескінченного порядку в групі $UT(n,F)$. Звідси випливає 2). Лема доведена.

Нехай характеристика поля F рівна $p > 0$. Розглянемо p-підгрупи повної лінійної групи $GL(n,F)$.

Лема 7.3. *Нехай* $\operatorname{char} F = p > 0$. *Якщо* H — *абсолютно незвідна* p*-підгрупа групи* $GL(n,F)$, *то* $n = 1$, $H = 1$.

Доведення. Якщо A — p-елемент групи, то всі власні значення матриці A рівні одиниці. Тоді $\operatorname{tr} A = n$ і, отже, $|\operatorname{tr}(H)| = 1$. Із теореми 5.1 Бернсайда слідує, що H — одинична група і тоді, в силу незвідності H, буде $n = 1$. Лема доведена.

Теорема 7.2. *Нехай* $\operatorname{char} F = p > 0$. *Будь-яка* p*-підгрупа групи* $GL(n,F)$ *спряжена з деякою підгрупою групи* $UT(n,F)$. *Група* $UT(n,F)$ *є силовська* p*-підгрупа групи* $GT(n,F)$. *Силовські* p*-підгрупи групи* $GL(n,F)$ *будуть спряжені між собою.*

Доведення. Нехай F' — алгебраїчне замикання поля F. Нехай G — p-підгрупа групи $GL(n,F)$. Із теореми про канонічний вигляд матричних груп і леми 7.3 слідує, що група G спряжена в групі $GT(n,F')$ з деякою підгрупою групи $UT(n,F')$. Нехай $A = [G]_F$, $B = \langle g - E | g \in G \rangle$ — підалгебра в A з вказаними твірними елементами. Тоді B спряжена з підалгеброю нільпотентної алгебри $[UT(n,F']_{F'}$ (див. лему 7.1) і, отже, B — нільпотентна алгебра. Окрім того, B — двосторонній ідеал в алгебрі A і $A/B \cong F$. Нехай V — лінійний простір, в якому діє група G і s — найменше натуральне число таке, що $B^s = 0$. Розглянемо ряд підпросторів

$$V \supset BV \supset \cdots \supset B^{s-1}V \supset B^sV = 0$$

і проведемо базис простору V через базиси цих підпросторів. Так як

$$(g-1)V \subseteq BV,\ (g-1)B^jV \subseteq B^{j+1}V\ (j \geq 1),$$

то у вибраному базисі всі оператори із групи G будуть мати унітрикутні матриці. Отже, будь-яка p-підгрупа G (в тому числі і силовська p-підгрупа) в групі $GL(n,F)$ спряжена в цій групі з підгрупою в унітрикутній групі $UT(n,F)$. Теорема доведена.

Приведемо інший варіант доведення теореми 7.2, заснований на такому результаті в теорії зображень скінченних груп над полями: скінченна p-група має тільки одне незвідне зображення над полем характеристики p — це одиничне зображення.

Нехай G — будь-яка незвідна p-підгрупа в групі $GL(n,T)$, де F — поле характеристики p. Існує скінченна незвідна система матриць із групи G така, що кожна матриця із групи G буде лінійною комбінацією над полем F цієї системи. Так як G — локально скінченна група, то підгрупа H, що породжується вибраною системою матриць буде скінченною незвідною підгрупою групи $GL(n,T)$. Із вказаного результату теорії зображень груп випливає, що група H — є одинична. Тоді $n = 1$ і G — одинична група. Тепер теорема 7.2 випливає з теореми про канонічний вигляд матричної групи.

§8. Примітивні розв'язні групи

Лема 8.1. *Нехай група A буде розширенням свого центра $F = \mathfrak{Z}(A)$ за допомогою скінченної абелевої групи і комутант $A' = [A, A]$ групи A є циклічна група порядку m. Тоді в групі A існують такі пари $(a_1, b_1), \ldots, (a_t, , b_t)$ елементів, що виконуються умови:*

1) *елементи різних пар перестановочні;*
2) *якщо m_i — порядок комутатора $[a_i, b_i]$, то $m_1 = m$, m_{i+1} ділить m_i $(i = 1, \ldots, t-1)$, при $t > 1$;*
3) *$A/F = \overline{a}_1 \times \overline{b}_1 \times \cdots \times \overline{a}_t \times \overline{b}_t$, де $\overline{a}$ позначає суміжний клас aF $(a \in A)$;*
4) *порядок елемента $\overline{a}_i$ дорівнює порядку $\overline{b}_i$ і дорівнює m_i $(i = 1, \ldots, t)$.*

Доведення. Якщо a, b, $c \in A$, то враховуючи, що A/F абелева $\overline{[a, c]} = [\overline{a}, \overline{c}] = \overline{1}$. Отже, $[a, c] \in F = \mathfrak{Z}(A)$ і $[a, c]^b = [a, c]$. Тому

$$[ab, c] = [a, c]^b [b, c] = [a, c][b, c], \quad \text{аналогічно} \quad [a, bc] = [a, b][a, c]. \tag{1}$$

Коли $b \in F$, то $[b, c] = [a, b] = 1$ і

$$[ab, c] = [a, bc] = [a, c].$$

Нехай $a \in A$ і $\varphi_a : A \to A'$ таке відображення, що

$$\varphi_a(x) = [a, x] \quad x \in A.$$

Тоді із (1) слідує, що φ_a — гомоморфізм групи A в комутант A'.

Нехай a такий елемент групи A, що $\overline{a}$ є елементом найвищого порядку m_1 в групі A/F. Відмітимо, що m_1 — найменше спільне кратне порядків всіх елементів скінченної абелевої групи A/F. Із (1) випливає, що $[a, A]$ — підгрупа циклічної групи A'. Нехай b такий елемент в A, що $\varepsilon = [a, b]$ є твірний елемент групи $[a, A]$. Так як

$$1 = [a^{m_1}, b] = \varepsilon^{m_1},$$

то порядок r елемента ε ділить m_1. З другого боку, якщо $x \in A$, то $[a^r, x] = [a, x]^r = (\varepsilon^t)^r = 1$, звідки випливає, що $a^r \in F$ і тоді m_1 ділить r. Отже, $r = m_1$. Далі, порядок s елемента $\overline{b}$ в групі A/F ділить m_1. А так як $1 = [a, b^s] = \varepsilon^s$, то m_1 ділить s. Отже, всі три елементи $\overline{a}, \overline{b}, [a, b]$ мають однаковий порядок m_1. Нехай x, y — довільні елементи групи A. Так як $x^{m_1} \in F$, то $1 = [x, y]^{m_1}$, тобто порядок комутатора $[x, y]$ ділить порядок підгрупи $[a, A]$ циклічної групи A'. Це значить, що $[x, y] \in [a, A]$. Отже, $A' \subset [a, A]$, тобто $A' = [a, A]$ і значить $m_1 = m$. За першу пару (a_1, b_1) можна взяти пару (a, b).

Неважко бачити, що φ_a, φ_b — епіморфізми і

$$A = \langle b, \operatorname{Ker} \varphi_b \rangle = \langle a, \operatorname{Ker} \varphi_a \rangle = \langle a, b, A_1 \rangle,$$

де $A_1 = \operatorname{Ker} \varphi_a \bigcap \operatorname{Ker} \varphi_b$.

Якщо для деяких натуральних чисел r, s виконується рівність $\overline{a}^r = \overline{b}^s$, то $1 = [b^s, b] = [a^r f, b] = [a^r, b] = \varepsilon^r$, де $f \in F$, що можливо тільки тоді, коли r ділиться на m_1. Отже, $\overline{a}^r = \overline{b}^s = \overline{1}$. Звідси випливає, що добуток $\langle \overline{a} \rangle \langle \overline{b} \rangle$ є прямий.

Центр $\mathfrak{Z}(A_1)$ групи A_1 суміщається з групою F. Якщо $A_1 \neq F$, то комутант $(A_1)'$ групи A_1 буде циклічною групою, порядок m_2 якої ділить m і в цьому випадку група A_1 задовольняє тим же умовам, що й група A. Нехай $A_1 \neq F$ і $\overline{A}_1 = A_1/F$. Якщо $\overline{a}^s \overline{b}^r \in \overline{A}_1$, то $a^s b^r \in \operatorname{Ker} \varphi_a$ і тоді $1 = [a, a^s b^r] = [a, b]^r$, звідки випливає, що r ділиться на m_1. Аналогічно доводиться, що s також ділиться на m_1. Таким чином, добуток

$\left(\langle\overline{a}\rangle \times \langle\overline{b}\rangle\right)\overline{A}_1$ є прямий і суміщається з групою $\overline{A}$. Окрім цього, до групи A_1 можна застосовувати індуктивне припущення. Це доводить лему.

Нагадаємо, група G називається *розв'язною*, коли її *ряд*

$$G \supset G' = [G,G] \supset \cdots \supset G^{(i)} \supset G^{(i+1)} = [G^{(i)}, G^{(i)}] \supset \cdots$$

послідовних комутантів доходить до одиничної підгрупи через скінченне число членів ряду. Група G є розв'язною тоді і тільки тоді, коли якщо існує нормальний ряд

$$1 = G_0 \subset G_1 \subset \ldots \subset G_{i-1} \subset G_i \subset \ldots \subset G_s = G,$$

всі фактори G_i/G_{i-1} $(i = 1, 2, \ldots, s)$ якого є абелеві групи. k-ою *комутаторною дужкою* називається індуктивно визначена функція

$$D^k(x_1, \ldots, x_s, y_1, \ldots, y_s)$$

від $2s = 2^k$ елементів групи G:

$$D^1(x,y) = [x,y];$$

$$D^2(x_1,x_2,y_1,y_2) = D^1(D^1(x_1,x_2), D^1(y_1,y_2));$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$D^k(x_1,\ldots,x_s,y_1,\ldots,y_s) = D^1(D^{k-1}(x_1,\ldots,x_s), D^{k-1}(y_1,\ldots,y_s)).$$

Група G буде розв'язною тоді і тільки тоді, коли для деякого натурального числа k довільна комутаторна дужка D^k тотожно рівна одиниці групи G.

Нехай далі G — розв'язна примітивна підгрупа групи $GL(n,T)$ над полем T; F — максимальна нормальна абелева підгрупа групи G; $V = \mathfrak{Z}_G(F)$ — *централізатор* підгрупи F в групі G (це сукупність всіх тих елементів групи G, які комутують з кожним елементом групи F); A — така максимальна нормальна підгрупа в групі G, що A міститься в групі V і фактор-група A/F є абелевою групою.

Відмітимо, що група V є нормальною підгрупою групи G. Ці 4 групи утворюють ряд

$$F \subset A \subset V \subset G,$$

нормальних підгруп групи G. Цей ряд будемо називати *рядом Супруненко*.

Лема 8.2. *Або $V = F$, або для групи G і її підгрупи F існує ряд Супруненка, в якому група A не суміщається з групою F.*

Доведення. Нехай V/F — неодинична група і A_1 — така підгрупа в групі V, що $F \subset A_1$ і група A_1/F — останій неодиничний член ряду комутантів групи V/F. Тоді A_1/F — абелева підгрупа в групі V/F, яка залишається незмінною при дії довільного автоморфізма групи V/F, зокрема, A_1 — нормальна підгрупа групи G. Далі групу A вибираємо так, щоб $A_1 \subseteq A$. Лема доведена.

Введемо ще деякі позначення. Нехай поле K — розширення степеня $d = (K:T)$ поля T і $\{e_1, \ldots, e_d\}$ — деякий T-базис поля K. Позначимо через $\widetilde{\alpha}$ — матрицю оператора множення на $\alpha \in K$ у вказаному базисі (j-ий стовпчик матриці $\widetilde{\alpha}$ це координатний стовпчик елемента αe_j поля K). Через $\widetilde{K}$ будемо далі позначати поле $\{\widetilde{\alpha} | \alpha \in K\}$. Очевидно, що $K \cong \widetilde{K}$, зокрема, $T \cong \widetilde{T} = \{aE_d | a \in T\}$.

Вивчимо властивості ряду Супруненка, в якому $A \neq F$.

Лема 8.3. *Існує таке точне незвідне зображення $\Delta : F \to GL(d,T)$ групи F, степінь d якого ділить n, що*

1) *група F спряжена з групою матриць*

$$\mathrm{diag}[\Delta(a), \ldots, \Delta(a)] \quad (a \in F);$$

2) *лінійна оболонка* $[\Delta(F)]_T$ *є полем* $\widetilde{K}$, *де поле* K — *деяке розширення степеня* d *поля* T;
3) *група* V *спряжена з підгрупою групи* $GL(r, \widetilde{K})$, *де* $r = n/d$;
4) *група* G/V *ізоморфна деякій підгрупі групи Галуа* $G(K, T)$ *поля* K *над полем* T.

Доведення. Зрозуміло, що F є нормальною підгрупою незвіднї групи G. Із теорем Кліффорда випливає, що група F є *однорідно цілком звідною групою*, точніше, існує таке точне незвідне T — зображення Δ групи F, що група F спряжена з групою матриць

$$\begin{pmatrix} \Delta(a) & 0 & \dots & 0 \\ 0 & \Delta(a) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \Delta(a) \end{pmatrix} \quad (a \in F),$$

звідки, зокрема, слідує, що степінь d зображення Δ ділить n. За наслідком 4.2 лінійна оболонка $[\Delta(F)]_T \cong M(s, K)$, де K — d/s-вимірне тіло над полем T. Оскільки F абелева група, то $[\Delta(F)]_T$ буде комутативною алгеброю, а, отже, $s = 1$, K — поле, що є d-вимірним розширенням поля T. Оскільки $[\Delta(F)]_T \cong K$, то $[\Delta(F)]_T = \widetilde{K}$. Група V буде спряжена з групою матриць над централізатором поля $\widetilde{K}$ в кільці $M(d, T)$. Згідно теорем Сколема-Ньотер, цей централізатор суміщається з самим полем $\widetilde{K}$. Отже, група V спряжена з підгрупою групи $GL(n/d, \widetilde{K})$. Внутрішній автоморфізм $I_{g^{-1}} : x \to gxg^{-1}$ групи G індукує деякий автоморфізм σ_g поля $\widetilde{K}$ над полем T. Відповідність $g \to \sigma_g$ $(g \in G)$ буде гомоморфізмом $\sigma : G \to G(\widetilde{K}, T)$ групи G в групу Галуа поля $\widetilde{K}$ над полем T. Ядро гомоморфізму σ суміщається з групою V. Це доводить лему.

Далі будемо вважати, що групи F, A, V є підгрупами групи $GL(r, \widetilde{K})$.

Лема 8.4. *Центр* $\mathfrak{Z}(A)$ *групи* A *суміщається з групою* F. *Комутант* A' *групи* A *є циклічна група, порядок якої ділить число* $r = n/d$. *Централізатор* $\mathfrak{Z}_V(A)$ *групи* A *в групі* V *суміщається з групою* F.

Доведення. $F \subseteq \mathfrak{Z}(A)$. Група $\mathfrak{Z}(A)$ залишається незмінною при дії довільного автоморфізма групи A. Тому $\mathfrak{Z}(A)$ буде нормальною підгрупою в групі G. Припущення $F \neq \mathfrak{Z}(A)$ веде до протиріччя з вибором групи F. Отже, $F = \mathfrak{Z}(A)$. Нехай $[a, b]$ — комутатор довільних елементів a, b групи A. Тоді $[a, b] \in F$ і, якщо $\alpha = \Delta([a, b])$, то $[a, b] = \alpha E_r$. Переходячи в рівності

$$ab = \alpha E_r ba$$

до детермінантів над полем $\widetilde{K}$, одержимо $\alpha^r = 1$ в полі $\widetilde{K}$. Так як A' є абелева група $(A' \subset F)$, то кожний елемент групи A' є коренем рівняння $x^r = 1$ над полем K. Отже, група A' є підгрупа циклічної групи порядку r. Очевидно, $F \subseteq C = \mathfrak{Z}_V(A)$ і C нормальна підгрупа групи G. Нехай $F \neq C$ і C_1 — така підгрупа в групі V, що абелева група C_1/F є першим неодиничним членом ряду комутантів групи C/F (тобто $C_1 \neq F$). Тоді C_1 — нормальна підгрупа групи G і група AC_1 є такою нормальною підгрупою в групі G, що $AC_1 \subset V$ і $(AC_1)/F$ — абелева група. Тоді $C_1 \subset A$, в силу вибору групи A, тобто, $C_1 \subset \mathfrak{Z}_V(A) \bigcap A = \mathfrak{Z}(A) = F$, інакше кажучи, $C_1 = F$. Протиріччя. Отже, $C = F$. Лема доведена.

Далі доцільно вважати, що групи F, A, V є підгрупами групи $GL(r, K)$ (досить замінити елементи поля $\widetilde{K}$ на відповідні елементи поля K). Якщо $f \in F$, $a \in A$, то $f = \alpha E_r$ для деякого $\alpha \in K$ і $fa = \alpha a$. Для a, $b \in A$ $[b, a] \in F$ і для деякого $\beta \in K$ $a^b = b^{-1}ab = a[b, a] = a\beta = \beta a$.

Лема 8.5. *Фактор-група* A/F *є скінченною групою і її порядок* $[A : F]$ *дорівнює розмірності* $\dim_K [A]_K$ *лінійної оболонки* $[A]_K$ *групи* A *над полем* K.

Доведення. Нехай $t = \dim_K [A]_K$ і

$$a_1, \ldots, a_t \tag{2}$$

— базис оболонки $[A]_K$ над полем K, вибраний із елементів групи A. Тоді суміжні класи групи A за підгрупою F

$$a_1 F, \ldots, a_t F \tag{3}$$

є попарно різні (якщо $a_i F = a_j F$, то $a_i = \alpha a_j (\alpha \in K)$). Припустимо, що (3) не вичерпує всі суміжні класи групи A за підгрупою F. Тоді існує суміжний клас $B = bF$ $(b \in A)$ такий, що

$$b = \beta_1 a_1 + \cdots + \beta_t a_t \quad (\beta_i \in K). \tag{4}$$

Нехай в (4), наприклад, $\beta_1 \neq 0$. Так як $b^{-1}a_1$ не належить $F = \mathfrak{Z}(A)$, то існує елемент $a \in A$, який не перестановочний з $b^{-1}a_1$. Нехай

$$a^{-1}ba = \gamma b,\ a^{-1}a_j a = \gamma_j a_j \quad (\gamma, \gamma_j \in K). \tag{5}$$

Тоді в (5) $\gamma \neq \gamma_1$ і із (4) випливає, що

$$b = \gamma^{-1}(\beta_1\gamma_1 a_1 + \cdots + \beta_t\gamma_t a_t). \tag{6}$$

Із однозначності розкладів за базисом випливає, що

$$\beta_1 = \gamma^{-1}\beta_1\gamma_1,$$

що суперечить умові $\gamma \neq \gamma_1$. Отже, припущення про існування суміжного класу B, який не входив би в систему суміжних класів (3), невірне. Лема доведена.

Із лем 8.1, 8.4, 8.5 випливає такий результат.

Теорема 8.1. *В групі A існує така система пар*

$$(a_1, b_1),\ \ldots,\ (a_t, b_t) \quad (t > 1)$$

елементів для якої виконуються умови:
1) $A/F = \overline{a}_1 \times \overline{b}_1 \times \ldots \times \overline{a}_t \times \overline{b}_t$;
2) *порядки елементів $\overline{a}_i, \overline{b}_i, [a_i, b_i]$ рівні;*
3) *елементи різних пар перестановочні;*
4) *m_1 ділить r, m_{i+1} ділить m_i (m_i — порядок $\overline{a}_i$).*

Лема 8.6. *Централізатор $\mathfrak{Z}_{V/F}(A/F)$ групи A/F в групі V/F суміщається з групою A/F.*

Доведення. Нехай c такий елемент групи V, що cF комутує з кожним елементом групи A/F. Тоді $[c, a] \in F$ $(a \in A)$. Потрібно довести, що $c \in A$. Для цього побудуємо такі елементи $c_0, \ldots, c_t \in cA$, що елемент c_j комутує з елементами пар (a_i, b_i) для всіх $i \leqslant j$ $(i = 0, \ldots, t; (a_0, b_0) = (1, 1))$. Очевидно, $c_0 = c$. Нехай $i > 1$ і для $j < i$ елемент c_j уже вибрано. Знайдемо c_i. Перш за все відмітимо, що

$$[c_{i-1}, a_i]^{m_i} = [b_i, c_{i-1}]^{m_i} = 1,$$

звідки слідує, що

$$[c_{i-1}, a_i] = [b_i, a_i]^s, [b_i, c_{i-1}] = [b_i, a_i]^r$$

для деяких натуральних s, r. Тоді елемент $a_i^{-r}c_{i-1}b_i^{-s}$ буде задовольняти вимогам для елемента c_i. Останній елемент c_t комутує з елементами всіх пар (a_i, b_i) $(i = 1, \ldots, t)$, тобто належить $\mathfrak{Z}_V(A) = F$. Отже, $c \in A$ і лема доведена.

Теорема 8.2 (Теорема Супруненка; [2]). *В кожній примітивній розв'язній підгрупі групи $GL(n,T)$ (T — поле) існує абелева нормальна підгрупа, індекс якої не перевищує деякої константи $c(n) \leqslant n \cdot (n^2)!$.*

Доведення. Нехай G — примітивна розв'язна підгрупа групи $GL(n,T)$. Розглянемо ряд Супруненка цієї групи. Нехай $v \in V$ і $\varphi_v : A/F \to A/F$ таке відображення, що

$$\varphi_v(aF) = v(aF)v^{-1} \quad (a \in A).$$

Тоді φ_v — автоморфізм групи A/F, а відповідність $v \to \varphi_v$ ($v \in V$) — буде гомоморфізмом φ групи V в групу $\mathrm{Aut}(A/F)$ автоморфізмів групи A/F. Ядро гомоморфізму φ суміщається з групою A (див. лему 8.6). Тоді порядок $|G : A|$ не перевищує порядку $|\mathrm{Aut}(A/F)|$, що в свою чергу не перевищує числа всіх тих взаємно однозначних відображень множини A/F на себе, що зберігають одиничний клас F. Враховуючи, що $[G : V] \leqslant n$ (див. лему 8.3) і $[A : F] \leqslant n^2$ (див. лему 8.5), отримуємо

$$[G : F] = [G : V] \cdot [V : A] \cdot [A : F] \leqslant n \cdot (n^2 - 1)! \cdot n^2 \leqslant n \cdot (n^2)!,$$

що доводить теорему.

Теорема 8.3. *В кожній незвідній розв'язній підгрупі групи $GL(n,T)$ існує абелева нормальна підгрупа, індекс якої не перевищує деякої константи $c_1(n)$, залежної тільки від n.*

Доведення. Нехай G — імпримітивна розв'язна підгрупа групи $GL(n,T)$. Для деякого дільника r числа n існує така примітивна розв'язна підгрупа H групи $GL(r,T)$ і така розв'язна підгрупа S симетричної групи S_t ($t = n/r$), що група G буде підгрупою сплетіння $W = H \wr S$. Нехай F_0 — така абелева нормальна підгрупа в групі H, що $[H : F_0] \leqslant c(r)$. Тоді F_0^t — абелева нормальна підгрупа в групі W, індекс якої не перевищує $(c(r))^t \cdot t!$. Нехай $F = G \bigcap F_0^t$. Тоді F — абелева нормальна підгрупа групи G і

$$[G : F] = [G \cdot F_0^t : F_0^t] \leqslant [W : F_0^t].$$

Оскільки $c(r) \leqslant c(n)$, $r \leqslant n$, то

$$[G : F] \leqslant (c(n))^n \cdot n!,$$

що доводить теорему.

Теорема 8.4 (Теорема Цассенхауза; [2]). *Локально розв'язна підгрупа групи $GL(n,T)$ є розв'язною групою.*

Доведення. Нехай G — розв'язна підгрупа групи $GL(n,T)$ і $l(G)$ — довжина ряду комутантів групи G. Відмітимо, що $l(G)$ — мінімум довжин розв'язних рядів (нормальних рядів з абелевими факторами) групи G. Із теореми про канонічний вигляд матричної групи слідує, що група G є розширення деякої підгрупи U в $UT(n,T)$ з допомогою деякої підгрупи H в прямомому добутку $G_1 \times \ldots \times G_t$ деяких незвідних розв'язних підгруп

$$G_i \subset GL(n_i,T) \quad (i = 1,\ldots,t; n_1 + \cdots + n_t = n).$$

Тоді

$$l(G) \leqslant l(U) + l(H) \leqslant l(UT(n,T)) + l(G_1) \cdots l(G_t) \leqslant$$
$$\leqslant (c_1(n_1) + 1) \cdots (c_1(n_t) + 1) \leqslant l(UT(n,T)) + (c_1(n) + 1)^n = c_2(n).$$

Звідси слідує, що $c_2(n) = r$-ова комутаторна дужка D^r рівна тотожно одиниці на будь-якій розв'язній підгрупі групи $GL(n,T)$. Так як будь-яка скінченна множина

елементів локально розв'язної групи M породжує розв'язну групу, то комутаторна дужка D^r рівна одиниці на будь-якому наборі 2^r елементів групи $M \subset GL(n,T)$. Отже, будь-яка локально розв'язна підгрупа M групи $G(n,T)$ є розв'язна група. Теорема доведена.

Підгрупу H групи $GL(n,T)$ назвемо *триангульованою*, якщо ця підгрупа спряжена з підгрупою групи $T(n,T)$ трикутних матриць.

Теорема 8.5 (Теорема Колчина, Мальцева; [2]). *Нехай T — алгебраїчно замкнене поле. В будь-якій розв'язній підгрупі групи $GL(n,T)$ існує нормальна триангульована підгрупа, індекс якої не перевищує деякої константи, залежної тільки від числа n.*

Доведення. Якщо G — примітивна розв'язна підгрупа групи $GL(s,T)$, то максимальна нормальна абелева підгрупа F групи G складається з скалярних матриць (див. лема 8.3). Якщо G — незвідна розв'язна підгрупа, то в G існує нормальна підгрупа F діагональних матриць така, що $(G:F) \leqslant c_1(s) \leqslant c_2(n)$ (див. теорему 8.3 і її доведення). Нехай G — довільна розв'язна підгрупа групи $GL(n,T)$. Скористаємось теоремою про канонічний вид. Існує гомоморфізм γ групи G в прямий добуток $G_1 \times \cdots \times G_t$ незвідних підгруп $G_i \subset GL(n_i,T)$ із $\ker\gamma \subset UT(n,T)$. Нехай F_i — нормальна підгрупа діагональних матриць в групі G_i і індекс цієї підгрупи відповідно обмежений. Тоді група $N = G \bigcap \gamma^{-1}(F_1 \times \cdots \times F_t)$ має обмежений індекс в G і буде тріангульованою. Теорема доведена.

На закінчення цього параграфа наведемо ще один результат.

Теорема 8.6. *Нехай $T = \mathbb{R}$ — поле дійсних чисел і n — непарне число. Будь-яка незвідна розв'язна підгрупа G групи $GL(n,\mathbb{R})$ є мономіальна.*

Доведення. Досить показати, що при $n > 1$ в групі $GL(n,\,\mathbb{R})$ не існують примітивні розв'язні підгрупи. Нехай це не так і G — примітивна розв'язна підгрупа в $GL(n,\mathbb{R}), n > 1$. Розглянемо ряд Супруненка групи G. Якщо $K \neq T$, то $(K:T) = 2$, що неможливо в силу непарності числа n і умови: $(K:T)$ ділить n. Отже $K = T$ і $G = V$. Якщо $V \neq F$, то група A/F — скінченна неодинична, порядки елементів цієї групи ділять n і ділять порядок комутанта A' — підгрупи порядку 2 в групі $\mathbb{R}^*$, що неможливо в силу непарності n. Отже, $V = F, n = 1$ і теорема доведена.

§9. Вправи

Будь-яку матрицю над кільцем $\mathbb{Z}$ можна вважати матрицею над довільним полем F. Якщо $\operatorname{char} F = p > 0$, то поле F містить $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ — поле класів лишків за простим модулем p. Тоді цілі числа — це представники суміжних класів за модулем p, причому, різні цілі a та b можуть представляти один клас і тоді слід вважати, що $a = b$. В розглядуваному випадку $a = b$ тоді і тільки тоді, коли $a \equiv b \pmod p$. Зокрема, якщо a не ділиться на p, то існує тільки один суміжний клас з представником b, такий, що $ab \equiv 1 \pmod p$, тобто $a^{-1} = b$ в полі F.

Вправа 1. Нехай T — поле, $GL(n,T)$ — повна лінійна група степеня n над полем T, $SL(n,T)$ — відповідна спеціальна лінійна група степеня n над полем T.

а) Показати, що такі діагональні матриці порядку n

$$d(\lambda) = \operatorname{diag}[1,\ldots,1,\lambda] \quad (\lambda \in T^*)$$

(T^* — мультиплікативна група поля T) будуть представниками всіх як лівих так і правих суміжних класів групи $GK(n,T)$ за підгрупою $SL(n,T)$.

б) Нехай $A \in GL(n,T)$ і $\alpha = \det A$. Показати, що існують тільки по одній матриці C_1, C_2 з групи $SL(n,T)$ такі, що

$$A = C_1 d(\alpha) = d(\alpha) C_2.$$

Знайти ці матриці.

в) Нехай

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & -1 & 1 \\ 3 & 1 & -1 \end{pmatrix}.$$

Показати, що $A \in GL(3, \mathbb{Q})$. Знайти матриці C_1, C_2 для матриці A (див. б)). Знайти характеристики всіх полів T, таких, що $A \in GL(3, T)$. Показати, що $A \in GL(3, 7) = GL(3, \mathbb{Z}_7)$ і знайти матриці C_1, C_2 для A.

Вправа 2. Нехай T — поле із q елементів. Знайти порядки груп

$$GL(n, q) = GL(n, T), \quad SL(n, q), \quad PGL(n, q), \quad PSL(n, q).$$

Вправа 3. Нехай F — довільне поле,

$$E^- = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ і } O^-(2, F) = \{A \in M(2, F) | A^T E^- A = E^-\}.$$

Показати

а) що $O^-(2, F)$ буде групою. Ця група називається *ортогональною групою степеня 2 типу мінус* над полем F;

б) якщо $\operatorname{char} F = 2$, то $O^-(2, F) = GL(2, F)$;

в) якщо $\operatorname{char} F \neq 2$, то

$$O^-(2, F) = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \quad (\alpha \in F^*), \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle,$$

зокрема, якщо $F = \mathbb{Z}_p$, то група $O^-(2, \mathbb{Z}_p)$ ізоморфна групі діедра D_{p-1} порядку $2(p-1)$. Відмітимо, що для групи $O^-(2, \mathbb{Z}_p)$ вживають позначення $O^-(2, p)$.

Вправа 4. Показати, що така множина матриць порядку n над полем F :

$$\{A | A^T A = E\}$$

буде групою. Ця група називається *ортогональною групою степеня n типу плюс* над полем F і позначається через $O^+(n, F)$ або $O^+(n, q)$ у випадку $|F| = q$.

Показати

а)

$$O^+(2, 2) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong C_2;$$

б)

$$O^+(2, 3) = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong D_4;$$

в)

$$O^+(2, 5) = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong D_4;$$

г)

$$O^+(2, 7) = \left\langle 2\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong D_8;$$

д)

$$O^+(2, 11) = \left\langle \begin{pmatrix} 3 & 5 \\ -5 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong D_{12};$$

е)

$$O^+(2,13) = \left\langle \begin{pmatrix} 2 & 6 \\ -6 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong D_{12};$$

є)

$$O^+(2,4) = \left\langle \begin{pmatrix} \theta & 1+\theta \\ 1+\theta & \theta \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong C_2 \times C_2 \quad (\theta^2 = \theta + 1);$$

ж)

$$O^+(2,9) = \left\langle \begin{pmatrix} i & i \\ -i & i \end{pmatrix} \ (i^2 = -1), \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong D_8.$$

Вправа 5. Чи існують поля з 64, 100, 169, 625 елементів? Які в них характеристики?

Вправа 6. В групі $GL(2,7)$ розв'язати рівняння

$$\begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix} X = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}.$$

Вправа 7. В $GL(2,7)$ знайти порядок класу спряжених елементів, якому належить матриця

$$a = \begin{pmatrix} 0 & -4 \\ 1 & 2 \end{pmatrix}.$$

Вправа 8. Знайти класи спряжених елементів в $GL(2,5)$.

Вказівка: скористатись формулою $N_q(n) = \frac{1}{n}\sum\limits_{d|n} \mu(d) q^{\frac{n}{d}}$ для числа $N_q(n)$ примітивних незвідних многочленів степеня n над полем із q елементів. (μ — *функція Мьобіуса*, $\mu(n) = 0$, якщо n ділиться на квадрат простого числа, $\mu(n) = (-1)^s$, якщо n — добуток s різних простих чисел і $\mu(1) = 1$).

Вправа 9. Довести, що скінченна матрична група $G \in GL(n,T)$ над полем T характеристики нуль є незвідна, якщо її централізатор $\mathfrak{Z}_T(G)$ є тіло (поле).

Вправа 10. Нехай $C_n = \langle \widetilde{\sigma} \rangle$ — група, що породжується підстановочною матрицею цикла $\sigma = (12\ldots n)$. Знайти централізатор цієї групи над любим полем.

Вправа 11. Нехай G — група підстановочних матриць. Довести, що G — звідна група.

Вправа 12. Довести, що якщо G — незвідна абелева підгрупа групи $GL(n,\mathbb{C})$, то $n = 1$.

Вправа 13. Довести, що якщо G — незвідна абелева підгрупа групи $GL(n,\mathbb{R})$, то $n \leqslant 2$.

Вправа 14. Нехай T — поле. Довести, що якщо скінченна абелева підгрупа G групи $GL(n,T)$ є незвідна, то група G буде циклічна.

Зауваження: якщо скінченна абелева група нециклічна, то її порядок строго більший найменшого спільного кратного порядків всіх елементів цієї групи.

Вправа 15. Довести, що в групі $GL(n,\mathbb{Q})$ існують незвідні циклічні підгрупи.

Вправа 16. Нехай

$$G = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \right\rangle.$$

Довести, що група G є незвідна над полем дійсних чисел і звідна над полем комплексних чисел.

Вправа 17. Довести, що група

$$G = \left\langle a = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle \subset GL(3, \mathbb{Q})$$

є абсолютно незвідна.

Вправа 18. Знайти порядки груп

$$GL(2,p), \quad SL(2,p), \quad PGL(2,p), \quad PSL(2,p)$$

для $p = 2, 3, 5, 7$.

Вправа 19. Показати, що

$$GL(2,3) = \left\langle a = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle;$$

$$SL(2,3) = \langle a, b, c \rangle;$$

група $H = \langle a, b \rangle$ буде нормальною підгрупою в групах $SL(2,3)$ і $GL(2,3)$.

Вправа 20. Нехай i — уявна одиниця: $i^2 = -1$ і $P = \langle i \rangle$. Знайти сплетіння $G = P \wr C_3$. Які порядки груп P, G? Показати, що група G буде абсолютно незвідною підгрупою групи $GL(3, \mathbb{C})$.

Вправа 21. Нехай

$$G = \left\langle a = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \subset GL(2, T)$$

(T — поле). Знайти базис алгебри $[G]_T$.

Вправа 22. Довести, що спряжені матричні групи G_1 і G_2 над полем T ізоморфні.

Вправа 23. Нехай

$$G_1 = \left\langle a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, \quad G_2 = \left\langle a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

— дві підгрупи групи $GL(2, \mathbb{C})$. Показати, що вони спряжені.

Вправа 24. Показати, що група

$$G = \left\langle a = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},\ b = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \subset GL(2, \mathbb{R})$$

примітивна як підгрупа групи $GL(2, \mathbb{R})$, але імпримітивна як підгрупа групи $GL(2, \mathbb{C})$.

Вправа 25. Знайти порядки елементів

а) $\begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix} \in GL(2,7)$; **б)** $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in GL(2,5)$.

Вправа 26. Показати спряженість елементів

а) $a = \begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$ і $b = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$

в групі $GL(2,\mathbb{Q})$;

$$\textbf{б)}\ a=\begin{pmatrix}1&2\\3&1\end{pmatrix}\ \text{ і }\ b=\begin{pmatrix}0&-2\\1&2\end{pmatrix}$$

в групі $GL(2,7)$.

Вправа 27. Нехай $f(t)$ — примітивний многочлен над полем T:

$$f(t)=t^n-\alpha_{n-1}t^{n-1}-\cdots-\alpha_1 t-\alpha_0\quad(\alpha_j\in T).$$

Супровідна матриця $\widetilde{f}$ многочлена $f(t)$ це матриця порядку n вигляду:

$$\widetilde{f}=\begin{pmatrix}0&0&\dots&0&\alpha_0\\1&0&\dots&0&\alpha_1\\0&1&\dots&0&\alpha_2\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\dots&1&\alpha_{n-1}\end{pmatrix}.$$

Показати, що будь-яка циклічна підгрупа G групи $GL(n,T)$ спряжена з підгрупою $\left\langle\widetilde{f}\right\rangle$, де $f(t)$ — многочлен, вільний член α_0 якого відмінний від нуля. Довести, що група G є незвідна тоді і тільки тоді, коли мночлен $f(t)$ є незвідний над полем T.

Вправа 28. Нехай

$$G_1=\left\langle a=\begin{pmatrix}0&0&1\\1&0&0\\0&1&1\end{pmatrix}\right\rangle,\quad G_2=\left\langle b=\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}\right\rangle$$

— дві циклічні підгрупи групи $GL(3,2)$. Показати, що вони незвідні і спряжені.

Вправа 29. Многочлен

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

називається *поліномом поділу круга* на n частин. Степінь цього многочлена рівна $\varphi(n)$, де φ — функція Ейлера. Многочлен $\Phi_n(x)$ незвідний над полем $\mathbb{Q}$. Коренями многочлена $\Phi_n(x)$ є первісні корені степеня n із одиниці.

а) Знайти

$$\Phi_{p^k}(x)\quad(p\text{ — просте число});\ \Phi_{10}(x);\ \Phi_{15}(x);\ \Phi_{20}(x).$$

б) Знайти всі скінченні незвідні циклічні підгрупи групи $GL(n,\mathbb{Q})$ для всіх $n\leqslant 10$.

Вправа 30. Нехай G — скінченна незвідна абелева p-підгрупа групи $GL(n,\mathbb{Q})$. Довести, що група G буде примітивною тоді і тільки тоді, коли $|G|=p$ і $n=p-1$.

РОЗДІЛ 2. СИЛОВСЬКІ ПІДГРУПИ ПОВНОЇ ЛІНІЙНОЇ ГРУПИ НАД ПОЛЕМ

§10. Силовські p-підгрупи симетричної групи

Введемо конструкцію сплетіння групи підстановок з ще однією групою підстановок. Нехай A — підгрупа групи S_n підстановок на n символах $\{1,\ 2,\ \ldots,\ n\}$ і $C_p = \langle\sigma = (1,\ 2,\ \ldots,\ p)\rangle$ — циклічна порядку p група підстановок степеня p, породжена циклом σ. Визначимо сплетіння $A \wr C_p$ групи A з групою C_p. Перш за все відмітимо, що це є підгрупа групи S_{pn} підстановок на pn символах. Нехай

$$U_i = \{(i-1)n + j | j = 1,\ 2,\ \ldots,\ n\} \quad (i = 1,\ \ldots,\ p),$$

$$U = U_1 \cup \cdots \cup U_p = \{1,\ 2,\ \ldots,\ np\}$$

і прямий добуток $A^p = A \times \cdots \times A$ діє в множині U, переставляючи символи лише в підмножинах U_i $(i = 1,\ \ldots,\ p)$, а саме, якщо

$$a = (a_1,\ \ldots,\ a_p),\ a_i \in A,\ u = (i-1)n + j \in U_i, \tag{1}$$

то

$$a(u) = (i-1)n + a_i(j) \quad (i = 1,\ \ldots,\ p;\ \ j = 1,\ 2,\ \ldots,\ n). \tag{2}$$

Тоді A^p буде підгрупою групи підстановок S_{pn} на множині U із pn елементів. Цикл σ визначає підстановку $\widetilde{\sigma}$ на U, яка переставляє підмножини $U_1, \ldots, U_p$:

$$\widetilde{\sigma}((i-1)n + j) = (\sigma(i) - 1)n + j \quad (i = 1,\ \ldots,\ p;\ \ j = 1,\ 2,\ \ldots,\ n).$$

Тоді *сплетіння*

$$A \wr C_p = \langle A^p, \widetilde{\sigma}\rangle$$

це підгрупа в S_{pn}, що породжується групою A^p і підстановкою $\widetilde{\sigma}$. Покажемо, що A^p — нормальна підгрупа в $A \wr C_p$. Дійсно, нехай $a' = (a_2,\ \ldots,\ a_p,\ a_1)$ (див. (1)). Якщо $i < p$, то

$$a\widetilde{\sigma}((i-1)n + j) = a(\sigma(i) - 1)n + j) = a(in + j) = in + a_{i+1}(j),$$

$$\widetilde{\sigma}a'((i-1)n + j) = \widetilde{\sigma}((i-1)n + a_{i+1}(j)) = (\sigma(i) - 1)n + a_{i+1}(j) = in + a_{i+1}(j).$$

Крім того,

$$a\widetilde{\sigma}((p-1)n + j) = a(\sigma(p) - 1)n + j) = a(j) = a_1(j),$$

$$\widetilde{\sigma}a'((p-1)n + j) = \widetilde{\sigma}((p-1)n + a_1(j)) = (\sigma(p) - 1)n + a_1(j) = a_1(j).$$

Отже, $a\widetilde{\sigma} = \widetilde{\sigma}a'$ і $\widetilde{\sigma}^{-1}a\widetilde{\sigma} = a'$. Тоді A^p — нормальна підгрупа в групі $A \wr C_p$. Відмітимо, що $|A \wr C_p| = |A|^p p$ і група $A \wr C_p$ є напівпрямий добуток підгрупи $\langle\widetilde{\sigma}\rangle$ і нормальної підгрупи A^p.

Для простого числа p визначимо функцію натурального аргументу

$$M(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots,$$

де $[a]$ — ціла частина числа a. Неважко бачити, що

$$M(p^s) = 1 + p + \cdots + p^{s-1} = \frac{p^s - 1}{p - 1}.$$

Лема 10.1. *Нехай* $0 \leqslant r < p, p^s > n$. *Тоді*

$$M(n + rp^s) = M(n) + rM(p^s).$$

Доведення. Оскільки $n + rp^s < p^s + rp^s = (r+1)p^s \leqslant p^{s+1}$, то

$$\left[\frac{n+rp^s}{p^j}\right] = \left[\frac{n}{p^j}\right] = 0 \text{ при } j > s.$$

Крім того,

$$\left[\frac{n+rp^s}{p^j}\right] = \left[\frac{n}{p^j}\right] + rp^{s-j} \text{ при } j \leqslant s.$$

Лема 10.2. *Порядок силовської p-підгрупи P групи S_n дорівнює $p^{M(n)}$.*

Доведення. Знайдемо кількість t множників p в порядку $n!$ групи S_n. Тоді $|P| = p^t$. Якщо x — кратний p множник в $n!$, то $x = pa$, де $a \leqslant [\frac{n}{p}]$. Виберемо з кожного множника x по одному p. В результаті ми одержимо $[\frac{n}{p}]$ множників p і число $[\frac{n}{p}]$ увійде доданком в t. Серед чисел $\frac{n}{p}$ можуть бути числа кратні p — це числа для $x = p^2a$, де $a \leqslant [\frac{n}{p^2}]$. Відберемо з кожного такого $\frac{x}{p}$ по одноме множнику p. В результаті ми одержали ще $\frac{n}{p^2}$ множників p і число $\frac{n}{p^2}$ увійде наступним доданком в t. Серед чисел $\frac{x}{p^2}$ шукаємо числа кратні p і т. д. Нарешті одержимо $t = M(n)$.

Лема 10.3. *Нехай*

$$P_0 = C_1, P_1 = C_p, P_j = P_{j-1} \wr C_p \quad (j > 1).$$

Група P_j буде силовською p-підгрупою групи S_{p^j} $(j = 0, 1, \ldots)$.

Доведення. Силовська p-підгрупа групи S_p буде циклічною групою C_p порядку p. Далі

$$|P_{j-1} \wr C_p| = p|P_{j-1}|^p = p(p|P_{j-2}|^p)^p = p^{\frac{p^2-1}{p-1}}|P_{j-2}|^{p^2} = \ldots = p^{M(p^j)} = |P_j|.$$

Звідси, а також в силу того, що $P_{j-1} \wr C_p$ — підгрупа в S_{p^j}, випливає, що $P_j = P_{j-1} \wr C_p$. Лема доведена.

Теорема 10.1. *Нехай*

$$n = n_0 + n_1 p + \cdots + n_s p^s$$

— p-ічний розклад натурального числа n $(0 \leqslant n_j < p,\ n_s \neq 0)$. Нехай P — силовська p-підгрупа симетричної групи S_n на n символах. Тоді

$$P = P_0^{n_0} \times P_1^{n_1} \times \cdots \times P_s^{n_s}. \tag{3}$$

Доведення. (Відмітимо, що A^r це прямий добуток r екземплярів групи A). Представимо множину U із n символів у вигляді об'єднання неперетинаючих підмножин із n_0 символів, n_1 множин по p символів і т. д., n_s множин по p^s символів. Тоді прямий добуток $S_1^{n_0} \times S_p^{n_1} \times \cdots \times S_{p^s}^{n_s}$ груп підстановок на цих підмножинах буде підгрупою в групі S_n. Права частина в (3) є p-підгрупа в цьому добутку. Із лем 10.1–10.3 випливає, що порядки груп в лівій і правій частинах рівності (3) є однакові. Це закінчує доведення теореми.

Наслідок 10.1. *Якщо група S_n містить транзитивну p-підгрупу, то $n = p^s$.*

§11. Відомості з теорії зображень груп

Нехай T — поле, $\overline{T}$ — алгебраїчне замикання поля T, G — скінченна група, H — підгрупа групи G і $\{g_1, \ldots, g_n\}$ — система представників всіх лівих суміжних класів групи G за підгрупою H. *Лінійним характером* групи H називається гомоморфізм $\chi : H \to \overline{T}^*$ групи H в мультиплікативну групу $\overline{T}^*$ поля $\overline{T}$. Лінійний характер — це зображення степеня один. Нехай $\Gamma = \chi^G$ — $\overline{T}$-зображення групи G, що індукується лінійним характером χ підгрупи H. Тоді

$$\Gamma(g) = (\dot{\chi}(g_j^{-1} g g_i)) \quad (g \in G)),$$

де $\dot{\chi} : G \to T$ така функція, що

$$\dot{\chi}(g) = \begin{cases} 0, & g \notin H, \\ \chi(g), & g \in H. \end{cases}$$

Нехай $M = \overline{T}e$ — $\overline{T}H$-модуль зображення χ:

$$he = \chi(h)e \quad (h \in H).$$

Тоді індукований $\overline{T}G$-модуль $L = M^G$ зображення Γ має $\overline{T}$-базис

$$e_1 = g_1 \otimes e, \ \ldots, \ e_n = g_n \otimes e$$

і для довільного g з групи G

$$ge_i = \chi(g_j^{-1} g g_i) e_j,$$

де для кожного i $(1 \leqslant i \leqslant n)$ індекс j $(1 \leqslant j \leqslant n)$ є єдиним таким, що $g_j^{-1} g g_i \in H$.

Теорема 11.1 (Хупперта, Бермана). *Нехай порядок скінченної розв'язної групи G не ділиться на характеристику поля T і в групі G існує така нормальна підгрупа G_0, що фактор-група G/G_0 є надрозв'язна і всі силовські підгрупи групи G_0 є абелеві. Якщо Γ — незвідне зображення групи G над полем $\overline{T}$, то існує така підгрупа H групи G і такий лінійний характер $\chi : H \to \overline{T}^*$, що зображення Γ еквівалентно індукованому зображенню χ^G.*

Опишемо алгоритм Бермана знаходження незвідних зображень групи G над полем $\overline{T}$ для групи G, яка задовольняє умовам теореми 11.1. Цим алгоритмом описуються пари (χ, H), де H — така підгрупа в G і χ — такий лінійний характер цієї підгрупи, що індуковане зображення χ^G групи G є незвідним над полем $\overline{T}$. Введемо попередньо поняття *нормалізатора* в групі G лінійного характера χ довільної підгрупи H:

$$N_G(\chi) = \{g \in G \mid g^{-1} H g = H, \ \chi(g^{-1} h g) = \chi(h) \ (h \in H)\}.$$

Нехай

$$1 \subset G_1 \subset \ldots \subset G_j \subset \ldots \subset G_s = G$$

— головний ряд групи G, що проходить через підгрупу G_0. На першому кроці алгоритму знаходимо множину M_1 всіх пар (χ, H), де $H = G_1$, χ пробігає всі лінійні характери абелевої групи G_1 (в цьому випадку нормалізатор $N_{G_1}(\chi) = G_1$ для лінійного характеру χ довільної підгрупи $H \subset G_1$). Нехай на j-му кроці знайдена множина M_j всіх пар (χ, H) таких, що H — підгрупа в групі G_j, χ — такий лінійний характер підгрупи H, що $N_{G_j}(\chi) = H$. Опишемо $(j+1)$-ий крок. Нехай $(\chi, H) \in M_j$. Знаходимо нормалізатор $N = N_{Gj+1}(\chi)$ характера χ в члені G_{j+1} головного ряду групи G. Якщо $N = H$, то пару (χ, H) відправляємо в множину M_{j+1}. Нехай $(N : H) = m > 1$. Тоді характер χ групи H має m різних продовжень $\chi_1, \ldots, \chi_m : N \to \overline{T}^*$ до лінійних

характерів групи N. Всі пари (χ_j, N) $(j = 1, \ldots, m)$ відправляємо в множину M_{j+1}. Переходимо до наступної пари $(\chi, H) \in M_j$ і т. д. На останьому кроці одержимо множину M_s всіх потрібних пар.

Нехай далі G — довільна скінченна група, характеристика поля T рівна нулю і Γ — незвідне зображення групи G над полем $\overline{T}$. Розширення T' поля T називається *полем розкладу* відносно T зображення Γ, якщо це зображення еквівалентно зображенню матрицями над полем T'. Згідно теореми Брауера [11], поле $T(\varepsilon)$ (ε — первісний корінь степеня $|G|$ із одиниці) є полем розкладу будь-якого незвідного $\overline{T}$-зображення групи G і можна далі обмежитись полями розкладу, які містяться в полі $T(\varepsilon)$. Поле $T(\varepsilon)$ є нормальне розширення поля T з абелевою групою Галуа і будь-яке підполе в цьому полі буде також нормальним розширенням поля T. Поле T' містить поле $T_1 = T(\chi)$ характера χ зображення Γ. Нехай K — таке поле розкладу зображення Γ, що степінь $(K : T)$ є найменша. Нехай в полі K вибрано який-небудь T-базис і нехай

$$\varrho_{K/T} : K \to M(s, T) \quad (s = (K : T))$$

— зображення поля K, що ставить у відповідність кожному елементу α поля K матрицю $\varrho_{K/T}(\alpha)$ оператора

$$\hat{\alpha} : K \to K \quad \hat{\alpha}(x) = \alpha x \quad (x \in K)$$

множення на α у вибраному T-базисі поля K. Будемо далі вважати, що Γ уже є зображенням над полем K. Нехай $\Delta = \varrho_{K/T}(\Gamma)$ — зображення групи G над полем T, що отримується із K-зображення Γ заміною кожного матричного елемента $\alpha \in K$ на матрицю $\varrho_{K/T}(\alpha)$. Нехай $\sigma_1, \ldots, \sigma_k$ — система представників всіх суміжних класів групи Галуа $G(K, T)$ поля K над полем T за її підгрупою $G(K, T_1)$. Відмітимо, що $k = (T_1 : T)$. Нехай $\sigma = \sigma_j$. Позначимо через Γ^σзображення групи G над полем K, що отримується із зображення Γ заміною всіх матричних елементів α на $\sigma(\alpha)$.

Твердження 11.1. *Зображення $\Gamma^{\sigma_1}, \ldots, \Gamma^{\sigma_k}$ групи G є незвідні і попарно неекквівалентні над полем K.*

Доведення. Автоморфізми $\sigma_1, \ldots, \sigma_k$ визначають всі попарно різні автоморфізми поля T_1 над полем T. Тоді характери вказаних зображень будуть попарно різні (якщо $\sigma(\chi) = \chi$, то $\sigma \in G(K, T_1)$). Це доводить твердження.

Твердження 11.2. *Зображення Δ групи G є незвідне над полем T. Має місце розклад*

$$\Delta = (K : T_1)(\Gamma^{\sigma_1} + \cdots + \Gamma^{\sigma_k})$$

T-зображення Δ групи G в суму незвідних зображень цієї групи G над полем K.

$$T \subset T_1 \subset K.$$

Доведення цього твердженнь опирається на декілька лем. Введемо в розгляд алгебри — лінійні оболонки K-зображення Γ над полями T, T_1, K відповідно:

$$A = [\Gamma]_T = [\Gamma(G)]_T, \ A_1 = [\Gamma]_{T_1}, \ A_2 = [\Gamma]_K.$$

Всі три алгебри будуть простими алгебрами, а алгебра A_2 буде ізоморфна алгебрі $M(n, K)$ (n — степінь зображення Γ).

Лема 11.1. *Центр $\mathfrak{Z}(A)$ алгебри A як лінійний простір над полем T породжується матрицями*

$$\mathrm{diag}[\chi(g), \ \ldots, \ \chi(g)] \ (g \in G).$$

Окрім цього, $\mathfrak{Z}(A) \cong T_1$. Алгебра A_1 є центральною алгеброю[2] над основним полем T_1. Якщо ототожнити $\mathfrak{Z}(A) = T_1$, то кільця A і A_1 сумістяться.

[2] *Центральна* алгебра над полем T — алгебра з одиницею над полем T, центр якої суміщається з основним полем T.

Доведення. Центри обох алгебр породжуються всіма матрицями вигляду $\Gamma(c)$, де c сума елементів класа C спряжених елементів групи G. Нехай матриця S належить центру алгебри A або алгебри A_1. Тоді

$$S\Gamma(g) = \Gamma(g)S \ (g \in G).$$

Так як Γ — абсолютно незвідне зображення, то матриця S буде скалярною матрицею. Отже, $\Gamma(c) = \mathrm{diag}[\lambda, \ldots, \lambda]$. Взявши сліди матриць, одержимо

$$\lambda = \frac{h\chi(a)}{n} \quad (h = |C|, a \in C).$$

Звідси випливає доведення леми.

Лема 11.2. *Нехай Γ_1 буде те T_1-зображення групи G, модуль якого суміщається з мінімальним лівим ідеалом U алгебри A_1. Тоді*

$$\Gamma_1 = (K : T_1)\Gamma,$$

тобто над полем K зображення Γ_1 є сума $(K : T_1)$ зображень Γ.

Доведення. Нехай D — центральне тіло над полем T_1 таке, що

$$A_1 = M(t, D), \ (D : T_1) = r^2.$$

Тоді степінь зображення Γ_1 дорівнює r^2t. Тензорний добуток $K \otimes_{T_1} A_1$ можна ототожнити з алгеброю A_2. Тоді $n^2 = r^2t^2$ і поле K розщеплює тіло D. Тоді, в силу вибору поля K, це поле буде максимальним підполем в тілі D. Отже, $r = (K : T_1)$. Тоді степінь зображення Γ_1 рівий $(K : T_1)n$. Так як KG-модуль $K \otimes_{T_1} U$ є сума мінімальних ідеалів алгебри A_2 і розмірності над K цих ідеалів рівні n, то $\Gamma_1 = (K : T_1)\Gamma$. Лема доведена.

Нехай V — T-зображення групи G, модуль якого суміщається з мінімальним лівим ідеалом алгебри A. Легко бачити, що

$$V = \varrho_{T_1/T}(\Gamma_1).$$

Всі матриці $\varrho_{T_1/T}(\alpha)$ $(\alpha \in T_1)$ одночасно подібні над полем T_1 діагональним матрицям

$$\mathrm{diag}[\sigma_1(\alpha), \ \ldots, \ \sigma_k(\alpha)].$$

Тоді над полем T_1 зображення V буде мати вигляд

$$V = \Gamma_1^{\sigma_1} + \cdots + \Gamma_1^{\sigma_k}.$$

Із леми 10.2 випливає, що

$$V = (K : T_1)(\Gamma^{\sigma_1} + \cdots + \Gamma^{\sigma_k}).$$

Незвідне T-зображення V і T-зображення $\varrho_{K/T}(\Gamma)$ мають однакові степені і містять Γ в розкладах над полем K. Це значить, що ці зображення є еквівалентні, що доводить твердження 11.2. До речі, над полем K

$$\varrho_{K/T}(\Gamma) = \bigoplus_{\sigma \in G(K,T)} \Gamma^{\sigma}.$$

§12. Силовські p-підгрупи групи $GL(n,T)$. Загальні властивості

В цьому параграфі будуть розглянуті деякі властивості силовських p-підгруп групи $GL(n,T)$ над довільним полем T.

Якщо $\operatorname{char} T = p$, то всі силовські p-підгрупи групи $GL(n,T)$ спряжені з унітрикутною групою $UT(n,T)$ над полем T (теорема 7.2).

Далі в цьому параграфі будемо вважати, що $\operatorname{char} T \neq p$.

Лема 12.1. *Нехай G — p-підгрупа групи $GL(n,T)$. Тоді*
1) *G — локально скінченна і локально нільпотентна група;*
2) *G — цілком звідна група;*
3) *G — розв'язна група.*

Доведення. 1) випливає із теореми Шура, 2) — із теореми Платонова, 3) випливає з теореми Цассенхауза.

Лема 12.2. *Нехай G — незвідна силовська p-підгрупа групи $GL(n,T)$. Тоді або група G примітивна, або $n = dp^r (r > 0)$ і в групі $GL(d,T)$ існує така примітивна силовська p-підгрупа H, що група G буде спряжена зі сплетінням $H \wr P_r$ матричної групи H і силовської p-підгрупи P_r симетричної групи S_{p^r}.*

Доведення. Нехай G — імпримітивна група. Тоді вона спряжена з підгрупою деякого сплетіння $H \wr A$ матричної групи $H \subset GL(d,T)$, де d ділить n з деякою групою A підстановок на $\frac{n}{d}$ символах. Так як G — p-група, то H і A — p-групи. Так як G — незвідна група, то A — транзитивна група і тоді $\frac{n}{d} = p^r$ (див. наслідок 10.1). Нарешті, групи H і A — силовські p-підгрупи в своїх групах (інакше G не силовська підгрупа). Лема доведена.

Лема 12.3. *Нехай G — примітивна p-підгрупа групи $GL(n,T)$. Тоді мають місце такі властивості, пов'язані з рядом Супруненка[3] групи G :*
1) *група F є p-підгрупою мультиплікативної групи K^* поля K;*
2) *поле K одержується приєднанням до поля T кореня степеня p^s із одиниці для деякого $s \geq 0$;*
3) *$V = F$;*
4) *група G/F діє в полі K автоморфізмами поля K над полем F.*

Доведення. Нехай $V \neq F$. За теоремою Супруненка група V/F скінченна. Тоді скінченна p-група V/F має неодиничний центр $Z = \mathfrak{Z}(V/F)$ і неодиничний *нижній шар* $N = N(Z)$ (це підгрупа породжена елементами порядку p) цього центру. Групи Z, N — залишається незмінною при дії довільного автоморфізма групи G/F, зокрема, Z, N — нормальна підгрупа групи G/F. Крім того, група G/F діє спряженням в елементарній абелевій групі[4] N, яку, в свою чергу, можна розглядувати як скінченно вимірний лінійний простір над полем $\mathbb{Z}_p$ із p елементів. Тоді в просторі N існує ненульовий вектор cF (c — деякий елемент із G) такий, що

$$g^{-1}(cF)g = cF \ (g \in G).$$

Звідси випливає, що група $\langle F, c\rangle$ є абелевою нормальною підгрупою в групі G і ця підгрупа строго містить F, що суперечить вибору групи F. Отже, $V = F$. Властивості 1)–4) тепер слідують із результатів про примітивні роз'язні групи.

---

[3] *Ряд Супруненка* примітивної розв'язної групи $G : F \subset A \subset V \subset G$ (F — максимальна нормальна абелева підгрупа групи G, $V = \mathfrak{Z}_G(F)$ — централізатор підгрупи F в групі G, A — така максимальна нормальна підгрупа в групі G, яка міститься в групі V і фактор-група A/F є абелевою групою.)

[4] *Елементарна абелева* група — абелева група, всі неодиничні елементи якої мають один і той же простий порядок.

Лема 12.4. *Нехай H — незвідна силовська p-підгрупа групи $GL(n,T)$ і $A=\langle\sigma\rangle$ — група підстановок, породжена циклом $\sigma=(1,\,2,\,\ldots,\,p)$. Тоді сплетіння $W(H)=H\wr A$ майже завжди буде незвідною силовською p-підгрупою групи $GL(pn,T)$. Виключення складає лише випадок, коли одночасно виконуються умови:*

1) $p=2$,
2) $n=1$,
3) $|H|=2$,
4) *поле T містить $\sqrt{2}$ або $\sqrt{-2}$.*

Доведення. Група $W=W(H)$ породжується нормальною підгрупою $A=H^p=H\times\cdots\times H$ і матрицею $b=\tilde{\sigma}$ підстановки σ (над кільцем $M(n,T)$). Відображення $\Delta: A\to GL(n,T)$, таке, що

$$\Delta(\mathrm{diag}[a_1,\ a_2,\ \ldots,\ a_p])=a_1\quad(a_i\in H)$$

є зображенням групи A над полем T. Так як $H=\Delta(A)$ — незвідна група, то зображення Δ також незвідне. Визначимо

$$\Delta^i(a)=\Delta(b^{-i}ab^i)\ (a\in A;\ i=0,\ 1,\ \ldots,\ p-1).$$

Тоді $\Delta^0=\Delta$, Δ^1, $\ldots$, Δ^{p-1} — незвідні T-зображення групи A, вони попарно нееквівілентні (в них різні ядра), але попарно спряжені відносно групи W, яка транзитивно їх переставляє. Із цих властивостей випливає, що індуковане зображення Δ^W групи W буде незвідним, а так як $W=\Delta^W(W)$, то W — незвідна група.

Покажемо, що W буде силовською p-підгрупою групи $GL(np,T)$. Нехай в цій групі існує така матриця

$$X=(x_{ij})\quad(x_{ij}\in M(n,T)),$$

що

$$X^p\in W,\ X^{-1}WX=W.$$

Досить показати, що $X\in W$.

Для цього розглянемо перші два члени $Z_1(W)$, $Z_2(W)$ верхнього центрального ряду групи W ($Z_1(W)=\mathfrak{Z}(W)$, $Z_2(W)/Z_1(W)=\mathfrak{Z}(W/Z_1(W))$). Очевидно, що

$$Z_1(W)=\{\mathrm{diag}[\alpha,\ \ldots,\ \alpha]|\alpha\in\mathfrak{Z}(H)\}.$$

Покажемо, що

$$Z_2(W)=\left\langle Z_1(W),\mathrm{diag}[1,\ \alpha,\ \ldots,\ \alpha^{p-1}]|(\alpha\in\mathfrak{Z}(H),\ \alpha^p=1)\right\rangle.$$

Якщо $\alpha\in\mathfrak{Z}(H)$ і $\alpha^p=1$, то

$$\mathrm{diag}[1,\ \alpha,\ \ldots,\ \alpha^{p-1}]\in Z_2(W).$$

Нехай

$$a=\mathrm{diag}[\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_p]\quad(\alpha_i\in H)$$

— елемент із $Z_2(W)$. Тоді для кожного $x\in W$ знайдеться $z\in Z_1(W)$ так, що $x^{-1}ax=az$. Нехай

$$x=\mathrm{diag}[x_1,\ x_2,\ \ldots,\ x_p]\quad(x_i\in H).$$

Тоді

$$x_i^{-1}\alpha_i x_i=\alpha_i\gamma\quad(\gamma\in\mathfrak{Z}(H)).$$

Нехай деяке α_j не міститься в $\mathfrak{Z}(H)$ і x_j такий елемент із H, що $x_j\alpha_j\neq\alpha_jx_j$. Візьмемо $x_i=1(i\neq j)$. Одержимо $\gamma=1$ і неможливе $x_j\alpha_j=\alpha_jx_j$. Отже, $\alpha_i\in\mathfrak{Z}(H)$ ($i=1,\ \ldots,\ p$). Тепер із умови $[a,b]\in Z_1(W)$ легко одержати

$$\alpha_i=\gamma^{i-1}\alpha_1\quad(\gamma\in\mathfrak{Z}(H),\gamma^p=1).$$

Ми встановили, які елементи групи A належать групі $Z_2(W)$. Покажемо, що інших елементів в $Z_2(W)$ нема. Нехай це не так і

$$\operatorname{diag}[\beta_1,\ \beta_2,\ \ldots,\ \beta_p]b \in Z_2(W)\ (\beta_i \in H).$$

Тоді для будь-яких елементів $x_i \in H$ $(i = 1,\ \ldots,\ p)$ знайдеться елемент $\delta \in \mathfrak{Z}(H)$ такий, що

$$\operatorname{diag}[x_1^{-1}\beta_1,\ \ldots,\ x_p^{-1}\beta_p]\ \operatorname{diag}[x_p,\ x_1,\ \ldots,\ x_{p-1}] = \operatorname{diag}[\beta_1\delta,\ \ldots,\ \beta_p\delta].$$

Якщо H — неабелева група, то, взявши $x_1 = 1$, $x_p \in H \setminus \mathfrak{Z}(H)$, одержимо протиріччя з рівністю

$$x_1^{-1}\beta_1 x_p = \beta_1\delta.$$

Нехай H — абелева група. Тоді

$$x_i = x_p\delta^{p-i} \quad (i = 1,\ \ldots,\ p-1)$$

і $\delta^p = 1$. Якщо $p > 2$, то одержимо протиріччя, взявши $x_p = x_{p-1} = 1$ і $x_{p-2} \neq 1$. Нехай $p = 2$, але $|H| > 2$. Тоді в групі H існує елемент γ, порядок якого більший ніж 2. Якщо взяти $x_2 = 1$, $x_1 = \gamma$, то одержиться протиріччя з рівністю $x_1 = x_2\delta$. Отже, у всіх випадках (за виключенням: $p = 2$, $|H| = 2$) група $Z_2(W)$ міститься в A. Якщо $p = 2$ і $|H| = 2$, то W — група діедра порядку 8 і $Z_2(W) = W$.

Перейдемо до розгляду матриці X. Перш за все відмітимо, що

$$X^{-1}Z_i(W)X = Z_i(W)\ (i \geq 1).$$

Нехай $\alpha \in \mathfrak{Z}(H)$ і $\alpha^p = 1$. Так як $\mathfrak{Z}(H)$ — циклічна група, то в ній існує тільки одна підгрупа порядку p, це група $\langle\alpha\rangle$. Тоді в $Z_1(W)$ також одна підгрупа порядку p, це група $\langle\alpha E\rangle$. Тоді в групі $Z_2(W)$ існує лише одна абелева типу (p,p) підгрупа, це група

$$\left\langle \alpha E, \operatorname{diag}[1, \alpha, \ldots, \alpha^{p-1}] \right\rangle.$$

Так як X — p-елемент і група $\langle\alpha\rangle$ не має автоморфізму порядку p, то $(\alpha E)X = X(\alpha E)$ і, отже, $\alpha x_{ij} = x_{ij}\alpha$. Існує $\beta \in \mathfrak{Z}(H)$, що

$$\operatorname{diag}[1, \alpha, \ldots, \alpha^{p-1}]X = X\operatorname{diag}[\beta, \alpha^t\beta, \ldots, \alpha^{t(p-1)}\beta]$$

для деякого $1 \leqslant t < p$. Звідси

$$\alpha^{i-1}x_{ij} = x_{ij}\alpha^{t(j-1)}\beta \quad (1 \leqslant i, j \leqslant p).$$

Для кожного індекса i $(i = 1,\ \ldots,\ p)$ існує тільки один індекс $j = j'$ $(1 \leqslant j' \leqslant p)$, такий, що

$$\alpha^{i-1} = \alpha^{t(j'-1)}\delta$$

(це слідує із того, що α, β — елементи порядку p в $\mathfrak{Z}(H)$). Для всіх інших j $(j = 1,\ \ldots,\ p; j \neq j')$ будемо мати $x_{ij} = 0$. Отже, існує підстановка ρ на p символах така, що

$$X = \operatorname{diag}[x_{1\rho(1)}, \ldots, x_{p\rho(p)}]\tilde{\rho}.$$

Розглянемо p-групу $W_1 = \langle W, X\rangle$. Це мономіальна група над кільцем $M(n,T)$. Кожний елемент групи W_1 представляється у вигляді добутку діагональної матриці на матрицю підстановки. Поставивши у відповідність елементам групи W_1 ці підстановки, одержимо деякий гомоморфізм $f : W_1 \to S_p$. p-підгрупа $f(W_1) \subset S_p$ містить підстановки σ, ρ, причому σ — елемент порядку p. Але в групі S_p існує лише одна

p-підгрупа, що містить підстановку σ. Отже, $f(W_1) = \langle\sigma\rangle$ і тоді $\rho = \sigma^r$ для деякого r. Таким чином, $\tilde{\rho} \in W$ і група W містить

$$X\tilde{\rho}^{-1} = \mathrm{diag}[x_1, \ldots, x_p](x_i = x_{i\rho(i)}).$$

Легко бачити, що x_i — p-елемент в групі $GL(n,T)$ і $\langle H, x_i\rangle$ — p-підгрупа в цій групі. Але H — силовська підгрупа в $GL(n,T)$. Це значить, що $x_i \in H$ і тоді $X \in W$, що й треба було показати. Доведення обґрунтовувалося на будові групи $Z_2(W)$. Випадок $p = 2, |H| = 2$ потрібно розглянути окремо. В цьому випадку $H = \{1, -1\}, n = 1$ і

$$W = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

Нехай поле T містить елемент $\gamma = \sqrt{\pm 2}$. Тоді матриця

$$V = \gamma^{-1} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

буде 2-елементом в групі $GL(2,T)$ і група $\langle W, V\rangle$ буде 2-підгрупою в $GL(2,T)$. Лема доведена.

§13. Деякі леми

Нехай p — просте число, T — поле, характеристика якого відмінна від p.

Лема 13.1. *Нехай G — скінченна p-група, що містить циклічну нормальну підгрупу $H = \langle a\rangle$ порядку p^n, яка суміщається зі своїм централізатором в цій групі. Тоді G одна із груп:*

$$G = H;$$

$$G_p = \left\langle a,\ b \mid a^{p^n} = b^{p^k} = 1,\ b^{-1}ab = a^{1+p^{n-k}} \right\rangle \quad (p \neq 2,\ 0 < k < n);$$

$$G_{21} = \left\langle a,\ b \mid a^{2^n} = b^{2^k} = 1,\ b^{-1}ab = a^{1+2^{n-k}} \right\rangle \quad (n > 2,\ 0 < k < n-1);$$

$$G_{22} = \left\langle a,\ b \mid a^{2^n} = b^{2^k} = 1,\ b^{-1}ab = a^{-1+2^{n-k}} \right\rangle \quad (n > 2,\ 1 < k < n-1);$$

$$G_{23} = \left\langle a,\ b,\ c \mid a^{2^n} = b^{2^k} = 1,\ c^2 = a^{j2^{n-1}},\ b^{-1}ab = a^{1+2^{n-k}},\ c^{-1}ac = a^{-1},\ bc = cb \right\rangle$$

$$(n > 2,\ j = 0, 1,\ k < n-1);$$

$$D_{2^n} = \left\langle a,\ b \mid a^{2^n} = b^2 = 1,\ b^{-1}ab = a^{-1} \right\rangle;$$

$$Q_{2^{n+1}} = \left\langle a,\ b \mid a^{2^n} = 1,\ b^2 = a^{2^{n-1}},\ b^{-1}ab = a^{-1} \right\rangle;$$

$$QD_{2^n} = \left\langle a,\ b \mid a^{2^n} = b^2 = 1,\ b^{-1}ab = a^{-1+2^{n-1}} \right\rangle.$$

В усіх випадках група G є розширення підгрупи H з допомогою деякої p-підгрупи групи автоморфізмів групи H.

Будемо далі вживати позначення ξ_n для первісного кореня степеня p^n із одиниці при $p \neq 2$ і для кореня степеня 2^n із мінус одиниці при $p = 2$. Ці корені будемо вибирати так, щоб $\xi_{s+1}^p = \xi_s$ $(s \geq 1)$.

Лема 13.2 (Лема Бермана). *Або для всіх $i = 1, 2, \ldots$ виконується рівність $T(\xi_i) = T(\xi_1)$, або існує таке натуральне n, що $T(\xi_n) = T(\xi_1)$ і $(T(\xi_r) : T(\xi_1)) = p^{r-n}$, якщо $r > n$.*

Доведення. Нехай $K = T(\xi_n)(n \geq 1)$ і ξ_{n+1} не міститься в K. Покажемо, що тоді ξ_{n+2} не міститься в $K(\xi_{n+1})$. Припустимо, що це не так і $\xi_{n+2} \in K(\xi_{n+1})$. Нехай φ — такий автоморфізм поля $K(\xi_{n+1})$ над полем K, що

$$\varphi(\xi_{n+1}) = \varepsilon\xi_{n+1}, \quad (\varepsilon^p = 1,\ \varepsilon \neq 1).$$

Очевидно, $\varphi^p = 1$. Так як ξ_{n+1} — корінь многочлена $x^{p^2} - \xi_n$ над полем K, то

$$\varphi(\xi_{n+2}) = \zeta\xi_{n+2},$$

ζ — корінь степеня p^2 із одиниці. Нехай $\varphi(\zeta) = \zeta$. Тоді

$$\varepsilon\xi_{n+1} = \varphi(\xi_{n+2}^p) = \zeta^p\xi_{n+1},$$

$$\xi_{n+2} = \varphi^p(\xi_{n+2}) = \zeta^p\xi_{n+2},$$

що дає протиріччя. Нехай

$$\varphi(\zeta) = \varepsilon^s\zeta.$$

Тоді $p \neq 2$ і $n = 1$. Маємо

$$\varphi^p(\xi_3) = \varepsilon^{st}\zeta^p\xi_3, \quad t = \frac{p-1}{2}p,$$

тобто і в цьому випадку одержимо протиріччя. Ми показали, що ξ_{n+2} не міститься в $T(\xi_{n+1})$, якщо ξ_{n+1} не міститься в $T(\xi_n)$. Звідси легко одержати доведення леми.

Наслідок 13.1. *Нехай* $(T(\xi_n) : T(\xi_1)) = p^s$. *Тоді* $T(\xi_1) = T(\xi_n^{p^s})$.

§14. Примітивні зображення деяких p-груп

Нехай G — p-група, T — поле, $\operatorname{char} T \neq p$ і при $p = 2$ $\operatorname{char} T = 0$. Будемо називати два точних T-зображення Γ_1, Γ_2 групи G *спряженими*, якщо групи $\Gamma_1(G), \Gamma_2(G)$ спряжені в групі $GL(m, T)$ (m — степінь цих зображень). Незвідне T-зображення Γ групи G назвемо *примітивним* (*імпримітивним*), якщо матрична група $\Gamma(G)$ є примітивна (імпримітивна). Будемо використовувати позначення попереднього параграфа.

Лема 14.1.

1) *Групи* G_p, G_{21}, G_{22}, G_{23} *не мають точного примітивного зображення над полем* T.
2) *Нехай циклічна група* H *має точне примітивне зображення* Δ *над полем* T. *Тоді* $T(\xi) = T(\xi_1)$, *де* ξ — *первісний корінь степеня* p^n *із одиниці,* $\xi_1 = \xi^{p^{n-1}}$ *при* $p \neq 2$ *і* $\xi_1 = i = \sqrt{-1}$ *при* $p = 2$. *Окрім цього, якщо* $p = 2$ *і* $n = 2$, *то* $i \in T$. *Поле* $T(\xi_1)$ *є модулем зображення* Δ.

Доведення. 1) Скористаємось результатами і позначеннями §11. Розглянемо спочатку випадок $G \neq G_{23}$. Нехай $K = T(\xi)$ і Δ_0 — точне незвідне K-зображення групи G. Зображення Δ_0 спряжено із зображенням χ^G, що індукується лінійним характером

$$\chi : H = \langle a \rangle \to K,\ \chi(a) = \xi,$$

підгрупи H групи G. Будемо вважати, що $\Delta_0 = \chi^G$. Відмітимо, що Δ_0 — абсолютно незвідне зображення групи G над полем K. Нехай δ — характер зображення Δ_0. Тоді

$$\delta(g) = \begin{cases} 0, & g \in G \setminus \left\langle a^{p^k} \right\rangle; \\ p^k\chi(g), & g \in \left\langle a^{p^k} \right\rangle. \end{cases}$$

Доведемо це. Якщо $t \in \{0, 1, \ldots, p^k - 1\}$, то всі значення $(1 + p^{n-k})^t$ попарно різні за $\bmod p^n$. Якщо при цьому $\alpha(t)$ — така функція, що $(1 + p^{n-k})^t = 1 + \alpha(t)p^{n-k}$, то ця функція приймає попарно різні значення за $\bmod p^k$. Нехай

$$\Phi(x) = x^{p^k-1} + \cdots + x + 1.$$

Тоді для $g \in \langle a \rangle$

$$\delta(g) = \sum_{t=0}^{p^k-1} \chi(g)^{(1+p^{n-k})^t} = \chi(g)\Phi(\chi(g)^{p^{n-k}}),$$

звідки слідують формули для характера δ. Нехай $\eta = \xi^{p^k}, T_1 = T(\eta), L = T_1[x]$ — степенева алгебра над полем T_1 така, що $x^{p^k} = \eta$. Ця алгебра буде T_1G-модулем:

$$a(v) = xv \ (v \in L), \ b^{-1}(1) = 1,$$

$$b^{-1}(x^j) = b^{-1}(a^j(1)) = b^{-1}a^j b(b^{-1}(1) = x^{j\mu} \ (\mu = 1 + p^{n-k}).$$

Нехай Γ — T_1-зображення групи G, що має модуль L. Легко бачити, що зображення Γ — імпримітивне. Неважко бачити, що характер зображення Γ такий же, як характер δ. Звідси і із рівності степенів випливає, що зображення Δ_0 і зображення Γ є еквівалентні над полем K. Таким чином, Γ є абсолютно незвідним зображенням групи G над полем T_1, що є полем характера цього зображення над полем T. Таким чином, T_1 — поле розкладу зображення Δ_0. Нехай $\rho : T_1 \to M(d, T)$ — зображення поля T_1 матрицями порядку $d = (T_1 : T)$ над полем T і $T\Gamma$ — T-зображення групи G, яке отримується із зображення Γ заміною кожного матричного елемента $\alpha \in T_1$ на матрицю $\rho(\alpha)$. Тоді $T\Gamma$ — точне незвідне зображення групи G над полем T і будь-яке точне незвідне T-зображення з точністю до спряженості одержується описаним способом. Так як зображення Γ є імпримітивне, то зображення $\rho\Gamma$ також імпримітивне. Отже, група G $(G \neq G_{23})$ не має точного примітивного зображеня над полем T. Нехай тепер $G = G_{23}$. Як і в розглянутому випадку, точне абсолютно незвідне K-зображення Δ_0 індукується характером χ підгрупи H. Нехай $H_1 = \langle H, c \rangle$ і $\delta_1 = \chi^{H_1}$. Тоді $\Delta_0 = \delta_1^G$ і поле розкладу зображення δ_1 буде полем розкладу зображення Δ_0. Тоді $\rho(\Delta_0) = (\rho(\delta_1))^G$ — точне незвідне, але імпримітивне T-зображення групи G_{23}. 1) доведено.

2) Нехай Δ — точне примітивне зображення циклічної групи H над полем T, але $r = (T(\xi) : T(\xi_1)) > 1$. Тоді $r = p^s$, $s > 0$ і нехай T_1 таке підполе в $T(\xi)$, що $(T(\xi) : T_1) = p$. Тоді $\xi^p \in T_1$. Поле $T(\xi)$ буде модулем зображення $\Delta : a(v) = \xi v$ $(v \in T(\xi))$. Неважко бачити, що $\{T_1, \xi T_1, \ldots, \xi^{p-1}T_1\}$ — система імпримітивності TG-модуля $T(\xi)$. Це суперечить примітивності зображення Δ. Отже, $T(\xi) = T(\xi_1)$. Якщо $p = 2$ і $s = 2$, але $(T(i) : T) = 2$, то

$$\Delta(a) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

що також суперечить примітивності Δ. Отже, $i \in T$. Лема доведена.

Введемо в розгляд такі 2-групи:

$$C_{2^{n+1}} = \left\langle a_n \mid a_n^{2^{n+1}} = 1 \right\rangle$$

— циклічна група порядку 2^{n+1};

$$C_{2^\infty} = \left\langle a_n \ (n = 0, 1, \ldots) \mid a_n^2 = a_{n-1}, \ a_0^2 = 1 \right\rangle$$

— група типу 2^∞;

$$D_{2^{n+1}} = \left\langle C_{2^{n+1}}, \ b \mid b^2 = 1, \ b^{-1}a_n b = a_n^{-1} \right\rangle$$

— група діедра порядку 2^{n+2};

$$D_{2^\infty} = \left\langle C_{2^\infty},\ b \mid b^2 = 1,\ b^{-1}ab = a^{-1}\ (a \in C_{2^\infty}) \right\rangle;$$

$$Q_{2^{n+2}} = \left\langle C_{2^{n+1}},\ b \mid b^2 = a_n^{2^n},\ b^{-1}a_n b = a_n^{-1} \right\rangle$$

— група кватерніонів порядку 2^{n+2} $(n \geq 2)$;

$$Q_{2^\infty} = \left\langle C_{2^\infty},\ b \mid b^2 = a_0,\ b^{-1}ab = a^{-1}\ (a \in C_{2^\infty}) \right\rangle;$$

$$QD_{2^{n+1}} = \left\langle C_{2^{n+1}},\ b \mid b^2 = 1,\ b^{-1}a_n b = a_n^{-1+2^n} \right\rangle$$

— квазідіедральна група порядку 2^{n+2} $(n \geq 2)$.

Нехай T — поле характеристики нуль, T' — його алгебраїчне замикання, ξ_n — первісний корінь степеня 2^{n+1} із одиниці, $\xi_n^2 = \xi_{n-1}$, $\xi_1 = \sqrt{-1}$,

$$\alpha_n = \xi_n + \xi_n^{-1},\ \beta_n = \xi_n - \xi_n^{-1}.$$

Нехай поле T не містить $i = \sqrt{-1}$ (тобто $\beta_1 = 2i$ не міститься в цьому полі). Відмітимо, що тоді при $n > 1$ поле T не може одночасно містити α_n і β_n. Вивчимо T-зображення вказаних 2-груп.

Лема 14.2.

1) *Нехай натуральне n найбільше таке, що $\alpha_n \in T$. Тоді відповідність*

$$\Delta D_{2^{n+1}} : a \to A_n = 1/2 \begin{pmatrix} \alpha_n & i\beta_n \\ -i\beta_n & \alpha_n \end{pmatrix},\ b \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

буде єдиним з точністю до спряженості абсолютно незвідним точним зображенням групи $D_{2^{n+1}}$ над полем T. Зображення $\Delta D_{2^{n+1}}$ є імпримітивним лише у випадку $n = 1$.

Далі нехай в полі T існує розв'язок (γ, δ) рівняння

$$x^2 + y^2 = -1$$

(з невідомими x, y). Тоді відповідність

$$\Delta Q_{2^{n+2}} : a \to A_n = 1/2 \begin{pmatrix} \alpha_n & i\beta_n \\ -i\beta_n & \alpha_n \end{pmatrix},\ b \to \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix}$$

буде єдиним з точністю до спряженості абсолютно незвідним точним і примітивним зображенням групи $Q_{2^{n+2}}$ над полем T. Нехай в полі T не існує розв'язку рівняння $x^2 + y^2 = -1$. Тоді точне незвідне T-зображення групи $Q_{2^{n+2}}$ з точністю до спряженості має вигляд:

$$\widetilde{\Delta} Q_{2^{n+2}} : a \to \begin{pmatrix} A_n & 0 \\ 0 & A_n^{-1} \end{pmatrix},\ b \to \begin{pmatrix} 0 & -E \\ E & 0 \end{pmatrix}.$$

Це зображення, очевидно, є імпримітивне.

2) *Нехай $\alpha_n \in T$ $(n = 1, 2, \ldots)$. Тоді розглянуті в 1) T-зображення $\Delta D_{2^{n+1}}$, $\Delta Q_{2^{n+2}}$ $(\widetilde{\Delta} Q_{2^{n+2}})$ груп $D_{2^{n+1}}$, $Q_{2^{n+2}}$ однозначно продовжуються до T-зображень ΔD_{2^∞}, ΔQ_{2^∞} $(\widetilde{\Delta} Q_{2^\infty})$ груп D_{2^∞}, Q_{2^∞} відповідно. Зображення ΔD_{2^∞}, ΔQ_{2^∞} примітивні, зображення $\widetilde{\Delta} Q_{2^\infty}$ є імпримітивне.*

Доведення. Нехай $K = T(i)$. Тоді $\xi_n \in K$. Поле K має єдиний неодиничний автоморфізм Σ над полем T : $\Sigma(i) = -i$, $\Sigma(\xi_n) = \xi_n^{-1}$. Очевидно, $\Sigma(i\beta_n) = i\beta_n \in T$ і

$$\xi_n = 1/2(\alpha_n + i(-i\beta_n))$$

є розкладом елемента ξ_n за базисом $1, i$ поля K над полем T. Отже, оператор множення на ξ_n в цьому базисі буде мати матрицю A_n. Одержано T-зображення $a_n \to A_n$ групи C_n, модулем якого є поле K. Продовжимо це зображення на діедральну і кватерніонну групи. Для цього в полі K визначимо дію оператора b. Нехай

$$b(1) = \alpha + i\beta,$$

де α, β деякі елементи поля T. Тоді

$$b(i) = b(a_1(1)) = ba_1b^{-1}(b(1)) = a_1^{-1}(b(1)) = -ib(1).$$

Звідси слідує, що

$$b(v) = \Sigma(v)b(1) \quad (v \in K).$$

Елемент $\omega = b(1)$ не може бути довільним. Так як $b^2 = 1$ в діедральній групі і $b^2 = a_n^{2^n}$ в кватерніонній групі, то

$$\omega\Sigma(\omega) = \pm 1,$$

де плюс береться для групи $D_{2^{n+1}}$, а мінус для групи $Q_{2^{n+2}}$ (другий випадок можливий тоді і тільки тоді, коли координати елемента $\omega = \gamma + i\delta$ будуть розв'язком рівняння $x^2 + y^2 = -1$). Нехай для $\omega = b(1)$ вказана умова виконується. Позначимо через K_ω одержаний при цьому TG-модуль ($G = \langle C_{2^n}, b\rangle$). Покажемо, що всі такі модулі є попарно ізоморфні. Нехай K_{ω_1}, K_{ω_2} — два TG-модулі. Тоді $N(\omega_1\omega_2^{-1}) = 1$ (N — функція норми: $N(\alpha + i\beta) = \alpha^2 + \beta^2$). Як відомо, $N(v) = 1$ ($v \in K$) тоді і тільки тоді, коли $v = u\Sigma(u^{-1})$ ($u \in K$). Отже, для деякого елемента $\rho \in K$

$$\rho\omega_1 = \omega_2\Sigma(\rho).$$

Тоді відображення $\varepsilon : K_{\omega_2} \to K_{\omega_1}$ таке, що $\epsilon(v) = \rho v$ ($v \in K$) буде ізоморфізмом TG-модулів. Таким чином, з точністю до еквівалентності існує тільки одне продовження зображення Δ групи C_{2^n} до зображення у випадку діедральної групи і не більше одного продовження для випадку кватерніонної групи. В першому випадку можна взяти $b(1) = 1$ і тоді $\Delta(b) = \mathrm{diag}[1, -1]$, а в другому — $b(1) = \gamma + i\delta$, $\gamma^2 + \delta^2 = -1$, $(\gamma, \delta \in T)$ і тоді

$$\Delta(b) = \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix}.$$

В результаті ми одержимо ті зображення, що вказані в лемі.

Нехай Γ — точне незвідне T'-зображення групи G. Тоді існує лінійний характер $\chi : C_{2^n} \to T'$ такий, що $\Gamma = \chi^G$, тобто це зображення індукується цим характером. Очевидно, $\chi(a_n) = \xi$ — один із коренів степеня 2^n із -1. Зображення, що здобувається для іншого значення характера буде спряжено із зображенням Γ. Нехай $\chi(a_n) = \xi_n$. Тоді характер зображення Γ буде таким же, як характер зображення Δ, яке вказане в лемі. Отже, ці зображення еквівалентні і лема доведена для груп діедра і доведена для груп кватерніонів у випадку розв'язності певного рівняння. Розглянемо випадок коли це рівняння не має розв'язку. Цей випадок стосується групи $Q_{2^{n+2}}$. Її зображення Γ має вигляд:

$$a_n \to \mathrm{diag}[\xi_n, \xi_n^{-1}],\ b \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Це зображення еквівалентно зображенню

$$a_n \to A_n,\ b \to i\,\mathrm{diag}[1, -1]$$

над полем K, а сума двох цих зображень буде еквівалентна (над K) тому T-зображенню (групи $Q_{2^{n+2}}$), яке наведене в лемі. (Відмітимо, що поле K є те найменше розширення поля T характера зображення Γ, над яким це зображення можна реалізувати,

інакше кажучи, індекс Шура зображення Γ відносно поля T дорівнює $(K : T) = 2$). Ми описали той шлях, з допомогою якого здобуваються точні незвідні T-зображення групи $Q_{2^{n+2}}$. Перша частина леми доведена. Друга частина є наслідком першої.

Розглянемо тепер випадок, коли поле T містить елементи вигляду β_n $(n > 1)$. Відмітимо, що поле T не може містити два таких різних елементи (інакше $i \in T$).

Лема 14.3. *Нехай $\beta_n \in T$ для деякого $n \geq 2$. Тоді відповідність*

$$\Delta Q_{2^{n+2}} : a \to A'_n = 1/2 \begin{pmatrix} \beta_n & i\alpha_n \\ -i\alpha_n & \beta_n \end{pmatrix}, \; b \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

буде з точністю до спряженості єдиним точним абсолютно незвідним і примітивним T-зображенням групи $Q_{2^{n+2}}$.

Доведення цієї леми аналогічне випадку попередньої леми. Відмінність тільки в іншій дії автоморфізму $\Sigma : \Sigma(\xi_n) = -\xi_n^{-1}$. Окрім цього, $\Sigma(\beta_n) = \beta_n$, $\Sigma(i\alpha_n) = i\alpha_n$ і

$$\xi_n = 1/2(\beta_n + i(-i\alpha_n)).$$

Нехай поле T задовольняє умові 1) леми 14.2 або умовам леми 14.3, T_0 — таке підполе в T, що $T = T_0(\alpha_n)$ або, відповідно, $T = T_0(\beta_n)$, G одна із груп $D_{2^{n+1}}$, $Q_{2^{n+2}}$ або, відповідно, $G = Q_{2^n}$ і Δ — T-зображення групи G, що описане в лемах 14.2, 14.3. Нехай $d = (T : T_0)$ і $\rho : T \to M(d, T_0)$ — матричне над полем T_0 зображення степеня d поля T, яке ставить у відповідність довільному елементу $\omega \in T$ матрицю $\rho(\omega)$ оператора $\widehat{\omega}$ множення на цей елемент $(\widehat{\omega}(x) = \omega x)$ $(x \in T)$ в певному базисі поля T над T_0. Якщо $A = (\alpha_{ij})$ — матриця порядку s над полем T, то через $\rho(A)$ позначимо матрицю порядку ds над полем T_0, що одержується заміною матричних елементів α_{ij} на відповідні матриці $\rho(\alpha_{ij})$.

Лема 14.4. *Відповідність*

$$\rho(\Delta) : g \to \rho(\Delta(g)) \quad (g \in G)$$

буде незвідним зображенням групи G над полем T_0. Будь-яке точне незвідне T_0-зображення групи G спряжено з зображенням $\rho(\Delta)$. Нехай $d > 1$. Зображення $\rho(\Delta)$ буде примітивним тоді і тільки тоді, коли виконуються умови:

$$T = T_0(\alpha_n), \quad G = Q_{2^{n+2}}$$

і рівняння $x^2 + y^2 = -1$ не має розв'язку в полі $T_0(\alpha_{n-1})$.

Доведення. Нехай $\Sigma_1, \ldots, \Sigma_d$ — всі автоморфізми поля T над полем T_0 і

$$\Delta_j : g \to \Sigma_j(\Delta(g)) \quad (g \in G)$$

— T-зображення групи G, спряжене автоморфізмом Σ_j до зображення Δ. Зображення $\Delta_1, \ldots, \Delta_d$ попарно нееквівалентні над полем T, а їх сума $\Delta_1 + \ldots + \Delta_d$ еквівалентна над полем T незвідному зображенню групи G матрицями над полем T_0. Характер зображення $\rho(\Delta)$ рівний характеру суми $\Delta_1 + \ldots + \Delta_d$ і, отже, з точністю до еквівалентності (над полем T)

$$\rho(\Delta) = \Delta_1 + \ldots + \Delta_d.$$

Звідси випливає незвідність T_0-зображення $\rho(\Delta)$ групи G. Так як всі точні незвідні T-зображення групи G попарно спряжені, то попарно спряженими будуть всі точні незвідні групи G над полем T_0.

Нехай $d > 1$. Дослідимо на примітивність зображення $\rho(\Delta)$ групи G над полем T_0. Модулем цього зображення є поле $K = T(i) = T_0(\gamma_n, i)$, де $\gamma_n = \alpha_n$, або $\gamma_n = \beta_n$. Група G діє в цьому модулі так, як вказано при доведені лем 14.2, 14.3. Так як

$$\alpha_n^2 = \alpha_{n-1} + 2, \quad \beta_n^2 = \alpha_{n-1} - 2,$$

то $\alpha_{n-1} \in T$, поле $T_1 = T_0(\alpha_{n-1})$ міститься в полі T і $(T : T_1) = 2$. Нехай $K^1 = T_1(i)$. Тоді $(K : K^1) = 2$,

$$K = K^1 + K^1\xi_n,\ \xi_n^2 \in K^1.$$

Нехай G — діедральна або квазідіедральна група. Тоді

$$a_n(K^1) = K^1\xi_n,\ a_n(K^1\xi_n) = K^1\xi_n^2 = K^1,$$

$$b(K^1) = \Sigma(K^1) = K^1,\ b(K^1\xi_n) = K^1\xi_n^{-1} = (K^1\xi_n^{-2})\xi_n = K^1\xi_n.$$

Звідси слідує, що T_0-підпростори K^1, $K^1\xi_n$ утворюють систему імпримітивності групи G, тобто зображення $\rho(\Delta)$ буде імпримітивним.

Розглянемо випадок групи $G = Q_{2^{n+2}}$ і нехай при цьому

$$K_\omega = K, \quad b(x) = \Sigma(x)\omega \quad (x \in K)$$

— буде модулем зображення $\rho(\Delta)$. Нехай в полі T_1 рівняння $x^2+y^2 = -1$ має розв'язок (γ_1, δ_1). Як показано при доведені леми 14.2, TG-модулі

$$K_\omega,\ K_{\omega_1} \quad (\omega_1 = \gamma_1 + i\delta_1 \in T_1)$$

будуть ізоморфні. Отже можна вважати, що T_0-зображення $\rho(\Delta)$ побудовано для модуля $K = K_{\omega_1}$. Так як, при цьому, $b(K^1) = K^1$, то $\{K^1, K^1\xi_n\}$ — система імпримітивності групи G, тобто T_0-зображення $\rho(\Delta)$ буде імпримітивним. Навпаки, нехай зображення $\rho(\Delta)$ групи $G = Q_{2^{n+2}}$ є імпримітивним і K_ω $(\omega \in T)$ є модулем цього зображення. Так як цей модуль імпримітивний, то

$$K_\omega = L_1 \oplus L_2$$

— пряма сума T_0-підпросторів таких, що

$$a_n(L_1) = L_2, \quad a_n(L_2) = L_1, \quad b(L_j) = L_j.$$

Це можливо тільки у випадку коли $L_1 = K^1$, $L_2 = K^1\xi_n$. Це значить, що K^1 є модулем для групи $Q_{2^{n+1}}$. Тоді $b(1) \in K^1$, тобто

$$b(1) = \gamma_1 + i\delta_1 \quad (\gamma_1,\ \delta_1 \in T_1,\ \gamma_1^2 + \delta_1^2 = -1).$$

Лема доведена.

§15. Силовські p-підгрупи групи $GL(n, T)$ ($p > 2$ або $p = 2$ і $\sqrt{-1} \in T$)

Як і раніше, T — поле, характеристика якого відмінна від p. Так само будемо вживати позначення ξ_n для первісного кореня степеня p^n із одиниці при $p \neq 2$ і для кореня степеня 2^n із -1. Нехай $d = (T(\xi_1) : T)$ і $\rho : T(\xi_1) \to M(d, T)$ — зображення поля $T(\xi_1)$ матрицями порядку d над полем T. Через $P_q(K)$ (q — просте) будемо позначати силовську q-підгрупу в мультиплікативній групі поля K.

Теорема 15.1. *Нехай $p > 2$ або при $p = 2$ поле T містить корінь $\sqrt{-1}$. В групі $GL(n, T)$ тоді і тільки тоді існує неодинична примітивна силовська p-підгрупи, коли $n = d = (T(\xi_1) : T)$. Якщо U — примітивна силовська p-підгрупа в групі $GL(d, T)$, то група U спряжена з групою $\rho(P_p(T(\xi_1)))$.*

Доведення. Нехай G — примітивна p-підгрупа групи $GL(n,T)$. Використаємо лему 12.3, згідно якої група G є розширення деякої p-підгрупи F в мультиплікативній групі K^* поля $K=T(\xi)$ $(\xi^{p^s}=1)$ з допомогою p-підгрупи G/F групи Галуа поля K над полем T.

Нехай G — нескінченна група. Тоді $F\cong C_{p^\infty}=\langle a_n\ (n=0,1,\ldots)\mid a_n^p=a_{n-1},\ a_0^p=1\rangle$ — група типу p^∞,

$$T(\xi_1)=T(\xi_m)\quad (m=1,2,\ldots),\quad K=T(\xi_1)$$

(див. лему 13.2). При $p>2$ група типу p^∞ не має автоморфізму порядку p, тобто $G=F$ і $n=(T(\xi_1):T)$. При $p=2$ група типу 2^∞ має автоморфізм порядку 2, який кожний елемент x цієї групи переводить в обернений x^{-1}. Нехай для цього автоморфізма існує автоморфізм σ поля K над полем T. Тоді $\sigma(\xi)=\xi^{-1}$, але неможливо $\sigma(i)=-i$ (поле T містить $i=\sqrt{-1}$). Отже, поле K такого автоморфізму не має. Таким чином, і при $p=2$ маємо $G=F$ і тоді $n=1=(T(\xi):T)$. Отже, в обох випадках $G=F=\rho(P_p(T(\xi_1)))$ і $n=(T(\xi):T)=(T(\xi_1):T)$.

Нехай G — скінченна група. Використаємо лему 13.1. При $p>2$ маємо $G=G_p$, а при $p=2$ група G може бути лише групою G_{21} (лише для цієї групи відповідні автоморфізми поля K зберігають елемент $i\in T$). З леми 14.1 випливає, що G — циклічна група і поле K є TG-модулем. Отже, $G=\rho(P_p(T(\xi_1)), n=d=(T(\xi_1):T)$. З другого боку, якщо поле $T(\xi_1)$ є модулем T-зображення для деякої p-групи G, то в силу обмеження $0\leqslant d<p$, цей модуль не може бути імпримітивним. Отже, група $\rho(P_p(T(\xi_1))$ — примітивна. Це доводить теорему.

Нехай виконуються умови теореми 15.1, $U=\rho(P_p(T(\xi_1))$ — силовська p-підгрупа групи $GL(d,T)$ $(d=(T(\xi_1):T)$, $\xi_1^p=1$ $(p\neq 2)$, $\chi^2=-1$ $(p=2))$. Введемо деякі позначення. Нехай C_p — циклічна порядку p група підстановок, породжена циклом $\sigma=(12\ldots p)$,

$$W_0=U,\quad W_1=W_0\wr C_p,\quad \ldots,\quad W_j=W_{j-1}\wr C_p$$

— сплетіння матричної групи W_{j-1} і групи підстановок C_p $(j=1,\ 2,\ \ldots)$. З леми 12.4 випливає, що група W_j буде незвідною силовською p-підгрупою групи $GL(dp^j,T)$. Нехай m — довільне натуральне число,

$$m=m_0+dn\quad (0\leqslant m_0<d),$$
$$n=n_0+n_1p+\cdots+n_sp^s\quad (0\leqslant n_i<p,\ n_s\neq 0)$$

— p-ічний розклад числа n. Нехай

$$U_m=\langle 1\rangle^{m_0}\times W_1^{n_1}\times\cdots\times W_s^{n_s}$$

— прямий добуток груп, взятий по всіх тих j, для яких $n_j\neq 0$ ($\langle 1\rangle^{m_0}$ — одинична група для випадку $m_0\neq 0$).

Теорема 15.2. *З точністю до спряженості група W_j є єдиною незвідною силовською p-підгрупою групи $GL(dp^j,T)$, а група U_m — єдиною силовською p-підгрупою в групі $GL(m,T)$.*

Наслідок 15.1. *Нехай характеристика поля T відмінна від p і при $p=2$ це поле містить $\sqrt{-1}$. Тоді силовські p-підгрупи групи $GL(m,T)$ попарно спряжені в цій групі.*

Наслідок 15.2. *Нехай характеристика поля T відміна від p. Будь-яка p-підгрупа H групи $GL(n,T)$ є групою Чернікова[5], зокрема, ця підгрупа задовольняє нормалізаторній умові[6].*

[5] *p-група Чернікова* — розширення прямого добутку скінченного числа груп типу p^∞ за допомогою скінченної p-групи.

[6] Група, яка задовольняє *нормалізаторній умові* — група H всяка власна підгрупа якої відмінна від свого нормалізатора в групі H.

§16. Силовські 2-підгрупи групи $GL(n,T)$ ($\operatorname{char} T = q > 2$)

Нехай ξ_s — корінь степеня 2^s із мінус одиниці і $\xi_s^2 = \xi_{s-1}, s \geq 1, \xi_0 = -1$. Через $P_2(K)$ будемо позначати силовську 2-підгрупу мультиплікативної групи K^* поля K.

Будемо вживати позначення:

$$\alpha_s = \xi_s + \xi_s^{-1}, \quad \beta_s = \xi_s - \xi_s^{-1} \quad (s \geq 1).$$

Відмітимо, що

$$\alpha_1 = 0, \quad \beta_1 = 2\xi_1, \quad \alpha_2 = \sqrt{2}, \quad \beta_2 = \sqrt{-2}.$$

Нехай T — поле характеристики $q > 2$ і $\mathbb{Z}_q$ — просте підполе із q елементів.

Лема 16.1. *Нехай $q \equiv 1 \pmod 4$ або поле T містить скінченне підполе парного степеня над полем $\mathbb{Z}_q$. Якщо H — примітивна силовська 2-підгрупа групи $GL(n,T)$, то $n = 1$ і $H = P_2(T)$.*

Доведення. $\xi_1 = \sqrt{-1} \in T$ і лема випливає із результатів §14.

Нехай $q \equiv -1 \pmod 4$ і будь-яке скінченне підполе в T має непарну степінь над полем $\mathbb{Z}_q$. Тоді $P_2(T) = \{1, -1\}$. Так як поле T містить $\sqrt{2}$ або $\sqrt{-2}$, то сплетіння $W_2(P_2(T)) = P_2(T) \wr S_2$ не буде силовською 2-підгрупою групи $GL(2,T)$.

Лема 16.2. *Нехай $q \equiv -1 \pmod 4$. В групі $GL(m,T)$ ($m > 1$) тоді і тільки тоді міститься примітивна силовська 2-підгрупа, коли $m = 2$. Нехай s — найбільший показник такий, що 2^s ділить $q + 1$. Тоді $s \geq 2$, $\beta_s \in T$ і квазідіедральна група (порядку 2^{s+2})*

$$QD_{2^{s+1}} = \left\langle a = \frac{1}{2}\begin{pmatrix} \beta_s & i\alpha_s \\ -i\alpha_s & \beta_s \end{pmatrix},\ b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \quad (a^{2^{s+1}} = b^2 = 1,\ b^{-1}ab = -a^{-1})$$

буде примітивною силовською 2-підгрупою в групі $GL(2,T)$ (див. також лему 14.3).

Доведення. Нехай G — примітивна силовська 2-підгрупа групи $GL(m,T)$ і F — максимальна нормальна абелева підгрупа в G. Тоді $F \cong P_2(T(\xi))$, де $\xi^{2^n} = 1$ для деякого n, а група G/F ізоморфна силовській 2-підгрупі групи Галуа $G(K,T)$ поля $K = T(\xi)$ над полем T. Ця група породжується автоморфізмом Фробеніуса: $\sigma(v) = v^q$ ($v \in K$), порядок якого дорівнює $(K : T) = 2^k$ для деякого натурального k. Так як група типу 2^∞ не має автоморфізму типу σ, то група F буде скінченною і тоді група G суміщається з групою G_{22} або з групою QD_{2^n} з леми 13.1. Група G_{22} не має точного примітивного зображення над полем T, а в силу лем 14.3–14.4, степінь примітивного зображення групи QD_{2^n} рівна 2. Отже, $m = 2$. Група $GL(2,T)$ містить циклічну 2-підгрупу найвищого порядку 2^{s+1}. Отже, $n = s + 1$, $\xi = \xi_s$, $\xi^q = -\xi^{-1}$, $\sigma(\beta_s) = \beta_s$ і $\beta_s \in T$. Тоді група $QD_{2^{s+1}}$ міститься в групі $GL(2,T)$ і є примітивною силовською 2-підгрупою в цій групі. Лема доведена.

Нехай

$$n = n_0 + n_1 2 + \cdots + n_t 2^t \quad (0 \leqslant n_j < 2,\ n_t \neq 0)$$

— 2-ічний розклад натурального числа n.

Теорема 16.1. *Нехай $q \equiv 1 \pmod 4$ або поле T містить скінченне підполе парного степеня над простим підполем. Тоді будь-яка силовська 2-підгрупа групи $GL(n,T)$ спряжена з групою*

$$(W_0)^{n_0} \times (W_1)^{n_1} \times \cdots \times (W_t)^{n_t}$$

($W_0 = P_2(T)$, $W_j = W_{j-1} \wr C_2$ $(j = 1, 2, \ldots)$).

Теорема 16.2. *Нехай $q \equiv -1 \pmod 4$ і будь-яке скінченне підполе поля T має непарну розмірність над простим підполем. Тоді будь-яка силовська 2-підгрупа групи $GL(n,T)$ спряжена з групою*

$$(\langle -1\rangle)^{n_0} \times (W_0)^{n_1} \times \cdots \times (W_{t-1})^{n_t}$$

($W_j = W_{j-1} \wr C_2$ $(j = 1, 2, \ldots)$, $W_0 = QD_{2^{s+1}}$ — група, що вказана в лемі 16.2).

§17. Силовські 2-підгрупи групи $GL(n,T)$ $(\operatorname{char} T = 0)$

Нехай T — поле характеристики нуль і $i = \sqrt{-1}$ не міститься в цьому полі. Використовуючи результати про примітивні зображення 2-груп (див. §14) дамо описання силовських 2-підгруп групи $GL(m,T)$ $(m > 1)$. Нагадаємо позначення. Нехай ξ_s — первісний корінь степеня 2^{s+1} із 1,

$$\alpha_s = \xi_s + \xi_s^{-1}, \quad \beta_s = \xi_s - \xi_s^{-1} \quad (s = 1,\ 2,\ \ldots).$$

Наприклад, $\alpha_1 = 0$, $\beta_1 = 2\sqrt{-1}$, $\alpha_2 = \sqrt{2}$, $\beta_2 = \sqrt{-2}$ і т. д. Якщо поле T містить α_s або β_s, то любому випадку $\alpha_{s-1} \in T$ $(s > 1)$. Поле T не може містити одночасно α_s, β_s $(s \geqslant 1)$ і не може містити одночасно двох різних β_s, β_k. Неважко бачити, що

$$\xi_s = \frac{1}{2}(\alpha_s - i(i\beta_s)) = \frac{1}{2}(\beta_s - i(i\alpha_s)),$$

що дає розклад за базисом 1, i. Окрім цього, ξ_s є коренем многочленів

$$x^2 - \alpha_s x + 1, \quad x^2 - \beta_s x - 1.$$

Нехай $K = T(i)$, $P_2 = P_2(T)$ і $P_2(K)$ — силовські 2-підгрупи в T^* і K^* відповідно. Очевидно, $P_2 = \langle -1\rangle = \{1,\ -1\}$, $i \in P_2(K)$.

Введемо в розгляд нормене відображення $N : K \to T$, поклавши

$$N(a + bi) = a^2 + b^2 \quad (a, b \in T).$$

Якщо $a \in T$, то $N(a) = a^2$. Якщо $w \in T(i)$, $w \notin T$, то норма $N(w)$ рівна вільному члену квадратного тричлена над T, коренем якого є w.

Нехай σ — автоморфізм поля $T(i)$ такий, що $\sigma(i) = -i$. Тоді $\sigma(\xi_s) = \xi_s^{-1}$. Якщо $\alpha_s \in T$, то $i\beta_s \in T$ і якщо $\beta_s \in T$, то $i\alpha_s \in T$. Далі

$$N(w) = w\sigma(w), \quad w \in T(i).$$

Якщо $\omega \in P_2(K)$, то $N(\omega) = \pm 1$. Отже, можливі два випадки:
1) $N(P_2(K)) = \{1\}$;
2) $N(P_2(K)) = \{1, -1\}$.

В залежності від цих випадків проведемо описання силовських 2-підгруп групи $GL(m,T)$. Нехай всюди далі

$$m = m_0 + m_1 2 + \cdots + m_s 2^s$$

— 2-ічний розклад натурального числа m. Нехай H — підгрупа групи $GL(d,T)$. Через $W(H) = H \wr C_2$ будемо позначати сплетіння групи H і циклічної групи C_2 підстановок степеня 2. Нехай

$$W_0(H) = H, \quad W_j(H) = W_{j-1}(H) \wr C_2 \quad (j = 1, 2, \ldots).$$

Група $W_j(H)$ — підгрупа в групі $GL(2^j d, T)$.

Розглянемо спочатку випадок нескінченних матричних 2-груп.

Теорема 17.1. *Нехай $N(P_2(K))$ — одинична група і поле T задовольняє умовам*
1) *всі елементи α_s $(s = 1, 2, \ldots)$ належать полю T;*
2) *рівняння $x^2 + y^2 = -1$ не має розв'язків над полем T.*

Тоді група

$$D_\infty = \left\langle b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ a_s = \frac{1}{2}\begin{pmatrix} \alpha_s & i\beta_s \\ -i\beta_s & \alpha_s \end{pmatrix} \quad (s = 1, 2, \ldots) \right\rangle$$

буде примітивною силовською 2-підгрупою групи $GL(2, T)$. Нехай $W_0(D_\infty) = D_\infty, W_J(D_\infty) = W_{j-1}(D_\infty) \wr C_2$. Тоді група $W_j(D_\infty)$ буде незвідною силовською 2-підгрурою групи $GL(2^{j+1}, T)$. Будь-яка силовська 2-підгрупа групи $GL(m, T)$ спряжена в цій групі з прямим добутком

$$P_2^{m_0} \times (W_0(H))^{m_1} \times \cdots \times (W_{s-1}(H))^{m_s},$$

де $H = D_\infty$.

Теорема 17.2. *Нехай $N(P_2(K))$ — одинична група і поле T задовольняє умовам*
1) *всі елементи α_s $(s = 1,\ 2,\ \ldots)$ належать полю T;*
2) *в полі T існують такі елементи γ, δ, що $\gamma^2 + \delta^2 = -1$.*

Тоді група D_∞ і група

$$Q_\infty = \left\langle c = \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix},\quad a_s\ (s = 1, 2, \cdots) \right\rangle$$

будуть неізоморфними примітивними силовськими 2-підгрупами групи $GL(2, T)$, а групи $W_j(D_\infty)$ і $W_j(Q_\infty)$ будуть неізоморфними незвідними силовськими 2-підгрупами групи $GL(2^{j+1}, T)$.
Нехай $m - m_0 = 2(u + v)$ і

$$u = u_0 + u_1 2 + \cdots + u_k 2^k, \quad v = v_0 + v_1 2 + \cdots + v_r 2^r$$

— 2-ічні розклади. Тоді прямий добуток

$$P_2^{m_0} \times (W_0(D_\infty))^{u_0} \times \cdots \times (W_{k-1}(D_\infty))^{u_k} \times (W_0(Q_\infty))^{v_0} \times \cdots \times (W_{r-1}(Q_\infty))^{v_r}$$

буде силовською 2-підгрупою групи $GL(m, T)$. Різні пари (u, v) визначають неізоморфні силовські 2-підгрупм групи $GL(m, T)$. З точністю до спряженості (і ізоморфізму) в групі $GL(m, T)$ існує $[\frac{m}{2}] + 1$ силовських 2-підгруп.

Розглянемо тепер випадки скінченних матричних 2-груп.

Теорема 17.3. *Нехай $N(P_2(K))$ — одинична група і поле T задовольняє умовам*
1) *не всі α_s містяться в полі T і нехай n найбільше таке, що $\alpha_n \in T$;*
2) *рівняння $x^2 + y^2 = -1$ не має розв'язку над полем $T(\alpha_1, \alpha_2, \ldots)$.*

Тоді діедральна група

$$D_{2^{n+1}} = \langle a_n,\ b = \mathrm{diag}[1, -1] \rangle$$

порядку 2^{n+2} буде незвідною і примітивною при $n > 1$ силовською 2-підгрупою групи $GL(2, T)$. Група $W_j(D_{2^{n+1}})$ буде незвідною силовською 2-підгрупою групи $GL(2^{j+1}, T)$. Будь-яка силовська 2-підгрупа групи $GL(m, T)$ буде спряжена з прямим добутком

$$P_2^{m_0} \times (W_0(H))^{m_1} \times \cdots \times (W_{s-1}(H))^{m_s},$$

де $H = D_{2^{n+1}}$ при $n > 1$ і $H = P_2 \wr C_2$ при $n = 1$.

Теорема 17.4. *Нехай $N(P_2(K))$ — одинична група і поле T задовольняє умовам*
1) *не всі α_s містяться в полі T і нехай n найбільше таке що $\alpha_n \in T$;*
2) *рівняння $x^2+y^2=-1$ має розв'язки над деякими полями $T(\alpha_s)$ і нехай r $(r \geq n)$ найменше таке, що вказане рівняння має розв'язок (γ, δ) над полем $T(\alpha_r)$.*

Тоді кватерніонна група

$$Q_{2^{r+2}} = \left\langle \widetilde{a_r} = \begin{pmatrix} \rho(\alpha_r) & \rho(i\beta_r) \\ -\rho(i\beta_r) & \rho(\alpha_r) \end{pmatrix}, \quad \widetilde{b} = \begin{pmatrix} \rho(\gamma) & \rho(\delta) \\ \rho(\delta) & -\rho(\gamma) \end{pmatrix} \right\rangle$$

порядку 2^{r+2} буде прмітивною силовською 2-підгрупою групи $GL(2d, T)$ (тут ρ — зображення поля $T(\alpha_r)$ матрицями порядку $d = (T(\alpha_r) : T)$.) Група $W_j(Q_{2^{r+2}})$ буде незвідною силовською 2-підгрупою групи $GL(2^{j+1}d, T)$. Окрім цього, в групі $GL(2^{j+1}d, T)$ є ще одна силовська 2-підгрупа — $W_{j+l}(D_{2^{n+1}})$ $(l = \log_2 d)$, що неізоморфна групі $W_j(Q_{2^{r+2}})$. Нехай $m = d_0 + 2dm'$, де $0 \leqslant d_0 < 2d$ і, якщо $m \geq 2d$, то

$$m' = 2d(u+v), \quad u = u_0 + u_1 2 + \cdots + u_t 2^t, \quad v = v_0 + v_1 2 + \cdots + v_k 2^k$$

— 2-ічні розклади. Тоді прямий добуток

$$H_0 \times (W_0(H_1))^{u_0} \times \cdots \times (W_{t-1}(H_1))^{u_t} \times (W_0(H_2))^{v_0} \times \cdots \times (W_{k-1}(H_2))^{v_k},$$

де H_0 — силовська 2-підгрупа групи $GL(d_0, T)$ (вона описується попередньою теоремою), $H_1 = W_l(D_{2^{n+1}})$, $H_2 = Q_{2^{r+2}}$. Число всіх попарно неспряжених силовських 2-підгруп групи $GL(m, T)$ дорівнює $[\frac{m}{2d}] + 1$.

Теорема 17.5. *Нехай $N(P_2(K)) = \{1, -1\}$. Тоді існує тільки один елемент $\beta_n \in$ $\in T$ $(n \geq 2)$. Єдиною (відмінною від групи $\langle -1 \rangle$) примітивною силовською 2-підгрупою матриць над полем T є квазідіедральна група матриць порядку 2:*

$$Q_{2^{n+2}} = \left\langle a'_n = \begin{pmatrix} \beta_n & i\alpha_n \\ i\alpha_n & \beta_n \end{pmatrix}, \quad b = \operatorname{diag}[1, -1] \right\rangle$$

порядку 2^{n+2}.

Будь-яка силовська 2-підгрупа групи $GL(m, T)$ буде спряжена в цій групі з прямим добутком

$$(\langle -1 \rangle)^{m_0} \times (W_0(H))^{m_1} \times \cdots \times (W_{s-1}(H))^{m_s},$$

де $H = Q_{2^{n+2}}$.

Теорема 17.6. *При будь-якому m силовські 2-підгрупи групи $GL(m, T)$ спряжені в цій групі тоді і тільки тоді, коли виконується одна з умов:*
1) *$N(P_2(K)) = \langle -1 \rangle$ $(K = T(i))$;*
2) *$N(P_2(K)) = 1$ і рівняння $x^2+y^2=-1$ нерозв'язне над полями $T(\alpha_s)$, $s = 1, 2, \ldots$*

Доведення теорем 17.1–17.6 випливає з описання примітивних зображень 2-груп над полем T (див. §14) і загальних властивостей матричних силовських підгруп (див. §12).

Як підсумок одержуємо такий результат про спряженість силовських підгруп в матричних групах.

Наслідок 17.1. *Нехай F — поле. Для всіх m силовські p-підгрупи групи $GL(m, F)$ спряжені в цій групі тоді і тільки тоді, коли виконується одна із умов:*
1) *$p > 2$ або $p = 2$ і $\sqrt{-1} \in F$;*
2) *$\operatorname{char} F > 0$;*
3) *$p = 2$, $\operatorname{char} F = 0$, $\sqrt{-1} \notin F$, $N(P_2(F(i))) = \langle -1 \rangle$ або $N(P_2(F(i))) = 1$ і рівняння $x^2+y^2=-1$ нерозв'язне над полями $F(\alpha_s)$, $s = 1, 2, \ldots$*

§18. Групи $GL(n,\mathbb{Z})$, $SL(n,\mathbb{Z})$

Нехай K — комутативне кільце з одиницею 1, $GL(n,K)$ — повна лінійна група матриць порядку n над кільцем K і E_n — одиниця цієї групи. Група $GL(n,K)$ суміщається з множиною всіх матриць порядку n над кільцем K, детермінанти яких належать мультиплікативній групі K^* кільця K. Будемо використовувати деякі позначення розділу 1:

$$e_{ij}\ (1 \leqslant i,j \leqslant n)$$

— матричні одиниці,

$$t_{ij}(\lambda) = E_n + \lambda e_{ij}\ (i \neq j)$$

— елементарна матриця з недіагональним елементом $\lambda \in K$. Нехай

$$SL(n,K) = \langle t_{ij}(\lambda) | i \neq j, \lambda \in K \rangle$$

— підгрупа в $GL(n,K)$, яка породжується всіма елементарними матрицями. Група $SL(n,K)$ називається *спеціальною лінійною групою* степеня n над кільцем K.

Нагадаємо, для того, щоб помножити матрицю A зліва (справа) на елементарну матрицю $t_{ij}(\lambda)$ потрібно до i-го рядка (j-го стовпчика) додати j-ий рядок (i-ий стовпчик), домноженний на λ. Ці перетворення називаються *елементарними*. Помножити матрицю A зліва на матрицю з групи $SL(n,K)$ — значить виконати в матриці декілька елементарних перетворень над рядками.

Нехай $K = \mathbb{Z}$ — кільце цілих раціональних чисел. Якщо $A \in GL(n,\mathbb{Z})$, то $\det A = \pm 1$.

Теорема 18.1. *Нехай $A \in GL(n,\mathbb{Z})$. Тоді існує єдина матриця C в групі $SL(n,\mathbb{Z})$ така, що $A = C\,\mathrm{diag}[1,\ldots,1,\pm 1]$.*

Доведення. При $n = 1$ теорема очевидна. Нехай $n > 1$. Елементарними перетвореннями над рядками (використовуючи вправи в кінці цього параграфа) з матриці A неважко одержати матрицю, в який перший стовчик буде складатись із нулів, окрім першого елемента, рівного одиниці. Застосувавши індуктивне припущення одержимо верхньотрикутну матрицю, в якій нульовими будуть елементи вище діагоналі, за виключенням елементів першого рядка. Додавши до 1-го рядка лінійну комбінацію інших рядків, одержимо діагональну матрицю, вказану в теоремі. Теорема доведена.

Наслідок 18.1. *Група $SL(n,\mathbb{Z})$ складається з матриць, детермінант яких дорівнює одиниці.*

Наслідок 18.2. *Група $SL(n,\mathbb{Z})$ буде нормальною підгрупою групи $GL(n,\mathbb{Z})$.*

Доведення випливає з рівності $[GL(n,\mathbb{Z}) : SL(n,\mathbb{Z})] = 2$.

Вправа 1. Показати, що якщо $d = \mathrm{diag}[\pm 1, \ldots, \pm 1]$, де кількість (-1) парна, то $d \in SL(n,K)$.

Вправа 2. Показати, що якщо $\sigma \in S_n$ і σ — парна підстановка, то підстановочна матриця $\widetilde{\sigma}$ міститься в $SL(n,K)$. Добуток $\widetilde{\sigma}A$ одержується, якщо в матриці A зробити перестановку рядків: $\sigma(i)$-ий рядок замінити i-им рядком ($i = 1, \ldots, n$).

Вправа 3. Показати, що якщо σ — непарна підстановка, то

$$\mathrm{diag}[1,\ldots,1,-1,1,\ldots,1] \cdot \widetilde{\sigma} \in SL(n,K).$$

Вправа 4. Показати, що

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in SL(3,K).$$

Вправа 5. Нехай $\alpha \in K^*$. Показати, що тоді

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \in SL(2, K).$$

§19. Гомоморфізм Мінковського

Нехай m — натуральне число більше 1. Природній гомоморфізм

$$\mu_m : \mathbb{Z} \to \mathbb{Z}_m$$

кільця $\mathbb{Z}$ в кільце $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ класів лишків за модулем m продовжується до гомоморфізму

$$\mu_m : GL(n, \mathbb{Z}) \to GL(n, \mathbb{Z}_m)$$

груп. Цей гомоморфізм називається *гомоморфізмом Мінковського*. Введемо позначення

$$C(n, \mathbb{Z}, m) = \operatorname{Ker} \mu_m, \quad S(n, \mathbb{Z}, m) = SL(n, \mathbb{Z}) \cap C(n, \mathbb{Z}, m).$$

Група $C(n, \mathbb{Z}, m)$ називається *m-конгруенц-підгрупою* групи $GL(n, \mathbb{Z})$, а група $S(n, \mathbb{Z}, m)$ — *спеціальною m-конгруенц-підгрупою* групи $GL(n, \mathbb{Z})$. Відмітимо, що

$$C(n, \mathbb{Z}, m) = S(n, \mathbb{Z}, m), \quad (m > 2),$$

$$[C(n, \mathbb{Z}, 2) : S(n, \mathbb{Z}, 2)] = 2.$$

(При $m = 2$ всі діагональні матриці належать 2-конгруенц-підгрупі, але матриця $d(-1)$ не належить спеціальній 2-конгруенц-підгрупі).

Нехай $E(n, \mathbb{Z}, m)$ — нормальна підгрупа в групі $SL(n, \mathbb{Z})$, яка породжується всіма елементарними матрицями

$$t_{ij}(\lambda), \text{ де } \lambda \in m\mathbb{Z}.$$

Конгруенц-підгрупи будуть розглянуті в параграфі 20.

Теорема 19.1 (Мінковського). *Нехай $m > 2$. Тоді в m-конгруенц-підгрупі $C(n, \mathbb{Z}, m)$ нема елементів скінченного порядку (окрім одиничного).*

Доведення. Нехай це не так і в групі $C(n, \mathbb{Z}, m)$ існують неодиничні елементи скінченного порядку. Нехай серед таких елементів a — елемент простого порядку p : $a^p = E_n$. Матрицю a як елемент групи $C(n, \mathbb{Z}, m)$ можна представити у вигляді

$$a = E_n + m_1 b,$$

де
1) $m_1 \equiv 0 \pmod{m}$,
2) НСД ненульових елементів матриці b дорівнює 1.

Нехай $p = 2$. Тоді

$$E_n = a^2 = E_n + 2m_1 b + m_1^2 b^2,$$

звідки

$$2b + m_1 b^2 = 0.$$

Число 2 не може ділити m_1, бо $\frac{m_1}{2}$ (більше 1) не ділить b, тим більше, m_1 не ділить b. Отже, випадок $p = 2$ неможливий.

Нехай $p > 2$. За біномом Ньютона для комутуючих матриць отримаємо

$$pm_1 b + \frac{p(p-1)}{2} m_1^2 b^2 + \cdots + pm_1^{p-1} b^{p-1} + m_1^p b^p = 0,$$

звідки, після скорочення на m_1, одержимо, що p ділить m_1. Тоді всі члени суми зліва діляться на p^2, окрім першого доданка, який ділиться лише на p. Це неможливо. Одержані протиріччя показують, що в групі $C(n, \mathbb{Z}, m)$ нема елементів скінченного порядку. Теорема доведена.

Теорема 19.2. *Будь-яка періодична підгрупа групи $GL(n,\mathbb{Z})$ є скінченна.*

Теорема 19.3. *Будь-яка скінченна підгрупа групи $GL(n,\mathbb{Z})$ ізоморфна деякій підгрупі скінченної групи $GL(n,\mathbb{Z}_m)$ $(m>2)$.*

Доведення. Нехай H — періодична підгрупа в $GL(n,\mathbb{Z})$ і $m>2$. Тоді перетин $H\cap C(n,\mathbb{Z},m)$ буде одиничною групою. Маємо ізоморфізми

$$\mu_m(H)\cong (H\cdot C(n,\mathbb{Z},m))/C(n,\mathbb{Z},m)\cong H/H\cap C(n,\mathbb{Z},m)=H,$$

що доводить обидві теореми.

§20. Нормальні підгрупи групи $GL(n,\mathbb{Z})$

Будемо користуватись позначеннями §19 для m-конгруенц-підгруп $C(n,\mathbb{Z},m)$, $S(n,\mathbb{Z},m)$ і підгрупи $E(n,\mathbb{Z},m)$ $(m>1)$ групи $GL(n,\mathbb{Z})$. Для $m=1$ покладемо

$$C(n,\mathbb{Z},1)=GL(n,\mathbb{Z}),\quad S(n,\mathbb{Z},1)=E(n,\mathbb{Z},1)=SL(n,\mathbb{Z}).$$

В цьому параграфі будуть розглянуті такі результати.

Теорема 20.1 ([7]). *Нехай $n>2, H$ — нецентральна підгрупа в $GL(n,\mathbb{Z})$, яка нормалізується групою $SL(n,\mathbb{Z})$. Тоді для деякого натурального m група H містить спеціальну m-конгруенц-підгрупу $S(n,\mathbb{Z},m)$.*

Наступні дві теореми є наслідками теореми 20.1

Теорема 20.2. *Нехай $n>2$ і H — нецентральна нормальна підгрупа групи $GL(n,\mathbb{Z})$ або групи $SL(n,\mathbb{Z})$. Тоді H — підгрупа скінченного індекса.*

Теорема 20.3. *Нехай $n>2$ і H — підгрупа групи $SL(n,\mathbb{Z})$ скінченного індекса. Тоді для деякого натурального m група H містить спеціальну m-конгруенц-підгрупу $S(n,\mathbb{Z},m)$.*

Доведення цих теорем засновано на ряді лем, які взяті з [1] з деякими змінами. Зокрема будуть використані лема Басса для цілих чисел λ, μ (див. розділ 1) і така теорема Дедекінда про арифметичні прогресії.

Теорема 20.4 (Теорема Дедекінда). *Нехай a і d взаємно прості цілі числа. Тоді в арифметичній прогресії*

$$a_t=a+d(t-1)\quad (t=1,2,\dots,)$$

існує скільки завгодно простих чисел.

Автори наполегливо рекомендують зацікавленим читачам спочатку ознайомитись з вправами 1–5.

Лема 20.1. *Нехай $n>2$ і H — нецентральна підгрупа в $GL(n,\mathbb{Z})$, яка нормалізується спеціальною групою $SL(n,\mathbb{Z})$. Тоді група H містить групу $E(n,\mathbb{Z},m)$ для деякого натурального m.*

Доведення. Використовуючи вправи 1–5, неважко показати, що в групі H міститься деяка елементарна матриця

$$t_{rs}(\alpha)\quad (\alpha\in\mathbb{Z},\ \alpha\neq 0).$$

З леми Басса випливає, що

$$t_{ij}(\lambda\alpha)\in H$$

для будь-яких $i\neq j$ і $\lambda\in\mathbb{Z}$. Якщо елементарні матриці $t_1=t_{ij}(\alpha)$, $t_2=t_{ij}(\beta)$ належать H, то елементарна матриця $t_1^k t_2^s=t_{ij}(k\alpha+s\beta)$ $(k,\ s\in\mathbb{Z})$ також належить групі

H. Звідси слідує, що всі цілі числа α такі, що група H містить всі елементарні матриці з недіагональним елементом α, утворюють деякий ідеал $m\mathbb{Z}$, породжений натуральним числом m. Отже, група H містить підгрупу $E_1(n, \mathbb{Z}, m)$, яка породжується всіма елементарними матрицями, недіагональні елементи яких діляться на m. Так як H нормалізується $SL(n, \mathbb{Z})$, то група H містить групу $E(n, \mathbb{Z}, m)$. Лема доведена.

Для доведення теореми 20.1 досить довести рівність

$$E(n, \mathbb{Z}, m) = S(n, \mathbb{Z}, m) \quad (n > 2). \tag{1}$$

Перш за все відмітимо очевидне: матриця $a \in GL(n, \mathbb{Z})$ належить групі $S(n, \mathbb{Z}, m)$ тоді і тільки тоді, коли

1) всі недіагональні елементи матриці a діляться на m;
2) всі діагональні елементи в a порівняні з одиницею за модулем m;
3) $\det a = 1$.

В групі $S(n, \mathbb{Z}, m)$ визначимо відношення еквівалентності R, вважаючи aRb, якщо матриця b одержується з матриці a в результаті ряду таких перетворень:

1) додавання до рядка (стовпчика) іншого рядка (стовпчика), домноженого на число з ідеала $m\mathbb{Z}$;
2) спряженя матрицями з групи $SL(n, \mathbb{Z})$ (див. вправа 1 г)).

Лема 20.2. *Нехай $n > 2$. Для всякої матриці*

$$a = (\alpha_{ij}) \in S(n, \mathbb{Z}, m)$$

існує така матриця

$$b = \operatorname{diag}[c, 1], \quad c \in S(n-1, \mathbb{Z}, m),$$

що aRb.

Доведення. Можно вважати, що в матриці a всі елементи її першого стовпчика, починаючи з 3-го, рівні нулю, елементи α_{21}, α_{11} взаємно прості і $\alpha_{23} \neq 0$. Будемо додавати до другого рядка перший, домноженний на tm $(t = 1, 2, \ldots)$. Тоді в позиції (2,1) буде

$$\alpha'_{21} = \alpha_{21} + tm\alpha_{11} = (t\alpha_{11} + \alpha_{21}m^{-1})m,$$

де в дужках члени арифметичної прогресії з взаємно простими різницею і першим членом. В силу теореми Дедекінда в цій прогресії існує просте число, взаємно просте з α_{32}. Отже, можна вважати, що НСД$(\alpha_{21}, \alpha_{32} = m)$ і нехай u, v — такі цілі числа, що

$$u\alpha_{21} + v\alpha_{32} = m.$$

Припустимо, що $\alpha_{22} = 1 + rm$ і нехай $c = t_{12}(ru)t_{23}(-rv)$. Тоді в матриці $c^{-1}ac$ буде 1 на позиції (2, 2). Віднімемо від всіх рядків 2-ий, домножений на відповідні елементи 2-го стовчика. В результаті в 2-му стовпчику всі недіагональні елементи будуть нульовими. Аналогічні перетворення зробимо з стовпчиками. Переставивши рядкі і відповідні стовпчики, одержимо матрицю b. Лема доведена.

Наслідок 20.1. *Нехай $n > 3$. Якщо $S(n-1, \mathbb{Z}, m) = E(n-1, \mathbb{Z}, m)$, то $S(n, \mathbb{Z}, m) = E(n, \mathbb{Z}, m)$.*

Лема 20.3. *Нехай*

$$\nu : SL(3, \mathbb{Z}) \to SL(3, \mathbb{Z})/E(3, \mathbb{Z}, m)$$

— природній гомоморфізм. Тоді група $\nu(C(3, \mathbb{Z}, m))$ належить центру $\mathfrak{Z}(\operatorname{Im}\nu)$ групи $\operatorname{Im}\nu$.

Доведення. Так як

$$t_{12}(1) = [t_{13}(1),\ t_{32}(1)],\quad t_{21}(1) = [t_{23}(1),\ t_{31}(1)],$$

то група $SL(3,\mathbb{Z})$ породжується матрицями t_{ij}, де i або j рівно 3. Якщо $a, b \in SL(3,\mathbb{Z})$ і aRb, то $\nu(a) \in \mathfrak{Z}(\operatorname{Im}\nu)$ тоді і тільки тоді, коли $\nu(b) \in \mathfrak{Z}(\operatorname{Im}\nu)$. Нехай матриця

$$a = \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (\alpha\delta - \gamma\beta = 1)$$

належить групі $S(3,\mathbb{Z},m)$. Неважко перевірити, що всі комутатори

$$[a, t_{ij}], \quad i = 3 \quad \text{або} \quad j = 3,$$

належать групі $E(3,\mathbb{Z},m)$, що доводить лему.

Для матриці a (див. лема 20.3) введемо послідовність

$$a_k = \begin{pmatrix} \alpha & \beta^k & 0 \\ (-1)^{k+1}\gamma^k & \delta_k & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (k = 1, 2, \ldots),$$

де δ_k однозначно визначається з умови $\det a_k = 1$. Неважко бачити, що $a_k \in S(3,\mathbb{Z},m)$.

Лема 20.4. $\nu(a_k) = (\nu(a))^k$.

Доведення випливає з леми 20.3 і вправи 7.

Лема 20.5. *Нехай* $\beta^k \equiv \varepsilon \pmod{\alpha}$, *де* $\varepsilon = \pm 1$ *Тоді*

$$a^k \in E(3,\mathbb{Z},m).$$

Доведення. Нехай $\lambda = (\beta^k - \varepsilon)\alpha^{-1} + \varepsilon$. Так як β ділиться на m і НСД$(\alpha, m) = 1$, то λ ділиться на m. Тоді

$$a' = a_k t_{12}(-\lambda) = \begin{pmatrix} \alpha & -\varepsilon(\alpha-1) & 0 \\ \gamma' & \delta' & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Покладемо

$$a'' = t_{21}(-\varepsilon)a' t_{21}(\varepsilon) = \begin{pmatrix} 1 & \varepsilon(\alpha-1) & 0 \\ \gamma'' & \delta'' & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Легко бачити, що $a'' = t_{21}(\gamma'')t_{12}(\varepsilon(\alpha-1)) \in E(3,\mathbb{Z},m)$. Значить $a_k \in E(3,\mathbb{Z},m)$. А так як $\nu(a^k) = \nu(a_k)$, то $a^k \in E(3,\mathbb{Z},m)$. Лема доведена.

Лема 20.6. $S(3,\mathbb{Z},m) = E(3,\mathbb{Z},m)$.

Доведення. В силу леми 20.2 досить показати, що довільна матриця a (див. лему 20.3 і далі) з групи $S(3,\mathbb{Z},m)$ належить групі $E(3,\mathbb{Z},m)$. Нехай для $n_s \in \mathbb{Z}$

$$b_s = t_{21}^{-1}(n_s) a t_{21}(n_s) = \begin{pmatrix} \alpha + n_s\beta & \beta & 0 \\ \gamma' & \delta' & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Якщо $\alpha_s = \alpha + n_s\beta$ і k_s — таке ціле число, що $\beta^{k_s} \equiv \pm 1 \pmod{\alpha_s}$, то згідно леми 20.5 $b_s^{k_s} \in E(3,\mathbb{Z},m)$. Але $b_s^{k_s} = t_{21}^{-1}(n_s)a^{k_s}t_{21}(n_s)$. Отже, $a^{k_s} \in E(3,\mathbb{Z},m)$. Досить довести існування таких α_1, α_2, що відповідні k_1, k_2 будуть взаємно простими. Нехай

$3 < \alpha_1 = p$ — таке просте число, що $p \equiv -1 \pmod 4$ і p або $-p$ належить прогресії $\alpha + n\beta$ $(n \in \mathbb{Z})$ (див. вправу 8). Нехай k — показник, якому належить β за модулем p. В силу обмежень $p-1 = 2q_1^{r_1} \cdots q_u^{r_u}$. Показник k ділить $p-1$. Покладемо $k_1 = k$, якщо k — непарне і $k_1 = \frac{k}{2}$, якщо k — парне. Тоді $\beta^{k_1} \equiv \pm 1 \pmod p$. Нехай $v = \beta q_1 \cdots q_u$ і q, q' — такі прості числа, що $q \equiv -1 \pmod v$, $\quad q' \equiv -p \pmod v$ і k_2 — показник, якому належить β за модулем qq'. Тоді k_2 ділить число $(q-1)(q'-1)$. Жодне з простих чисел q_j не ділить це число. Отже, показники k_1, k_2 — взаємно прості і по одному із чисел $\pm p$ та $\pm qq'$ лежать у прогресії $\alpha + n\beta$ $(n \in \mathbb{Z})$. Лема доведена.

Теорема 20.1 випливає з леми 20.1, наслідку 20.1 і леми 20.6. Теорема 20.2 випливає з теореми 20.1 і скінченності групи $G_m = GL(n, \mathbb{Z}_m)$, $(G_1 = 1)$. Теорема 20.3 випливає з теореми 20.2 і вправи 9.

Теореми 20.1–20.3 невірні для $n = 2$. В групі $GL(2, \mathbb{Z})$ існують підгрупи скінченного індекса, які не містять жодної спеціальної конгруенц-підгрупи. Наведемо рузультат Райнера, що це підтверджує.

Нехай p — просте число і

$$\Gamma(p) = S(2, \mathbb{Z}, p)$$

— спеціальна p-конгруенц-підгрупа матриць порядку 2, $\Gamma'(p)$ — комутант групи $\Gamma(p)$. Нехай s — взаємно просте з p натуральне число, більше за одиницю і $\Omega(s, p)$ — підгрупа в $\Gamma(p)$, яка породжується комутантом $\Gamma'(p)$ і s-степенями X^s для всіх матриць $X \in \Gamma(p)$.

Теорема 20.5 (Райнера [12]). *Група $\Omega(s, p)$ є тією нормальною скінченного індекса підгрупою групи $GL(2, \mathbb{Z})$, яка не містить жодної нетривіальної спеціальної конгруенц-підгрупи групи $GL(2, \mathbb{Z})$.*

Нехай в вправах 1–5 H буде нецентральна підгрупа в $GL(n, \mathbb{Z})$, яка нормалізується групою $SL(n, \mathbb{Z})$ і $n > 2$. Відмітимо, якщо t — елементарна матриця і $a \in H$, то комутатор $[t, a]$ також належить H.

Вправа 1.

а) Нехай $g \in GL(n, \mathbb{Z})$. Група $H^g = g^{-1}Hg$ також нормалізується групой $SL(n, \mathbb{Z})$;

б) Відображення $h \to (h^{-1})^T$ $(h \in H)$ є ізоморфізм групи H на групу H^T транспонованих матриць, яка також нормалізується групою $SL(n, \mathbb{Z})$. В деяких доведеннях групу H можна замінити на H^g або H^T.

в) Якщо в матриці $h \in H$ поміняти місцями i-ий та j-ий рядки і i-ий та j-ий стовпчики, то одержана матриця $GL(n, \mathbb{Z})$-спряжена з h, а якщо додатково k-ий рядок або стовчик домножити на (-1), то одержиться матриця $SL(n, \mathbb{Z})$-спряжена з h.

г) Нехай $t = t_{ij}(\lambda), h \in H$. Матриця $t^{-1}ht$ одержується з матриці h, якщо від i-го рядка відняти, домножений на λ, j-ий рядок і потім до j-го стовпчика додати i-ий, домножений на λ.

Вправа 2. Нехай група H містить матрицю

$$a = \begin{pmatrix} E_r & b \\ 0 & E_{n-r} \end{pmatrix},$$

де b — ненульова матриця. Тоді H містить деяку елементарну матрицю.

Вправа 3. Нехай група H містить таку матрицю $a = (\alpha_{ij})$, що

$$\alpha_{31} = \ldots = \alpha_{n1} = 0, \quad \alpha_{12} \neq 0.$$

Тоді H містить елементарну матрицю.

Вправа 4. Група H не буде мономіальною.

Вправа 5. Нехай b така матриця із H, що не всі недіагональні елементи її першого стовпчика рівні нулю і нехай α — найбільший спільний дільник цих елементів. Тоді матриця b спряжена з матрицею a (див. вправу 3).

Розв'язання. Нехай α є НСД$(\alpha_{21}, \alpha_{31})$ і x, y такі цілі числа, що $x\alpha_{21} + y\alpha_{31} = 1$. Нехай

$$c = \begin{pmatrix} x & y \\ -\frac{\alpha_{31}}{\alpha} & \frac{\alpha_{21}}{\alpha} \end{pmatrix}.$$

Тоді c належить $SL(2, \mathbb{Z})$ і $c(\alpha_{21}, \alpha_{31})^T = (\alpha, 0)$. Далі провести індукцію за $n-1$ і розглянути спряженя з допомогою матриці $\mathrm{diag}[1, c_{n-1}]$.

Вправа 6. Нехай p — просте непарне число, $n > 2$. Розглянемо p-конгруенц-підгрупи в $GL(n, \mathbb{Z})$. Нехай $E_1(n, p)$ — підгрупа в $SL(n, \mathbb{Z})$, яка порджується всіма елементарними матрицями $t_{ij}(\lambda)$, з недіагональними елементами $\lambda \in \mathbb{Z}p$. Нехай

$$a = t_{21}(1)t_{12}(p)(t_{21}(1))^{-1} = \begin{pmatrix} 1-p & p & 0 \\ -p & 1+p & 0 \\ 0 & 0 & E_{n-2} \end{pmatrix}.$$

Довести, що матриця a не належить групі $E_1(n, p)$. Отже, група $E_1(n, p)$ не буде нормальною підгрупою групи $SL(n, \mathbb{Z})$.

Вправа 7. Використаємо позначення для матриці a_k, які введені після леми 20.3. Показати, що

$$a_{k+1} = c_2^{-1} t_{21}(\gamma') t_{31}(-\beta) t_{13}(-\gamma) a_k c_1^{-1} a c_1 t_{12}(-\beta^k) c_2,$$

де $c_2 = \mathrm{diag}[-1, 1, 1]\widetilde{(1\,3)}$, $\gamma' = (-1)^k\delta$, $c_1 = \widetilde{(1\,2\,3)}$.

Вправа 8. Нехай α, β — взаємно прості цілі числа і $\alpha + n\beta$ $(n \in \mathbb{Z})$ — відповідна арифметична прогресія. Довести існування простих чисел $p \equiv -1 \pmod 4$ таких, що p або $-p$ належить цій прогресії.

Вправа 9. Довести, що підгрупа скінченного індекса містить нормальну підгрупу також скінченного індекса.

Вказівка. Нехай A, B — підгрупи скінченного індекса в групі G. Індекс $(B : A \cap B)$ дорівнює числу тих суміжних класів за підгрупою A, які містяться в подвійному суміжному класі AB. Нехай $a_1, \ldots, a_s$ — повна система представників суміжних класів групи G за підгрупою A. Розглянути підгрупу $A^{a_1} \cap \cdots \cap A^{a_s}$.

§21. Силовські підгрупи групи $GL(n, \mathbb{Z})$

В цьому параграфі будуть доведені такі теореми.

Теорема 21.1 ([8]). *Силовські p-підгрупи групи $GL(n, \mathbb{Z})$ $(n > 1)$ спряжені в цій групі тоді і тільки тоді, коли виконується одна з умов:*
1) *$p > 2$, $n \leqslant p - 1$ і, якщо $n = p - 1$, то кільце $\mathbb{Z}[\varepsilon]$ $(\varepsilon^p = 1, \varepsilon \neq 1)$ буде кільцем головних ідеалів;*
2) *$p = 2$, $n = 2$.*

Теорема 21.2 ([9]). *Силовські p-підгрупи групи $GL(n, \mathbb{Z})$ $(n > 1)$ попарно ізоморфні тоді і тільки тоді, коли виконується одна з умов:*
1) *$p > 2$, $n < 3\ (p - 1)$;*
2) *$p = 2$, $n \leqslant 3$.*

Нагадаємо описання силовських p-підгруп групи $GL(n, \mathbb{Q})$ над полем раціональних чисел $\mathbb{Q}$. Нехай ε — первісний корінь степеня p із одиниці,

$$K = \mathbb{Z}[\varepsilon], \quad (K = \mathbb{Z} \text{ при } p = 2).$$

Нехай

$$P_p(K) = \langle \varepsilon \rangle \quad (P_p = \{1, -1\} \text{ при } p = 2)$$

— силовська p-підгрупа мультиплікативної групи кільця K;

$$W_0(P) = P = P_p(K), \quad W_j(P) = W_{j-1}(P) \wr C_p \quad (j = 1, 2, \ldots).$$

Група $W_j(P)$ буде єдиною з точністю до спряженості силовською p-підгрупою групи $GL(p^j, F)$, де $F = \mathbb{Q}(\varepsilon)$ — поле відношень кільця K. Окрім цього, група $W_j(P)$ незвідна над полем F і є силовською p-підгрупою групи $GL(p^j, K)$. Нехай

$$n = n_0 + n_1 p + \cdots + n_s p^s, \quad (0 \leqslant n_j < p,\ n_s \neq 0 \text{ при } s > 0)$$

— p-ічний розклад числа n. *Нехай*

$$G(P, n) = W_0(P)^{n_0} \times W_1(P)^{n_1} \times \cdots \times W_s(P)^{n_s}.$$

Тоді $G(P, n)$ — єдина з точністю до спряженості силовська p-підгрупа групи $GL(n, F)$. Група $G(P, n)$ є також силовською p-підгрупою групи $GL(n, K)$.

Нехай $\rho : F \to M(p-1, \mathbb{Q})$ — зображення елементів поля F матрицями порядку $p-1$ над полем $\mathbb{Q}$ (якщо $\alpha \in \mathbb{Q}$, то $\rho(\alpha) = \alpha E_{p-1}$, $\rho(\varepsilon) = \widetilde{\varepsilon}$ і т. д.). Будемо вважати, що це зображення продовжено на матриці над полем F.

Група

$$\rho(G(P, n)) = \rho(W_0(P)^{m_0}) \times \rho(W_1(P)^{n_1}) \times \cdots \times \rho(W_s(P)^{n_s})$$

— єдина з точністю до спряженості силовська p-підгрупа групи $GL((p-1)n, \mathbb{Q})$. Група $\rho(G(P, n))$ є також силовською p-підгрупою групи $GL((p-1)n, \mathbb{Z}$.)

Нехай

$$m = m_0 + (p-1)n, \quad 0 \leqslant m_0 < p - 1.$$

Тоді група

$$G = \langle 1 \rangle^{m_0} \times \rho(G(P, n))$$

є єдиною з точністю до спряженості силовською p-підгрупою групи $GL(m, \mathbb{Q}$.) Група G є також силовською p-підгрупою групи $GL(m, \mathbb{Z})$.

Відмітимо деякі властивості матричних груп над кільцем $\mathbb{Z}$. Скінченна підгрупа G в групі $GL(n, \mathbb{Z})$ є незвідна тоді і тільки тоді, коли G є незвідною підгрупою групи $GL(n, \mathbb{Q})$. Якщо G — скінченна підгрупа в $GL(n, \mathbb{Z})$, то група G є цілком звідною підгрупою групи $GL(n, \mathbb{Q})$, тобто група G спряжена в групі $GL(n, \mathbb{Q})$ з підпрямим добутком деяких незвідних підгруп $G_j \subset GL(n_j, \mathbb{Q})$, $(n_1 + \ldots + n_t = n, t \geq 1)$. Групи G_j визначаються групою G однозначно з точністю до спряженості над полем $\mathbb{Q}$. Назвемо групи G_j незвідними компонентами групи G. З описання силовських p-підгруп групи $GL(n, \mathbb{Q})$ випливає, що будь-яка p-підгрупа групи $GL(n, \mathbb{Z})$ є скінченною групою.

Лема 21.1. *Нехай H є незвідна силовська p-підгрупа групи $GL(d, \mathbb{Z})$. Тоді сплетіння $W(H) = H \wr C_p$ буде незвідною силовською p-підгрупою групи $GL(dp, \mathbb{Z})$.*

В розділі 2 є подібна лема 12.4, доведення леми 21.1 аналогічне.

Лема 21.2. *В умовах леми* 21.1 *група H^r $(1 \leqslant r < p)$ буде силовською p-підгрупою групи $GL(dr, \mathbb{Z})$.*

Доведення. Так як H — незвідна p-група, то центр $\mathfrak{Z}(H)$ цієї групи циклічний, а центр $\mathfrak{Z}(H^r)$ прямого добутку H^r буде прямим добутком $\mathfrak{Z}(H)^r$. Нижній шар[7] N групи $\mathfrak{Z}(H)^r$ буде елементарною абелевою групою порядку p^r. Нехай a — елемент порядку p в $\mathfrak{Z}(H)$ і $d_j = \operatorname{diag}[E_d, \ldots, a, \ldots, E_d]$ $(j = 1, \ldots, r)$ — базис групи N, де E_d — одинична матриця порядку d. Припустимо, що в групі $GL(dr, \mathbb{Z})$ існує p-елемент A, що нормалізує групу H^r. Тоді $A^{-1} N A = N$. Всі матриці d_j мають однаковий спектр[8],

[7] Нижній шар абелевої p-групи — підгрупа її елементів g, що задовольняють умову $g^p = e$.

[8] *Спектр* квадратної матриці — множина власних значень матриці з врахуванням кратності входження її елементів.

що відмінний від спектрів інших матриць з групи N. Це значить, що дія A індукує підстановку на матрицях d_j, а так як A — p-елемент, то ця підстановка тривіальна, тобто матриця A комутує з матрицями d_j. Це можливо лише коли $A \in (GL(d,\mathbb{Z}))^r$, а так як H — силовська група, то $A \in H^r$. Отже p-нормалізатор[9] групи H^r в групі $GL(dr,\mathbb{Z})$ суміщається з H^r. Лема доведена.

Лема 21.3. *Нехай G і H будуть силовськими p-підгрупами груп $GL(n,\mathbb{Z})$ і $GL(m,\mathbb{Z})$ відповідно. Якщо жодна незвідна компонента групи G не спряжена з незвідною компонентою групи H, то прямий добуток $G \times H$ буде силовською p-підгрупою групи $GL(n+m,\mathbb{Z})$.*

Доведення. Розглянемо такі два $\mathbb{Z}$-зображення групи $G \times H$:

$$\Gamma(\mathrm{diag}[g,h]) = g; \quad \Delta(\mathrm{diag}[g,h]) = h,$$

де $\mathrm{diag}[g,h] \in G \times H$ $(g \in G, h \in H)$. Очевидно, що $\mathrm{Im}\,\Gamma = G$, $\mathrm{Im}\,\Delta = H$. Далі, нехай деякий p-елемент

$$C = \begin{pmatrix} A & X \\ Y & B \end{pmatrix} \in GL(n+m,\mathbb{Z})$$

нормалізує групу $G \times H$ (A, B — квадратні матриці порядків n, m відповідно). Нехай φ — автоморфізм групи $G \times H$ такий, що

$$C^{-1}UC = \varphi(U) \quad (U \in G \times H).$$

Тоді

$$\Gamma(U)X = X(\Delta\varphi)(U).$$

Розглянемо розклади $\mathbb{Q}$-зображень Γ, $\Delta\varphi$ в суми незвідних зображень. З умови леми слідує, що жодне із незвідних зображень в розкладі Γ нееквівалентно якомусь незвідному зображенню в розкладі $\Delta\varphi$. З леми Шура випливає, що матриця X є нульова. Аналогічно, матриця Y є також нульовою. Тоді $C \in G \times H$. Лема доведена.

Нехай виконуються умови леми 21.1 і $n = n_0 + n_1 p + \cdots + n_s p^s$ — p-ічний розклад натурального числа n. Покладемо

$$W_0(H) = H, \quad W_j(H) = W_{j-1}(H) \wr C_p \quad (j = 1, \ldots),$$

$$G(H,n) = \prod_{j=0}^{s} (W_j(H))^{n_0}.$$

Твердження 21.1. *Група $W_j(H)$ буде незвідною силовською p-підгрупою групи $GL(dp^j,\mathbb{Z})$. Група $G(H,n)$ буде силовською p-підгрупою групи $GL(dn,\mathbb{Z})$. Нехай $0 < < d_0 < d$ і H_0 — силовська p-підгрупа групи $GL(d_0,\mathbb{Z})$. Тоді група $H_0 \times G(H,n)$ буде силовською p-підгрупою групи $GL(d_0+dn,\mathbb{Z})$.*

Доведення випливає з лем 21.1–21.3.

Для простого числа p введемо такі позначення.

$$d_p = \begin{cases} p, & \text{якщо} \quad p > 3; \\ 9, & \text{якщо} \quad p = 3; \\ 8, & \text{якщо} \quad p = 2; \end{cases}$$

$$V_p = \begin{cases} W_1(P_p(K)) = P_p(K) \wr C_p, & \text{якщо } p > 3; \\ W_2(P_3(K)) = (P_3(K) \wr C_3) \wr C_3, & \text{якщо } p = 3; \\ W_3(P_2) = ((P_2 \wr C_2) \wr C_2) \wr C_2, & \text{якщо } p = 2. \end{cases}$$

[9] *p-нормалізатор* p-підгрупи H в групі G — максимальна p-підгрупа групи $N_G(H)$, що містить H.

Група V_p є силовською p-підгрупою в групах $GL(d_p, F)$ і $GL(d_p, K)$.

Введемо в розгляд підгрупу групи V_p :

$$U_p = \begin{cases} V_p \cap SL(d_p, K), & \text{якщо } p > 3; \\ \text{підгрупа індекса 2 в } V_2, & \text{якщо } p = 2 \end{cases}$$

і, при цьому, $V_2 = \langle U_2, \mathrm{diag}[-1, 1, \ \ldots, \ 1] \rangle$.

Очевидно, $|V_p| = p|U_p|$.

Будемо вважати, що група V_p діє у вільному рангу d_p K-модулі L і всі матриці з групи V_p будуть матрицями відповідних операторів в базисі

$$e_1, \ldots, e_n \quad (n = d_p)$$

цього модуля.

Нехай M — K-підмодуль в L з базисом:

$$f_1 = \omega^2 e_1, \ f_2 = \omega(e_2 - e_1), \ \ldots, \ f_{n-1} = \omega(e_{n-1} - e_{n-2}),$$
$$f_n = e_1 + e_2 + \cdots + e_n,$$

де

$$\omega = \varepsilon - 1$$

— необоротний елемент кільця $K = \mathbb{Z}[\varepsilon]$. Відмітимо, що

$$\omega^{p-1} p^{-1} \in K^*,$$
$$\varepsilon^s - 1 \equiv s\omega \pmod{\omega^2} \quad (m \in \mathbb{Z})$$

в кільці K.

Лема 21.4. *K-модуль M є U_p-модуль, але не буде V_p-модулем.*

Доведення. Перш за все, відмітимо, що $\omega^2 L \subset M$, але ωL не міститься в M. Нехай

$$L_0 = \left\{ \sum_j \alpha_j e_j | (\alpha_j \in K), \ \sum_j \alpha_j \equiv 0 \pmod{\omega} \right\}.$$

Тоді $M = \omega L_0 + K f_n$. Неважко бачити, що K-модуль L_0 є V_p-простором. Якщо b — підстановочна матриця з V_p, то $b f_n = f_n$. Нехай

$$a = \mathrm{diag}[\varepsilon^{t_1}, \ldots, \varepsilon^{t_n}] \quad (t_j \in \mathbb{Z}).$$

Тоді

$$a f_n = \varepsilon^{t_1} e_1 + \cdots + \varepsilon^{t_n} e_n \equiv f_n + \omega(t_1 + \cdots + t_n) e_1 \pmod{L_0}$$

і $a f_n \in M$ тоді і тільки тоді, коли сума $t_1 + \cdots + t_n$ цілих чисел ділиться на ω, тобто коли ця сума ділиться на p, інакше кажучи, коли $a \in U_p$. Лема доведена.

Наслідок 21.1. *Нехай T — матриця переходу від K-базиса $\{e_j\}$ модуля L до K-базиса $\{f_j\}$ модуля M і*

$$\hat{U_p} = T^{-1} U_p T.$$

Тоді $\hat{U_p} \in GL(d_p, K)$, але група $T^{-1} V_p T$ не міститься в $GL(d_p, K)$.

Лема 21.5. *Група $\hat{U_p}$ буде незвідною силовською p-підгрупою групи $GL(d_p, K)$. Група $\rho(\hat{U_p})$ буде незвідною силовською p-підгрупою групи $GL((p-1)d_p, \mathbb{Z})$.*

Доведення. Нехай $X \in GL(d_p, K)$ така матриця, що

$$X^p \in \hat{U}_p, \quad X^{-1}\hat{U}_p X = \hat{U}_p.$$

Досить показати, що $X \in \hat{U}_p$. Нехай $Y = TXT^{-1}$. Тоді

$$Y^p \in U_p, \quad Y^{-1}U_p Y = U_p, \quad Y^{-1}Z^2(U_p)Y = Z^2(U_p).$$

Використовуючи вправи 1–4 параграфа 20, неважко впевнитись в тому, що матриця Y повинна належати групі V_p. Якщо це так, то матриця X належить групі $(T^{-1}V_pT) \cap GL(d_p, K) = \hat{U}_p$ (див. наслідок 21.1). Отже, $\hat{U}_p$ — силовська p-підгрупа групи $GL(d_p, K)$. Нехай G — та силовська p-підгрупа в $GL((p-1)d_p, \mathbb{Z})$, яка містить групу $\rho(\hat{U}_p)$. Неважко бачити, що $\mathfrak{Z}(G) = \mathfrak{Z}(\rho(\hat{U}_p))$. Звідси слідує, що $G = \rho(H)$, де H деяка p-підгрупа в $GL(d_p, K)$, яка містить $\hat{U}_p$, що можливо лише при $H = \hat{U}_p$. Отже, $G = \rho(\hat{U}_p)$, тобто, $\rho(\hat{U}_p)$ — силовська p-підгрупа групи $GL((p-1)d_p, \mathbb{Z})$. Лема доведена.

Твердження 21.2. *Покладемо в твердженні* 21.1 *відповідно*

$$d = (p-1)d_p, \quad H = \rho(V_p) \quad \textit{або} \quad H = \rho(\hat{U}_p), \quad 0 \leqslant d_0 < d.$$

Тоді групи

$$H_0 \times G(dn, \rho(V_p)) \quad i \quad H_0 \times G(dn, \rho(\hat{U}_p)$$

будуть силовськими p-підгрупами різних порядків в групі $GL(d_0 + dn, \mathbb{Z})$ (якщо $d_0 = 0$, то множник H_0 відсутній).

Таким чином, задача про ізоморфізм силовських p-підгруп в $GL(n, \mathbb{Z})$ зводиться до випадків: 1) $n < (p-1)p$, $p > 3$; 2) $p = 3$, $n < 18$; 3) $p = 2$, $n < 8$.

Лема 21.6. *Нехай $p > 3$, $n = n_0 + (p-1)t$ і $2 < t < p$. Тоді в групі $GL(n, \mathbb{Z})$ існують силовські p-підгрупи, які є елементарними абелевими групами порядків p^2 і p^t відповідно.*

Доведення. В групі $GL(n, \mathbb{Z})$ існує силовська p-підгрупа, яка є елементарною абелевою групою порядку p^t. Побудуємо в групі $GL(n, \mathbb{Z})$ силовську p-підгрупу, яка буде елементарною абелевою групою порядку p^2. Перш за все відмітимо, що група $P_p(K)^t$ є силовська p-підгрупа груп $GL(t, F), GL(t, K)$. Нехай $i_1, \ldots, i_t$ — попарно різні за модулем p цілі числа і Λ_s — p-підгрупа в $GL(s, K)$, яка породжується матрицями

$$A_s = \operatorname{diag}[\varepsilon, \ldots, \varepsilon], \quad B_s = \begin{pmatrix} \varepsilon^{i_1} & 1 & & 0 \\ & \varepsilon^{i_2} & \ddots & \\ & & \ddots & 1 \\ 0 & & & \varepsilon^{i_s} \end{pmatrix}.$$

Індукцією за s покажемо, що група Λ_s є силовська p-підгрупа групи $GL(s, K)$. Нехай C_s — такий елемент порядку p в $GL(t, K)$, що $C_sB_s = B_sC_s$. Очевидно, $C_2 \in \Lambda_2$. Нехай $2 \leqslant s < t$ і $C_s \in \Lambda_s$. Тоді існують такі цілі числа k і r, що

$$C_{s+1}A_{s+1}^k B_{s+1}^r = \begin{pmatrix} E_s & X \\ 0 & \varepsilon^j \end{pmatrix},$$

де $X^T = (x_1, \ldots, x_s) \quad (x_i \in K)$. З умови $C_{s+1}B_{s+1} = B_{s+1}C_{s+1}$ одержуємо рівняння для x_i:

$$(\varepsilon^{i_r} - \varepsilon^{i_{s+1}})x_r + x_{r+1} = 0 \quad (r = 1, \ldots, s-1), \quad (\varepsilon^{i_s} - \varepsilon^{i_{s+1}})x_s = 1 - \varepsilon^j.$$

Якщо j не дорівнює нулю за модулем p, то x_s — оборотний елемент кільця K. Але тоді x_{s-1} не належить кільцю K. Отже, $C_{s+1} \in \Lambda_{s+1}$. Це значить, що Λ_s — силовська підгрупа в $GL(s, K)$. Неважко бачити, що $\rho(\Lambda_t)$ — силовська p-підгрупа порядку p^2 в групі $GL((p-1)t, \mathbb{Z})$. Лема доведена.

Лема 21.7. *Нехай $p > 2$ і $n = n_0 + 2(p-1)$, $0 \leqslant n_0 < p-1$. Тоді будь-яка силовська p-підгрупа групи $GL(n, \mathbb{Z})$ є абелева група типу (p, p).*

Доведення. Нехай $H = \langle a \rangle$ — циклічна порядку p група і Γ не цілком звідне $\mathbb{Z}$-зображення цієї групи, степінь якого рівна $2(p-1)$. Як відомо [11], модуль M цього зображення є пряма сума $M = I \oplus V$ $\mathbb{Z}$-модулів, де I — деякий ідеал в кільці $K = \mathbb{Z}[\varepsilon]$ і V — вільний $\mathbb{Z}$-модуль з базисом $v_1, \ldots, v_{p-1}$. Оператор a діє в M за правилом:

$$a(\alpha) = \varepsilon\alpha \quad (\alpha \in I); \quad a(v_j) = v_j + \omega \quad (j = 1, \ \ldots, \ p-1),$$

де ω деякий елемент ідеала I. Визначимо новий оператор b в M :

$$b(\alpha) = \alpha \quad (\alpha \in I); \quad b(v_j) = v_{j+1} \quad (j = 1, \ \ldots, \ p-2),$$

$$b(v_{p-1}) = -v_1 - \cdots - v_{p-1} + p(\varepsilon - 1)^{-1}\omega.$$

Відмітимо, що $p(\varepsilon-1)^{-1} \in K$. Неважко перевірити, що $b^p = 1$ і $\quad ab = ba$. Це значить, що в групі $GL(2(p-1, \mathbb{Z}))$ нема циклічних силовських p-підгруп. Лема доведена.

Лема 21.8. *Нехай H — така силовська 2-підгрупа групи $GL(n, \mathbb{Z})$, що $\ker \mu_2|_H = \{E_n, -E_n\}$ (μ_2 — гомоморфізм Мінковського). Тоді група $W = H \wr C_2$ буде силовською 2-підгрупою групи $GL(2n, \mathbb{Z})$. Нехай $n > 1$, $1 \leqslant m < n$ і H_1 — силовська 2-підгрупа групи $GL(m, \mathbb{Z})$. Тоді група $V = H \times H_1$ буде силовською p-підгрупою групи $GL(n+m, \mathbb{Z})$.*

Доведення. Очевидно,

$$A = \ker \mu_2|_W = \langle d_1 = \operatorname{diag}[-E_n, E_n], d_2 = \operatorname{diag}[E_n, -E_n] \rangle .$$

Нехай C — матриця з 2-нормалізатора групи W в групі $GL(2n, \mathbb{Z})$. Тоді $C^{-1}AC = A$, $C^{-1}d_1C = d_1$ або d_2. Нехай b — матриця цикла (1 2), яка міститься в групі W. Матриця C або bC комутує з d_1. Можна вважати, що $d_1 = d_1C$. Тоді $C = \operatorname{diag}[C_1, C_2]$, де C_j — матриця з 2-нормалізатора групи H в групі $GL(n, \mathbb{Z},)$ який суміщається з групою H (нагадаємо, що H — силовська). Це значить, що $C \in W$. Отже, W — силовська підгрупа.

Нехай $B = \ker \mu_2|V$. Тоді

$$B = \{\operatorname{diag}[\pm E_n, h] | h \in \ker \mu_2|H_1\} \ \text{ і } \ a = \operatorname{diag}[-E_n, E_m] \in B.$$

Нехай X належить 2-нормалізатору групи V в групі $GL(n+m, \mathbb{Z})$ і $X^{-1}aX = a' = \operatorname{diag}[\pm E_n, h]$, де $h \in \ker \mu_2|H_1$. Тоді

$$-n + m = \pm n + \operatorname{tr} h.$$

Так як $n > m$, то $\operatorname{tr} h = m$ і тоді $h = e, a' = a$, звідки слідує, що $X \in V$. Це закінчує доведення леми.

Введемо в розгляд 2-підгрупу в $GL(3, \mathbb{Z})$:

$$\Gamma_3 = \left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle .$$

Група Γ_3 спряжена в $GL(3,\mathbb{Q})$ з групою $P_2 \times (P_2 \wr C_2)$ — силовською 2-підгрупою групи $GL(3,\mathbb{Q})$.

Покладемо в лемі 21.8 $H = \Gamma_3$. Одержимо:

1) $\Gamma_4 = P_2 \times \Gamma_3$ — силовська 2-підгрупа групи $GL(4,\mathbb{Z})$;
2) $\Gamma_5 = W(P_2) \times \Gamma_3$ — силовська 2-підгрупа групи $GL(5,\mathbb{Z})$;
3) $\Gamma_6 = W(\Gamma_3) = \Gamma_3 \wr C_2$ — силовська 2-підгрупа групи $GL(6,\mathbb{Z})$.

Окрім цього, група $\Gamma_7 = P_2 \times \Gamma_6$ буде силовською 2-підгрупою групи $GL(7,\mathbb{Z})$. Дійсно, в групі Γ_7 існує тільки одна матриця a, така, що $\operatorname{tr} a = 5$. Це $a = \operatorname{diag}[-1, E]$. Тоді будь-яка матриця C, нормалізуюча групу Γ_7, комутує з матрицею a. Звідси неважко одержати, що група Γ_7 суміщається з своїм 2-нормалізатором в групі $GL(7,\mathbb{Z})$.

Лема 21.9. *Нехай $4 \leqslant n \leqslant 7$. В групі $GL(n,\mathbb{Z})$ існує пара $H_1(n), H_2(n)$ силовських 2-підгруп різних порядків. Ці пари наведені в таблиці.*

$GL(n,\mathbb{Z})$	$H_1(n)$	$H_2(n)$	$\lvert H_1(n)\rvert$	$\lvert H_2(n)\rvert$
$GL(4,\mathbb{Z})$	Γ_4	$W_2(P_2) = (P_2 \wr C_2) \wr C_2$	2^5	2^7
$GL(5,\mathbb{Z})$	Γ_5	$P_2 \times W_2(P_2)$	2^7	2^8
$GL(6,\mathbb{Z})$	Γ_6	$W(P_2) \times W_2(P_2)$	2^9	2^{10}
$GL(7,\mathbb{Z})$	Γ_7	$P_2 \times W(P_2) \times W_2(P_2)$	2^{10}	2^{11}

Для доведення досить відмітити, що група $H_2(n)$ є силовська 2-підгрупа групи $GL(n,\mathbb{Q})$.

Група $\widetilde{P_p} = \rho(P_p(K))$ породжується матрицею $\rho(\varepsilon) = \widetilde{\varepsilon}$, $\varepsilon^p = 1$, $\varepsilon \neq 1$.

Введемо в розгляд групу

$$\Delta_p = \left\langle a = \begin{pmatrix} \widetilde{\varepsilon} & 0 \\ 0 & \widetilde{\varepsilon} \end{pmatrix},\ b = \begin{pmatrix} \widetilde{\varepsilon} & E_{p-1} \\ 0 & E_{p-1} \end{pmatrix} \right\rangle.$$

Група Δ_p — нерозкладна p-підгрупа в $GL(2(p-1),\mathbb{Z})$ і разом з цілком звідною групою $(\widetilde{P_p})^2$ утворюють пару неспряжених силовських p-підгруп групи $GL(2(p-1),\mathbb{Z})$.

Лема 21.10.

1) *Група $\Delta_3 \times \Delta_3$ є силовська 3-підгрупа групи $GL(8,\mathbb{Z})$;*
2) *Група $\Delta_3 \times \Delta_3 \times \widetilde{P_3}$ буде силовською 3-підгрупою групи $GL(10,\mathbb{Z})$;*
3) *Група $\Delta_3 \times \widetilde{P_3}$ є силовська 3-підгрупа групи $GL(6,\mathbb{Z})$.*

Доведення. 1) Нехай

$$a_1 = \operatorname{diag}[a, E_4],\ a_2 = \operatorname{diag}[E_4, a],\ a_3 = \operatorname{diag}[b, E_4],\ a_4 = [E_4, b].$$

Групи

$$A_1 = \langle a_1, a_2 \rangle,\ A_2 = \langle a_1 a_3, a_2 \rangle,\ A_3 = \langle a_1, a_2 a_2 a_4 \rangle,\ A_4 = \langle a_1 a_3, a_2 a_4 \rangle$$

утворюють повний список максимальних цілком звідних підгруп в групі $G = \Delta_3 \times \Delta_3$. Нехай $X \in N(G)$ — 3-нормалізатору групи G в групі $GL(8,\mathbb{Z})$ і $\tau(g) = X^{-1} g X g \in G$. Тоді

$$\tau(\{A_1, A_2, A_3, A_4\}) = \{A_1, A_2, A_3, A_4\}.$$

Так як τ — 3-елемент, то існує група $A \in \{A_1, A_2, A_3, A_4\}$ така, що $\tau(A) = A$. Окрім цього, τ зберігає власні значення матриць. Це все можливо тільки в тому випадку, коли τ — одиничний автоморфізм групи A. При цій умові неважко впевнитись в тому, що $X = \operatorname{diag}[X_1, X_2]$, де X_j належить 3-нормалізатору групи Δ_3, тобто $X \in G$.

2) Матриця $C = \operatorname{diag}[E_8, \widetilde{\varepsilon}]$ породжує в $G \times \widetilde{P_3}$ єдину цілком звідну підгрупу, що має тільки одну нетривіальну незвідну компоненту $\widetilde{P_3}$. Використавши цю властивість неважко показати, що група $G \times \widetilde{P_3}$ суміщається зі своїм 3-нормалізатором в групі $GL(10,\mathbb{Z})$.

Доведення 3) аналогічно 2). Слід лише розглянути матрицю $C_1 = \operatorname{diag}[E_4, \widetilde{\varepsilon}]$.

Лема 21.11. *Нехай $6 \leqslant n < 18$. В групі $GL(n,\mathbb{Z})$ існує пара $G_1(n), G_(n)$ силовських 3-підгруп різних порядків. Ці пари наведені в таблиці.*

$GL(n,\mathbb{Z})$	$G_1(n)$	$G_2(n)$	$\lvert G_1(n)\rvert$	$\lvert G_2(n)\rvert$
$GL(6,\mathbb{Z})$	$\Delta_3 \times \widetilde{P_3}$	$W(\widetilde{P_3})$	3^3	3^4
$GL(8,\mathbb{Z})$	$\Delta_3 \times \Delta_3$	$\widetilde{P_3} \times W(\widetilde{P_3})$	3^4	3^5
$GL(10,\mathbb{Z})$	$\Delta_3 \times \Delta_3 \times \widetilde{P_3}$	$(\widetilde{P_3})^2 \times W(\widetilde{P_3})$	3^5	3^6
$GL(k+1,\mathbb{Z})$ $(k = 6,8,10)$	$G_1(k) \times \langle 1\rangle$	$G_2 \times \langle 1\rangle$		
$GL(k+6,\mathbb{Z})$ $(6 \leqslant k \leqslant 11)$	$G_1(k) \times \widetilde{P_3}$	$G_2(k) \times \widetilde{P_3}$		

Доведення випливає з леми 21.11, леми 21.3 та описання силовських 3-підгруп в групі $GL(\mathbb{Q})$. Відмітимо, що групи $G_2(n)$ будуть силовськими над полем $\mathbb{Q}$.

Доведення теореми 21.2 випливає з твердження 21.2, лем 21.6, 21.7, 21.9, 21.11.

Доведення теореми 21.1. В силу теореми 21.2, доведення зводиться до розгляду силовських p-підгруп в групі $GL(n,\mathbb{Z})$ $(n > 1)$ в наступних 4-х випадках:
1) $p > 2$, $2(p-1) \leqslant n < 3(p-1)$;
2) $p > 2$, $p-1 < n < 2(p-1)$;
3) $p > 2$, $n = p-1$;
4) $p = 2$, $n = 2$ або $n = 3$.

Відмітимо, що в усіх інших випадках для простого числа p і натурального числа n силовські p-підгрупи групи $GL(n,\mathbb{Z})$ не спряжені в цій групі.

1) Як уже відмічалось, група Δ_p є звідною, але нерозкладною підгрупою групи $GL(2(p-1),\mathbb{Z})$. Разом з цілком звідною групою $\widetilde{P_p}^2 = \widetilde{P_p} \times \widetilde{P_p}$ група Δ_p складають пару силовських p-підгруп в групі $GL(2(p-1),\mathbb{Z})$, які не спряжені в цій групі. Домножуючи ці підгрупи на $\langle 1\rangle^k$ $(1 \leqslant k < p-1)$, одержимо пару $\Delta_p \times \langle 1\rangle^k$ і $\widetilde{P_p}^2 \times \langle 1\rangle^k$ силовських підгруп в групі $GL(k+2(p-1),\mathbb{Z})$, не спряжених в цій групі.

2) Нехай

$$a = \begin{pmatrix} \widetilde{\varepsilon} & A \\ 0 & 1 \end{pmatrix}, \quad A^T = (1,0,\ldots,0).$$

Неважко показати, що група $\langle a\rangle$ є звідною і нерозкладною підгрупою порядку p в групі $GL(p,\mathbb{Z})$. Разом з цілком звідною групою $\widetilde{P_p} \times \langle 1\rangle$ група $\langle a\rangle$ складають пару силовських p-підгруп в групі $GL(p,\mathbb{Z})$, не спряжених в цій групі. Домножуючи ці підгрупи на $\langle 1\rangle^k$ $(1 \leqslant k < p-1)$, одержимо пару силовських p-підгруп в групі $GL(k+p,\mathbb{Z})$, не спряжених в цій групі.

3) Нехай $H = \langle a\rangle$ — циклічна група порядку p. Будь-яка p-підгрупа групи $GL(p-1,\mathbb{Z})$ ізоморфна групі H. Кільце K і будь-який ідеал U цього кільця буде $\mathbb{Z}H$-модулем, якщо дію оператора a визначити так:

$$a(\alpha) = \varepsilon\alpha \quad (\alpha \in K).$$

Нехай Γ_U — $\mathbb{Z}$-зображення групи H, модуль якого є ідеал U. Тоді будь-яка p-підгрупа в $GL(p-1,\mathbb{Z})$ буде спряжена з групою $\langle \Gamma_U(a)\rangle$ для деякого ідеала $U \subseteq K$. Зображення Γ_U, Γ_V (V — ідеал) еквівалентні тоді і тільки тоді, коли ідеали U, V лежать в одному класі ідеалів (тобто $V = U\omega$ для деякого елемента $\omega \in K$.) Отже, якщо K — кільце головних ідеалів, то всі p-підгрупи групи $GL(p-1,\mathbb{Z})$ спряжені в цій групі.

Нехай кільце K містить неголовний ідеал U, але групи $\langle \Gamma_K(a)\rangle$ і $\langle \Gamma_U(a)\rangle$ спряжені в групі $GL(p-1,\mathbb{Z})$, тобто

$$C^{-1}\Gamma_U(a)C = \Gamma_K(\sigma(a))$$

для деякої матриці $C \in GL(p-1,\mathbb{Z})$ і деякого автоморфізма σ групи H. Зображення Γ_K і $\Gamma_K\sigma$ еквівалентні над кільцем $\mathbb{Z}$ (див. вправу 6). Тоді ідеали U та K лежать в одному класі: $U = K\omega$, що протирічить вибору ідеала U. Отже, групи $\langle\Gamma_K(a)\rangle$ і $\langle\Gamma_U(a)\rangle$ не спряжені в групі $GL(p-1,\mathbb{Z})$.

4) Нехай $p = 2$. Випадок $n = 2$ розглятуто в вправі 5. Нехай $n = 3$. Тоді нерозкладна група Γ_3 разом з цілком звідною групою $W(P_2) \times P_2$ утворюють пару силовських 2-підгруп групи $GL(3,\mathbb{Z},)$ не спряжених в цій групі. Теорема 21.1 доведена.

Дамо авторське доведення теореми 21.1 (ця терема доведена значно раніше теореми 21.2), засноване на теорії цілочислових зображень скінченних груп. Відмітимо, що будь-яка p-підгрупа групи $GL(n,\mathbb{Z})$ є скінченна і скінченна підгрупа групи $GL(n,\mathbb{Z})$ буде незвідна в $GL(n,\mathbb{Z})$ тоді і тільки тоді, коли ця підгрупа є незвідна в групі $GL(n,\mathbb{Q})$. Нехай силовська p-підгрупа G в групі $GL(n,\mathbb{Z})$ буде силовською і в групі $GL(n,\mathbb{Q})$. Розглянемо спочатку випадок звідної групи G. В цьому випадку група G є прямим добутком

$$G = G_1 \times G_2 \times G_3,$$

де G_1, G_2 — незвідні групи і хоча би одна з них неодинична, G_3 — прямий добуток незвідних груп або група G_3 відсутня. Нехай

$$g = \mathrm{diag}[g_1, g_2, g_3] \quad (g_j \in G_j)$$

довільний елемент групи G. Розглянемо два відображення Δ_j $(j = 1, 2)$ такі, що

$$\Delta_j(g) = g_j \quad (g \in G).$$

Тоді Δ_j $(j = 1, 2)$ два незвідних $\mathbb{Z}$-зображення групи G, нееквівалентних над полем $\mathbb{Q}$. З теорії цілочислових зображень випливає існування $\mathbb{Z}$-зображення Δ групи G, яке має вигляд

$$\Delta : g = \mathrm{diag}[g_1, g_2, g_3] \to \begin{pmatrix} \Delta_(g) & * \\ 0 & \Delta_2(g) \end{pmatrix} \quad (g \in G)$$

і яке є нерозкладним навіть над кільцем цілих p-адичних чисел. Тоді підгрупа $\overline{G} = \Delta(G) \times G_3$ групи $GL(n,\mathbb{Z}))$ не розкладається в прямий добуток незвідних підгруп цієї групи, але в групі $GL(n,\mathbb{Q})$ ця підгрупа спряжена з цілком звідною групою G. Отже, групи G і $\overline{G}$ будуть неспряженими силовськими p-підгрупами групи $GL(n,\mathbb{Z})$.

Нехай тепер G — незвідна силовська p-підгрупа групи $GL(n,\mathbb{Z})$. Тоді $n = (p-1)p^r$. Розглянемо випадки $r > 0$ $(p > 2)$ і $r > 1$ $(p = 2)$. Скористаємось теоремами 15.2 (для $p > 2$) і 17.3 (для $p = 2$). Тоді

$$G = W_r(\rho(P_p)) = \rho(W_r(P_p)),$$

де P_p — силовська p-підгрупа в K^* $(K = \mathbb{Q}(\varepsilon))$, $\varepsilon^p = 1$). Нехай далі H — силовська p-підгрупа в $GL(n,\mathbb{Z})$, яка містить в своєму центрі матрицю $a = \rho(\mathrm{diag}[\varepsilon, \ldots, \varepsilon])$. Тоді $H = \varrho(H_1)$, де H_1 — p-підгрупа в групі $GL(p^r, K)$. Якщо групи G і H спряжені над кільцем $\mathbb{Z}$, то групи $W_r(P_p)$ і H_1 будуть спряжені над кільцем K. Розглянемо гомоморфізм Мінковського

$$\mu : GL(n,K) \to GL(n, K/K\omega),\ \omega = \varepsilon - 1.$$

Тоді група $\overline{W_r} = \mu(W_r(P_P))$ складається із матриць підстановок, кожна з яких є добутком циклів довжини p^s $(0 \leqslant s \leqslant r)$. Нормальні форми таких матриць є суми кліток Жордана $J_{p^s}(1)$. Нехай $p > 2$ і

$$a = \begin{pmatrix} \varepsilon & 1 \\ 0 & 1 \end{pmatrix}$$

або $p = 2$ і

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

Очевидно, $\mu(a) = J_2(1)$, а матриця $\mu(b)$подібна $J_3(1)$. Отже, матриця $\mathrm{diag}[a, 1, \ldots, 1]$ (або $\mathrm{diag}[b, 1, \ldots, 1]$) не подібна жодній матриці в групі $\overline{W_r}$, тобто групи $\overline{W_r}$ і $\mu(H_1)$ не будуть спряженими над полем $K/K\omega$. Таким чином, в розглянутому випадку силовські p-підгрупи в $GL(n, \mathbb{Z})$ не спряжені в цій групі. Інші випадки розглядаються так як в першому доведенні. П. М. Гудивок і О. А. Кирилюк [13–14] досліджували питання про спряженість силовських p-підгруп повної лінійної групи над дискретно нормованими кільцями.

Нехай R — кільце головних ідеалів характеристики нуль і просте число p необоротне в R. П. М. Гудивок, В. П. Рудько і Н. В. Юрченко [15] знайшли критерії ізоморфізму і спряженості силовських p-підгруп групи $GL(n, R)$. Відмітимо, що будь-яка p-підгрупа в групі $GL(n, R)$ є скінченна.

Крім того, був одержаний такий результат.

Теорема 21.3 ([16]). *Нехай S — кільце всіх цілих алгебраїчних чисел. Тоді в групі $GL(n, S)$ $(n > 1)$ для будь-якого простого p існує нескінченно багато неізоморфних силовських p-підгруп.*

Нехай $\mathfrak{Z}(G)$ — центр групи G (перший центр). *Другий центр* $\mathfrak{Z}^2(G)$ — це така підгрупа в G, що

$$\mathfrak{Z}^2(G)/\mathfrak{Z}(G) = \mathfrak{Z}(G/\mathfrak{Z}(G)).$$

Вправа 1. Нехай

$$P_2 = \{1, -1\},\ C_2 = \langle (12) \rangle,\ W_1(P_2) = P_2 \wr C_2,$$

$$W_2(P_2) = W_1(P_2) \wr C_2 \ \text{ і } \ H = SL(4, \mathbb{Z}) \cap W_2(P_2).$$

Показаити, що $\mathfrak{Z}^2(H)$ — елементарна абелева група порядку 8.

Вправа 2. Нехай

$$W_3(P_2) = W_2(P_2) \wr C_2 \ \text{ і } \ U = SL(8, \mathbb{Z}) \cap W_3(P_2).$$

Показати, що

$$\mathfrak{Z}^2(U) = \langle -E_8, \mathrm{diag}[-E_4, E_4] \rangle.$$

Вправа 3. Нехай

$$K = \mathbb{Z}[\varepsilon],\ \varepsilon^3 = 1,\ \varepsilon \neq 1,\ P_3 = \langle \varepsilon \rangle,\ C_3 = \langle (123) \rangle,\ W_1(P_3) = P_3 \wr C_3.$$

а) Показати, що якщо $H = SL(3, K) \cap W_1(P_3)$, то $H \cong UT(3, 3)$ і $\mathfrak{Z}^2(H) = H$.

б) Показати, що незвідні силовські 3-підгрупи групи $GL(3, K)$ з точністю до спряженості вичерпуються трьома групами

$$T_j^{-1} W_1(P_3) T_j (j = 0, 1, 2),$$

де $T_0 = E_3$,

$$T_1 = \begin{pmatrix} \omega & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix},\ T_2 = \begin{pmatrix} \omega & 0 & 1 \\ 0 & \omega & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad (\omega = \varepsilon - 1).$$

в) Нехай

$$W_2(P_3) = W_1(P_3) \wr C_3 \ \text{ і } \ H = SL(9, K) \cap W_3(P_3).$$

Показати, що

$$\mathfrak{Z}^2(H) = \left\langle \varepsilon E_9, \operatorname{diag}[E_3, \varepsilon E_3, \varepsilon^2 E_3] \right\rangle .$$

Вправа 4. Нехай

$$p > 3,\ P_p = \{\varepsilon\},\ \varepsilon^p = 1,\ \varepsilon \neq 1,$$

$$W(P_p) = P_p \wr C_p,\ C_p = \langle\ (12\dots p)\rangle \quad \text{і} \quad H = SL(p, K) \cap W(P_p).$$

Показати, що

$$Z^2(H) = \left\langle \varepsilon E_p, \operatorname{diag}[1, \varepsilon, \dots, \varepsilon^{p-1}] \right\rangle .$$

Вправа 5. Показати, що будь-яка силовська 2-підгрупа групи $GL(2, \mathbb{Z})$ спряжена в цій групі з групою $P_2 \wr C_2$ (діедра порядку 8).

Вправа 6. Нехай $H = \langle a \rangle$ — циклічна група порядку n, ξ — первісний корінь степеня n із одиниці і $K = \mathbb{Z}[\xi]$. Кільце K буде $\mathbb{Z}H$-модулем з такою дією :

$$a(\alpha) = \xi\alpha \quad (\alpha \in K).$$

Нехай Γ $\mathbb{Z}$-зображення групи H, модуль якого є кільце K. Довести, що якщо σ — автоморфізм групи H, то зображення Γ і $\Gamma\sigma$ еквівалентні над кільцем $\mathbb{Z}$.

§22. Силовські p-підгрупи повної лінійної групи над комутативним кільцем характеристики p^s

Розглянемо спочатку властивості унітрикутної підгрупи $UT(n, K)$ повної лінійної групи $GL(n, K)$ над довільним комутативним кільцем K з одиницею характеристики p^s ($s \in \mathbb{N}$), тобто підгрупа всіх трикутних матриць з одиницями на діагоналі. Будемо позначати через $A \circ B$ *приєднаний добуток* $A + B + AB$ квадратних матриць A і B однакових порядків, $T_0(n, K)$ — множину верхніх трикутних матриць порядку n над кільцем K з нулями на діагоналі.

Лема 22.1. *Нехай A — деяка квадратна матриця порядку $n > 1$ над кільцем K. Якщо $\det(A \circ B) = 0$ для всякої матриці B із $T_0(n, K)$, то $\det(A + B) = 0$ для всякої матриці B із $T_0(n, K)$.*

Доведення. Нехай B — довільна матриця із $T_0(n, K)$. 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 $B' = (E_n - B)^{-1} - E_n \in T_0(n, K)$. Оскільки $\det(A \circ B') = 0$, то

$$\det(A + B) = \det\left(A + E_n - (E_n - B)\right) =$$

$$= \det\left(\left(A(E_n - B)^{-1} + (E_n - B)^{-1} - E_n\right)(E_n - B)\right) =$$

$$= \det\left((A(E_n + B') + B')(E_n - B)\right) =$$

$$= \det\left((A + B' + AB')(E_n - B)\right) = \det(A \circ B') \det(E_n - B) = 0.$$

Лема доведена.

Неважко довести такі дві леми.

Лема 22.2. *Нехай $A = (a_{ij})$ — деяка матриця порядку $n > 1$ над кільцем K. Якщо $\det(A \circ B) = 0$ для всякої матриці B із $T_0(n, K)$, то $a_{n1} = 0$.*

Лема 22.3. *Нехай P — деяка підгрупа групи $GL(n, K)$ ($n \in \mathbb{N}$, $n > 1$). Якщо у всіх матриць 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 матриці A порядку n над кільцем K такої, що $E_n + A \in P$.*

Далі через K^* будемо позначати мультиплікативну групу кільця K, $\operatorname{rad} K$ — первісний радикал кільця K, який у комутативному випадку складається з усіх нільпотентих елементів кільця K.

Теорема 22.1 ([10]). *Нехай K є комутативним кільцем характеристики p, $\operatorname{rad} K = \{0\}$, $n \in \mathbb{N}$. Група $UT(n, K)$ є силовською p-підгрупою групи $GL(n, K)$.*

Доведення. Легко бачити, що $UT(n, K)$ є p-підгрупою групи $GL(n, K)$. Припустимо, P — деяка p-підгрупа групи $GL(n, K)$, що містить групу $UT(n, K)$ і покажемо, що $P = UT(n, K)$. Нехай $n > 1$. Доведемо спочатку, що у всіх матриць з групи P елемент у позиції $(n, 1)$ рівний нулю. Дійсно, нехай A' — довільна матриця з групи P, $A = A' - E_n$, B — довільна матриця з $T_0(n, K)$. Тоді $E_n + A \in P$, $E_n + B \in UT(n, K)$. Таким чином, 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 $\det(A \circ B) \in \operatorname{rad} K$. Тому $\det(A \circ B) = 0$. За лемою 22.2 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 з групи P елемент у позиції $(i, 1)$ рівний нулю $(i = k + 1, \ldots, n)$. 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 $T_0(n, K)$. Тоді $E_n + A \in P$, $E_n + B \in UT(n, K)$. Звідси одержимо, що $E_n + A \circ B \in P$, матриця $A \circ B$ нільпотентна. За лемою 22.3 елемент матриці $(B \circ A)^r$ у позиції $(i, 1)$ рівний нулю $(i = k+1, \ldots, n$; $r \in \mathbb{N})$.

Позначимо через $M(C)$ матрицю, утворену з квадратної матриці C порядку n над кільцем K відкиданням останніх $n - k$ рядків і останніх $n - k$ стовпців. Очевидно, у матриць $M\left((A \circ B)^m\right)$ і $\left(M(A \circ B)\right)^m$ однакові перші стовпці при будь-якому натуральному числу m.

Оскільки матриця $A \circ B$ нільпотентна, то для досить великого m перший стовпець матриці $(M(A \circ B))^m$, рівний нулю. Звідси $\left(\det M(A \circ B)\right)^m = \det\left(M(A \circ B)\right)^m = 0$. Тому $\det(M(A \circ B)) \in \operatorname{rad} K$. Отже, $\det M(A \circ B) = 0$. Легко бачити, що $M(A + B + AB) = M(A) + M(B) + M(AB)$. Так як $B \in T_0(n, K)$, 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 $T_0(k, K)$. Очевидно, знайдеться така матриця $B_1 \in T_0(n, K)$, що $B' = M(B_1)$. Тоді $\det\left(M(A) \circ B'\right) = \det\left(M(A) \circ M(B_1)\right) = 0$. За лемою 22.2 елемент матриці $M(A)$ у позиції $(k, 1)$ рівний нулю, тому рівний нулю і елемент матриці A і $A' = E_n + A$ у позиції $(k, 1)$. Отже, у будь-якої 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, в такому разі, p-елементом кільця K і через це він рівний 1.

Нескладною індукцією по n можна показати, що всі матриці з P містяться в $UT(n, K)$. Тому $UT(n, K)$ є силовською p-підгрупою групи $GL(n, K)$. Теорема доведена.

Далі через $\widetilde{z} = z + \operatorname{rad} K$ будемо позначати елемент фактор–кільця $K/\operatorname{rad} K$ кільця K, де $z \in K$, $\widetilde{T} = \|t_{ij} + \operatorname{rad} K\|$ — матрицю над фактор–кільцем $K/\operatorname{rad} K$ кільця K, де $T = \|t_{ij}\|$ — деяка матриця над кільцем K. Неважко встановити зв'язок між p-підгрупами групи $GL(n, K)$ та — групи $GL(n, K/\operatorname{rad} K)$

Теорема 22.2 ([10]). *Нехай K — комутативне кільце характеристики p^s, $n \in \mathbb{N}$. $\varphi\colon X \to \widetilde{X}$ є гомоморфним відображенням групи $GL(n, K)$ на групу $GL(n, K/\operatorname{rad} K)$. При цьому відображенні повний прообраз будь-якої силовської p-підгрупи групи $GL(n, K/\operatorname{rad} K)$ є силовською p-підгрупою групи $GL(n, K)$ і, навпаки, будь-яка силовська p-підгрупа групи $GL(n, K)$ є повним прообразом деякої силовської p-підгрупи групи $GL(n, K/\operatorname{rad} K)$. Дві силовські p-підгрупи групи $GL(n, K)$ спряжені тоді і*

тільки тоді, коли їх образи при гомоморфізмі φ є спряженими силовськими p-підгрупами групи $GL(n,\, K/\operatorname{rad} K)$.

Безпосередньо з теореми одержуємо такий наслідок.

Наслідок 22.1. *Нехай K — комутативне кільце характеристики p^s, $n \in \mathbb{N}$. Силовські p-підгрупи групи $GL(n, K)$ попарно спряжені тоді і тільки тоді, коли силовські p-підгрупи групи $GL(n, K/\operatorname{rad} K)$ попарно спряжені.*

Теорема 22.3 ([10]). *Нехай K — комутативне кільце характеристики p^s, $n \in \mathbb{N}$. Множина*

$$H = \{X \in GL(n, K) | \widetilde{X} \in UT(n, K/\operatorname{rad} K)\}$$

є силовською p-підгрупою групи $GL(n, K)$.

Доведення теореми випливає з теорем 22.1 і 22.2.

Область цілісності з одиницею називатимемо *кільцем Безу*, якщо кожен її скінченно породжений ідеал є головним.

Теорема 22.4 ([10]). *Нехай K — область Безу характеристики p. Будь-яка силовська p-підгрупи групи $GL(n, K)$ спряжена в $GL(n, K)$ з $UT(n, K)$.*

Доведення. Нехай K — поле відношень кільця K, P — силовська p-підгрупа групи $GL(n, K)$. Очевидно, P є p-підгрупою групи $GL(n, K)$. З теореми 7.2 випливає, що для деякої матриці $C \in GL(n, K)$ $C^{-1}PC \subset UT(n, K)$. Отже, перший стовпець матриці $C^{-1}AC$ як і AC рівний нулю, де $E_n + A$ — довільна матриця із групи P. Нехай

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

— перший стовпчик матриці C ($x_i \in F$, $i = 1, \ldots, n$). Нехай $x_i = \alpha x_i^{(0)}$, де $\alpha \in F$ ($x_i' \in K$, $i = 1, \ldots, n$). Тоді $X = \alpha X^{(0)}$, де

$$X^{(0)} = \begin{pmatrix} x_1^{(0)} \\ x_2^{(0)} \\ \vdots \\ x_n^{(0)} \end{pmatrix}.$$

Очевидно, $X^{(0)} \neq 0$, $\alpha \neq 0$ і для будь-якої матриці $E_n + A \in P$ $AX^{(0)} = 0$.

Припустимо,

$$X^{(k)} = \begin{pmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \vdots \\ x_n^{(k)} \end{pmatrix}$$

містить хоча б k нулів ($0 \leqslant k < n - 1$). Покажемо, що для деякої матриці $D \in$ $\in GL(n, K)$ $DX^{(k)}$ містить хоча б $k + 1$ нулів. Якщо $X^{(k)}$ не містить $k + 1$ нулів, то хоча б дві його компоненти відмінні від нуля. Не зменшуючи загальності, будемо вважати, що $x_1^{(k)} \neq 0$, $x_2^{(k)} \neq 0$. Нехай $x_1^{(k)}K + x_2^{(k)}K = xK$ ($x \in K$). Нехай далі α, β, γ, δ — елементи кільця K, такі, що $\alpha x_1^{(k)} + \beta x_2^{(k)} = x$, $x_1^{(k)} = \gamma x$, $x_2^{(k)} = \delta x$. Очевидно, $x(\alpha\gamma + \beta\delta) = x$, $x(\gamma x_2^{(k)} - \delta x_1^{(k)}) = 0$. Звідси $\alpha\gamma + \beta\delta = 1$, $\gamma x_2^{(k)} - \delta x_1^{(k)} = 0$. Тоді

$$M = \begin{pmatrix} \alpha & \beta \\ -\delta & \gamma \end{pmatrix} \in GL(2, K),$$

$$M\begin{pmatrix} x_1^{(k)} \\ x_2^{(k)} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\delta & \gamma \end{pmatrix}\begin{pmatrix} x_1^{(k)} \\ x_2^{(k)} \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}.$$

Тоді

$$X^{(k+1)} = \begin{pmatrix} M & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} X^{(k)}$$

містить хоча б $k+1$ нулів.

Проведена індукція показує, що для деякої матриці $D' \in GL(n, K)$

$$D'X^{(0)} = \begin{pmatrix} \alpha \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

($\alpha \in K$). Очевидно, $\alpha \neq 0$ і $X^{(0)} = \alpha Y$, де Y — перший стовпчик матриці $S = D'^{-1}$. Тоді $AY = 0$ і перший стовпчик матриць AS як і $S^{-1}AS$ рівний нулю для будь-якої матриці $E_n + A \in P$, де A — квадратна матриця порядку n над кільцем K. Отже, всі матриці із групи $S^{-1}PS$ мають 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 по n можна показати, що P спряжена із $UT(n, K)$. Теорема доведена.

Для локальних кілець було доведено теорему.

Теорема 22.5 ([10]). *Нехай K — комутативне локальне кільце характеристики p^s ($s \in \mathbb{N}$), $n \in \mathbb{N}$ і $n > 1$. Силовські p-підгрупи групи $GL(n, K)$ попарно спряжені тоді і тільки тоді, коли $K/\operatorname{rad} K$ — кільце Безу.*

З цієї теореми випливає така теорема.

Теорема 22.6 ([10]). *Нехай $n \in \mathbb{N}$, K — комутативне локальне кільце характеристики p^s ($s \in \mathbb{N}$). Якщо $K/\operatorname{rad} K$ — кільце Безу, то всі, з точністю до спряженості, силовські p-підгрупи групи $GL(n, K)$ вичерпуються групою $H = \{X \in \in GL(n, K) | \widetilde{X} \in UT(n, K/\operatorname{rad} K)\}$.*

ЛІТЕРАТУРА

1. *Супруненко Д. А.* Группы матриц. – М.: Наука, 1972.
2. *Супруненко Д. А.* Линейные p-группы // Докл. АН БССР. – 1960. – **35**, №6. – С. 233–235.
3. *Вольвачев Р. Т.* p-подгруппы Силова полной линейной группы // Изв. АН СССР. Сер. матем. – 1963. – **27**. – С. 1031–1054.
4. *Конюх В. С.* О линейных p-группах // Изв. АН БССР. Сер. физ.-мат. наук. – 1987. – №1. – С. 3–8.
5. *Юрченко Н. В., Рудько В. П.* Про силовські 2-підгрупи повної лінійної групи над полем характеристики нуль, // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2006. – Вип. 12–13. – С. 128–136.
6. *Петечук В. М.* Линейные p-группы над телами // Докл. АН Украины. Сер. мат. наук. – 1997. – №11. – С. 21–24.
7. *Mennice I.* Finite factor groups of the unimodular group // Annals of Math. – 1965. – **81**, №1. – P. 31–37.
8. *Гудивок П. М.* О силовских p-подгруппах полной линейной группы над кольцом целых чисел // Алгебра и анализ. – 1990. – **2**, №6. – С. 121–128.
9. *Gudivok P. M., Rud'ko V. P.* On isomorphism of Sylow subgroups of the general linear groups over the ring of itegers // J. Math. Sci. – 2000. – **102**, №3. – P. 3998–4008.
10. *Тилищак О. А.* Про силовські p-підгрупи повної лінійної групи над комутативним локальним кільцем характеристики p^s // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2000. – Вип. 5. – С. 95–102.
11. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр. – М.: Наука, 1969.
12. *Reiner I.* Normal subgrouhs of the unimodular group // Illinois J. Math. – 1958. – **2**, №1. – P. 142–144.
13. *Гудивок П. М.* О силовских подгруппах полной линейной группы над полными дискретно нормированными кольцами // Укр. мат. журн. – 1991. – **43**, № 7–8. – С. 918–924.
14. *Гудивок П. М., Кирилюк О. А.* Силовские p-подгруппы полной линейной группы над дискретно нормированными кольцами // Докл. АН УССР. – Сер. А. – 1979. – № 5. – С. 326–328.
15. *Гудивок П. М., Рудько В. П., Юрченко Н. В.* О силовских p-подгруппах полной линейной группы над областями главных идеалов // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2001. – Вип. 6. – С. 31–47.
16. *Юрченко Н. В.* Силовські p-підгрупи повної лінійної групи над кільцем всіх цілих алгебраїчних чисел // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2006. – Вип. 12–13. – С. 136–143.
17. *Гудивок П. М., Рудько В. П.* О силовских подгруппах полной линейной группы над областями целосности // Доп. НАН України. – 1995. – №8. – С. 5–7.

ПРЕДМЕТНИЙ ПОКАЗЧИК

Позначення

$\mathbb{Z}$ — множина всіх цілих чисел,
$\mathbb{Q}$ — множина всіх раціональних чисел,
$\mathbb{R}$ — множина всіх дійсних чисел,
$\mathbb{C}$ — множина всіх комплексних чисел,
$\mathbb{Z}_m$ — кільце класів лишків за модулем m,
$d|n$ — d ділить n,
НСД$(\alpha_1, \ldots, \alpha_n)$ — найбільший спільний дільник елементів $\alpha_1, \ldots, \alpha_n$,
$A \cup B$ — об'єднання множин A і B,
$A \cap B$ — переріз множин A і B,
$A \backslash B$ — різниця множин A і B,
$f : M_1 \to M_2$ — відображення f множини M_1 в множину M_2,
$GL(n, K)$ — повна лінійна група степеня n над кільцем K,
$SL(n, K)$ — спеціальна лінійна група степеня n над кільцем K,
$T(n, F)$ — трикутна група степеня n над полем F,
$UT(n, K)$ — унітрикутна група степеня n над кільцем K,
$PGL(n, T)$ — повна проективна група степеня n над тілом T,
$PSL(n, T)$ — спеціальна проективна група степеня n над тілом T,
$D(n, F)$ — група всіх діагональних матриць степеня n над полем F,
$C(n, \mathbb{Z}, m)$ — m-конгруенц-підгрупа групи $GL(n, \mathbb{Z})$,
$S(n, \mathbb{Z}, m)$ — спеціальна m-конгруенц-підгрупа групи $GL(n, \mathbb{Z})$,
S_n — симетрична група степеня n,
C_n — абстрактна циклічна група порядку n,
C_{p^∞} — група типу p^∞,
D_{2^n} — група діедра порядку 2^{n+1},
Q_{2^n} — група кватерніонів порядку 2^n,
QD_{2^n} — квазідіедральна група порядку 2^{n+1},
$a \equiv b \pmod m$ — a конгруентне b за модулем m,
$\mathrm{diag}[a_1, \ldots, a_n]$ — діагональна матриця порядку n з діагональними елементами $a_1, \ldots, a_n$,
$|A|$, $\det A$ — детермінант Д'єдонне квадратної матриці A,
$\mathrm{tr}\, A$ — слід квадратної матриці A,
$\mathrm{tr}(G)$ — множина слідів всіх елементів матричної групи G,
$A \circ B$ — приєднаний добуток квадратних матриць A і B,
$|G|$ — порядок групи G,
$[G : H]$ — індекс підгрупи H в групі G,
a^b — елемент спряжений з елементом a за допомогою елемента b деякої групи,
Δ^g — зображення підгрупи спряжене до зображення Δ за допомогою елемента g деякої групи,
L^G — індукований TG-модуль для деякого поля T, TH-модуля L та підгрупи H групи G,
$[a, b]$ — комутатор елементів a, b деякої групи,
$[A, B]$ — взаємним комутантом підгруп A та B деякої групи,
V/U — фактор-група (-простір, -кільце) V за U,
G' — комутант групи G,
$\mathfrak{Z}(G)$ — центр групи G,
$\mathfrak{Z}^2(G)$ — другий центр групи G,
$G_1 \times G_2$ — прямий добуток груп G_1, G_2,
$\langle X|Y\rangle$ — група породжена множиною X із визначальними співвідношеннями Y,
$\mathrm{Ker}\, f$ — ядро гомоморфізма $f : M_1 \to M_2$,

$\operatorname{Im} f$, $f(M_1)$ — образ гомоморфізма $f : M_1 \to M_2$,
$\operatorname{Aut} G$ — група всіх автоморфізмів групи G,
$\mathfrak{Z}_H(M)$ — централізатор множини M в підгрупі H,
$N_H(M)$ — нормалізатор множини M в підгрупі H,
$N_G(\chi)$ — нормалізатор лінійного характера χ підгрупи в групі G,
$\operatorname{St}(M)$ — стабілізатор підпростору M лінійного простору, в якому діє деяка група,
$[H]_T$ — лінійна оболонка групи H над полем T,
$A \otimes B$ — кронекеровий добуток матриць A та B,
$G_1 \otimes G_2$ — тензорним добутком груп G_1 та G_2,
$H \wr A$ — сплетення групи H та підгрупа A симетричної групи,
$U_1 \oplus U_2$ — пряма сума підпросторів U_1, U_2,
$\operatorname{char} K$ — характеристика кільця K,
$\operatorname{Rad} K$ — радикал Джекобсона кільця K,
$\operatorname{rad} K$ — первісний радикал кільця K,
$\operatorname{End}_T(V)$ — кільце всіх лінійних операторів простору V над тілом T,
$(F : T)$ — степінь розширення F поля T.

ГУДИВОК Петро Михайлович
РУДЬКО В'ячеслав Павлович
ТИЛИЩАК Олександр Андрійович
ЮРЧЕНКО Наталія Василівна

ЛІНІЙНІ ГРУПИ

Формат 60 × 84/16. Умов. друк. арк. 7,05. Замовлення № 76. Наклад 100 екз.

Розтиражовано з готових оригінал-макетів
ПП Данило С. І.
м. Ужгород, пл Ш. Петефі, 34/1
Тел. 61-23-51