

РОЗДІЛ 3. ЛІНІЙНІ ГРУПИ НАД КОМУТАТИВНИМ КІЛЬЦЕМ

§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:

$$e_{ij} \quad (1 \leq i, j \leq n)$$

— матричні одиниці,

$$t_{ij}(\lambda) = E_n + \lambda e_{ij} \quad (i \neq j)$$

— 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), домножений 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 единиця матриця C в групі $SL(n, \mathbb{Z})$ така, що $A = C \operatorname{diag}[1, \dots, 1, \pm 1]$.*

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 стовпчик 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 $d = \operatorname{diag}[\pm 1, \dots, \pm 1]$, 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 $\tilde{\sigma}$ міститься в $SL(n, K)$. Добуток $\tilde{\sigma}A$ одержується, якщо в матриці A зробити перестановку рядків: $\sigma(i)$ -ий рядок замінити i -им рядком ($i = 1, \dots, n$).

Вправа 3. Показати, що якщо σ — непарна підстановка, то

$$\operatorname{diag}[1, \dots, 1, -1, 1, \dots, 1] \cdot \tilde{\sigma} \in SL(n, K).$$

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

$$\mu_m : \mathbb{Z} \rightarrow \mathbb{Z}_m$$

кільця \mathbb{Z} в кільце $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ класів лишків за модулем m продовжується до гомоморфізму

$$\mu_m : GL(n, \mathbb{Z}) \rightarrow GL(n, \mathbb{Z}_m)$$

груп. Цей гомоморфізм називається *гомоморфізмом Мінковського*. Введемо позначення

$$C(n, \mathbb{Z}, m) = \text{Ker } \mu_m, \quad S(n, \mathbb{Z}, m) = SL(n, \mathbb{Z}) \cap C(n, \mathbb{Z}, m).$$

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 $E(n, \mathbb{Z}, m)$ — нормальні підгрупи 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 противріччя 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 скінчена.

Теорема 19.3. Будь-яка скінчена підгрупа групи $GL(n, \mathbb{Z})$ ізоморфна деякій підгрупі скінченої 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 t група H містить спеціальну t -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 t група H містить спеціальну t -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 t .*

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 Баса 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

$$E(n, \mathbb{Z}, m) = S(n, \mathbb{Z}, m) \quad (n > 2). \quad (1)$$

Перш за все відмітмо 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) спряження 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

$$b = \text{diag}[c, 1], \quad c \in S(n - 1, \mathbb{Z}, m),$$

що aRb .

Доведення. Можна 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, домножений на tm ($t = 1, 2, \dots$). 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 $\text{НСД}(\alpha_{21}, \alpha_{32} = m)$ 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 стовпчика. 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*

$$\nu : SL(3, \mathbb{Z}) \rightarrow SL(3, \mathbb{Z}) / E(3, \mathbb{Z}, m)$$

— природний гомоморфізм. Тоді група $\nu(C(3, \mathbb{Z}, m))$ належить центру $\mathfrak{Z}(\text{Im } \nu)$ групи $\text{Im } \nu$.

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 $\nu(a) \in \mathfrak{Z}(\text{Im } \nu)$ тоді і тільки тоді, коли $\nu(b) \in \mathfrak{Z}(\text{Im } \nu)$. 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

$$a_k = \begin{pmatrix} \alpha & \beta^k & 0 \\ (-1)^{k+1}\gamma^k & \delta_k & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (k = 1, 2, \dots),$$

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 $\text{НСД}(\alpha, m) = 1$, 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 $n_s \in \mathbb{Z}$

$$b_s = t_{21}^{-1}(n_s)at_{21}(n_s) = \begin{pmatrix} \alpha + n_s\beta & \beta & 0 \\ \gamma' & \delta' & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

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 $q \equiv -1 \pmod{v}$, $q' \equiv -p \pmod{v}$ 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 розуміння 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 нормальню скінченного індекса підгрупою групи $GL(2, \mathbb{Z})$, яка не містить жодної нетривіальної спеціальної конгруенц-підгрупи $GL(2, \mathbb{Z})$.*

Нехай в правах 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 групою $SL(n, \mathbb{Z})$;
- б) Відображення $h \rightarrow (h^{-1})^T$ ($h \in H$) 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 стовпчик 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

$$\alpha_{31} = \dots = \alpha_{n1} = 0, \quad \alpha_{12} \neq 0.$$

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 $\alpha \in \text{НСД}(\alpha_{21}, \alpha_{31})$ 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 спряження з допомогою матриці $\text{diag}[1, c_{n-1}]$.

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 породжується 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 нормальнюю підгрупою групи $SL(n, \mathbb{Z})$.

Вправа 7. Використаємо позначення для матриці a_k , які введені після леми 20.3. Показати, що

$$a_{k+1} = c_2^{-1}t_{21}(\gamma')t_{31}(-\beta)t_{13}(-\gamma)a_kc_1^{-1}ac_1t_{12}(-\beta^k)c_2,$$

де $c_2 = \text{diag}[-1, 1, 1](\widetilde{1 \ 3})$, $\gamma' = (-1)^k\delta$, $c_1 = (\widetilde{1 \ 2 \ 3})$.

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, \dots, a_s — повна система представників суміжних класів групи G за підгрупою A . Розглянути підгрупу $A^{a_1} \cap \dots \cap A^{a_s}$.

§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 ;

$$W_0(P) = P = P_p(K), \quad W_j(P) = W_{j-1}(P) \wr C_p \quad (j = 1, 2, \dots).$$

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 . Okрім цього, група $W_j(P)$ незвідна над полем F і є силовською p -підгрупою групи $GL(p^j, K)$. Нехай

$$n = n_0 + n_1 p + \cdots + n_s p^s, \quad (0 \leq n_j < p, \quad n_s \neq 0 \text{ при } s > 0)$$

— 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 $\rho : F \rightarrow M(p-1, \mathbb{Q})$ —ображення елементів поля F матрицями порядку $p-1$ над полем \mathbb{Q} (якщо $\alpha \in \mathbb{Q}$, то $\rho(\alpha) = \alpha E_{p-1}$, $\rho(\varepsilon) = \tilde{\varepsilon}$ і т. д.). Будемо вважати, що цеображення продовжено на матриці над полем F .

Група

$$\rho(G(P, n)) = \rho(W_0(P)^{m_0}) \times \rho(W_1(P)^{m_1}) \times \cdots \times \rho(W_s(P)^{m_s})$$

— 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

$$m = m_0 + (p-1)n, \quad 0 \leq m_0 < p-1.$$

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} . Скінчена 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 — скінчена 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 $G_j \subset GL(n_j, \mathbb{Q})$, ($n_1 + \dots + n_t = n, t \geq 1$). 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 скінченою 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 ($1 \leq r < p$) 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 шар⁷ N групи $\mathfrak{Z}(H)^r$ буде елементарною абелевою групою порядку p^r . Нехай a — елемент порядку p в $\mathfrak{Z}(H)$ і $d_j = \text{diag}[E_d, \dots, a, \dots, E_d]$ ($j = 1, \dots, r$) — 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 $A^{-1}NA = N$. Всі матриці d_j мають одинаковий спектр⁸,

⁷Нижній шар абелевої p -групи — підгрупа її елементів g , що задовільняють умову $g^p = e$.

⁸Спектр 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 -нормалізатор⁹ 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 $G \times H$:

$$\Gamma(\text{diag}[g, h]) = g; \quad \Delta(\text{diag}[g, h]) = h,$$

де $\text{diag}[g, h] \in G \times H$ ($g \in G, h \in H$). Очевидно, що $\text{Im } \Gamma = G$, $\text{Im } \Delta = H$. 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 $\Gamma, \Delta\varphi$ 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 $n = n_0 + n_1p + \dots + n_sp^s$ — p -ічний розклад натурального числа n . Покладемо

$$W_0(H) = H, \quad W_j(H) = W_{j-1}(H) \wr C_p \quad (j = 1, \dots),$$

$$G(H, n) = \prod_{j=0}^s (W_j(H))^{n_0}.$$

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.

$$d_p = \begin{cases} p, & \text{якщо } p > 3; \\ 9, & \text{якщо } p = 3; \\ 8, & \text{якщо } p = 2; \end{cases}$$

$$V_p = \begin{cases} W_1(P_p(K)) = P_p(K) \wr C_p, & \text{якщо } p > 3; \\ W_2(P_3(K)) = (P_3(K) \wr C_3) \wr C_3, & \text{якщо } p = 3; \\ W_3(P_2) = ((P_2 \wr C_2) \wr C_2), & \text{якщо } p = 2. \end{cases}$$

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, $V_2 = \langle U_2, \text{diag}[-1, 1, \dots, 1] \rangle$.

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

$$e_1, \dots, e_n \quad (n = d_p)$$

цього модуля.

Нехай M — K -підмодуль в L з базисом:

$$\begin{aligned} f_1 &= \omega^2 e_1, \quad f_2 = \omega(e_2 - e_1), \quad \dots, \quad f_{n-1} = \omega(e_{n-1} - e_{n-2}), \\ f_n &= e_1 + e_2 + \dots + e_n, \end{aligned}$$

де

$$\omega = \varepsilon - 1$$

— необоротний елемент кільця $K = \mathbb{Z}[\varepsilon]$. Відмітимо, що

$$\begin{aligned} \omega^{p-1}p^{-1} &\in K^*, \\ \varepsilon^s - 1 &\equiv s\omega \pmod{\omega^2} \quad (m \in \mathbb{Z}) \end{aligned}$$

в кільці K .

Лема 21.4. K -модуль M є U_p -модулем, але не буде V_p -модулем.

Доведення. Перш за все, відмітимо, що $\omega^2 L \subset M$, але ωL не міститься в M . Нехай

$$L_0 = \left\{ \sum_j \alpha_j e_j \mid (\alpha_j \in K), \sum_j \alpha_j \equiv 0 \pmod{\omega} \right\}.$$

Тоді $M = \omega L_0 + Kf_n$. Неважко бачити, що K -модуль L_0 є V_p -простором. Якщо b — підстановочна матриця з V_p , то $bf_n = f_n$. Нехай

$$a = \text{diag}[\varepsilon^{t_1}, \dots, \varepsilon^{t_n}] \quad (t_j \in \mathbb{Z}).$$

Тоді

$$af_n = \varepsilon^{t_1} e_1 + \dots + \varepsilon^{t_n} e_n \equiv f_n + \omega(t_1 + \dots + t_n)e_1 \pmod{L_0}$$

і $af_n \in M$ тоді і тільки тоді, коли сума $t_1 + \dots + t_n$ 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

$$\hat{U}_p = T^{-1}U_pT.$$

Тоді $\hat{U}_p \in GL(d_p, K)$, але група $T^{-1}V_pT$ 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 $(T^{-1}V_p T) \cap GL(d_p, K) = \hat{U}_p$ (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*

$$d = (p-1)d_p, \quad H = \rho(V_p) \quad \text{або} \quad H = \rho(\hat{U}_p), \quad 0 \leq d_0 < d.$$

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, \dots, i_t — попарно різні за модулем p цілі числа і Λ_s — p -підгрупа в $GL(s, K)$, яка породжується матрицями

$$A_s = \text{diag}[\varepsilon, \dots, \varepsilon], \quad B_s = \begin{pmatrix} \varepsilon^{i_1} & 1 & & 0 \\ & \varepsilon^{i_2} & \ddots & \\ & & \ddots & 1 \\ 0 & & & \varepsilon^{i_s} \end{pmatrix}.$$

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 $C_s B_s = B_s C_s$. Очевидно, $C_2 \in \Lambda_2$. Нехай $2 \leq s < t$ 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 $X^T = (x_1, \dots, x_s)$ ($x_i \in K$). З умови $C_{s+1} B_{s+1} = B_{s+1} C_{s+1}$ одержуємо рівняння для x_i :

$$(\varepsilon^{i_r} - \varepsilon^{i_{s+1}})x_r + x_{r+1} = 0 \quad (r = 1, \dots, s-1), \quad (\varepsilon^{i_s} - \varepsilon^{i_{s+1}})x_s = 1 - \varepsilon^j.$$

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 $n = n_0 + 2(p-1)$, $0 \leq n_0 < p-1$. 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, \dots, v_{p-1} . Оператор a діє в M за правилом:

$$a(\alpha) = \varepsilon\alpha \quad (\alpha \in I); \quad a(v_j) = v_j + \omega \quad (j = 1, \dots, p-1),$$

де ω деякий елемент ідеала I . Визначимо новий оператор b в M :

$$b(\alpha) = \alpha \quad (\alpha \in I); \quad b(v_j) = v_{j+1} \quad (j = 1, \dots, p-2),$$

$$b(v_{p-1}) = -v_1 - \dots - v_{p-1} + p(\varepsilon - 1)^{-1}\omega.$$

Відмітимо, що $p(\varepsilon - 1)^{-1} \in K$. Неважко перевірити, що $b^p = 1$ і $ab = ba$. 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 $n > 1$, $1 \leq m < n$ 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,

$$A = \ker \mu_2|_W = \langle d_1 = \text{diag}[-E_n, E_n], d_2 = \text{diag}[E_n, -E_n] \rangle.$$

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 $C = \text{diag}[C_1, C_2]$, 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

$$B = \{\text{diag}[\pm E_n, h] | h \in \ker \mu_2|H_1\} \text{ і } a = \text{diag}[-E_n, E_m] \in B.$$

Нехай X належить 2-нормалізатору групи V в групі $GL(n+m, \mathbb{Z})$ і $X^{-1}aX = a' = \text{diag}[\pm E_n, h]$, де $h \in \ker \mu_2|H_1$. Тоді

$$-n + m = \pm n + \text{tr } h.$$

Так як $n > m$, то $\text{tr } h = m$ 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 $H = \Gamma_3$. Одержано:

- 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 $\text{tr } a = 5$. Це $a = \text{diag}[-1, E]$. 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 $4 \leq n \leq 7$. В групі $GL(n, \mathbb{Z})$ існує пара $H_1(n), H_2(n)$ силовських 2-підгруп різних порядків. Ці пари наведені в таблиці.*

$GL(n, \mathbb{Z})$	$H_1(n)$	$H_2(n)$	$ H_1(n) $	$ H_2(n) $
$GL(4, \mathbb{Z})$	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

$$a_1 = \text{diag}[a, E_4], \quad a_2 = \text{diag}[E_4, a], \quad a_3 = \text{diag}[b, E_4], \quad a_4 = [E_4, b].$$

Групи

$$A_1 = \langle a_1, a_2 \rangle, \quad A_2 = \langle a_1 a_3, a_2 \rangle, \quad A_3 = \langle a_1, a_2 a_3 a_4 \rangle, \quad A_4 = \langle a_1 a_3, a_2 a_4 \rangle$$

утворюють повний список максимальних цілком звідних підгруп в групі $G = \Delta_3 \times \Delta_3$. Нехай $X \in N(G)$ — 3-нормалізатор групи G в групі $GL(8, \mathbb{Z})$ і $\tau(g) = X^{-1}gXg \in G$. 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 $X = \text{diag}[X_1, X_2]$, де X_j належить 3-нормалізатору групи Δ_3 , тобто $X \in G$.

2) Матриця $C = \text{diag}[E_8, \widetilde{\varepsilon}]$ 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 $C_1 = \text{diag}[E_4, \widetilde{\varepsilon}]$.

Лема 21.11. Нехай $6 \leq n < 18$. В групі $GL(n, \mathbb{Z})$ існує пара $G_1(n), G_2(n)$ силовських 3-підгруп різних порядків. Ці пари наведені в таблиці.

$GL(n, \mathbb{Z})$	$G_1(n)$	$G_2(n)$	$ G_1(n) $	$ G_2(n) $
$GL(6, \mathbb{Z})$	$\Delta_3 \times \widetilde{P}_3$	$W(\widetilde{P}_3)$	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
$GL(k+1, \mathbb{Z})$ ($k = 6, 8, 10$)	$G_1(k) \times \langle 1 \rangle$	$G_2 \times \langle 1 \rangle$		
$GL(k+6, \mathbb{Z})$ ($6 \leq k \leq 11$)	$G_1(k) \times \widetilde{P}_3$	$G_2(k) \times \widetilde{P}_3$		

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) $p > 2$, $2(p-1) \leq n < 3(p-1)$;
- 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 $\langle 1 \rangle^k$ ($1 \leq k < p-1$), 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

$$a = \begin{pmatrix} \tilde{\varepsilon} & A \\ 0 & 1 \end{pmatrix}, \quad A^T = (1, 0, \dots, 0).$$

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 $\langle 1 \rangle^k$ ($1 \leq k < p-1$), 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 $n = 2$ розглянуто 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 скінчена і скінчена 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

$$g = \text{diag}[g_1, g_2, g_3] \quad (g_j \in G_j)$$

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

$$\Delta : g = \text{diag}[g_1, g_2, g_3] \rightarrow \begin{pmatrix} \Delta(g) & * \\ 0 & \Delta_2(g) \end{pmatrix} \quad (g \in G)$$

і яке є нерозкладним навіть над кільцем цілих p -адичних чисел. Тоді підгрупа $\bar{G} = \Delta(G) \times G_3$ 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 \bar{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 $r > 1$ ($p = 2$). Скористаємося 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 $a = \rho(\text{diag}[\varepsilon, \dots, \varepsilon])$. Тоді $H = \rho(H_1)$, 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

$$\mu : GL(n, K) \rightarrow GL(n, K/K\omega), \quad \omega = \varepsilon - 1.$$

Тоді група $\bar{W}_r = \mu(W_r(P_p))$ складається із матриць підстановок, кожна з яких є добутком циклів довжини p^s ($0 \leq s \leq r$). 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 $\text{diag}[a, 1, \dots, 1]$ (або $\text{diag}[b, 1, \dots, 1]$) 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 необортне в R . П. М. Гудивок, В. П. Рудько і Н. В. Юрченко [15] знайшли критерій ізоморфізму і спряженості силовських p -підгруп групи $GL(n, R)$. Відмітимо, що будь-яка p -підгрупа в групі $GL(n, R)$ є скінчена.

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 нескінчено 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

$$P_2 = \{1, -1\}, \quad C_2 = \langle (12) \rangle, \quad W_1(P_2) = P_2 \wr C_2,$$

$$W_2(P_2) = W_1(P_2) \wr C_2 \quad \text{i} \quad H = SL(4, \mathbb{Z}) \cap W_2(P_2).$$

Показати, що $\mathfrak{Z}^2(H)$ — елементарна абелева група порядку 8.

Вправа 2. Нехай

$$W_3(P_2) = W_2(P_2) \wr C_2 \quad \text{i} \quad U = SL(8, \mathbb{Z}) \cap W_3(P_2).$$

Показати, що

$$\mathfrak{Z}^2(U) = \langle -E_8, \text{diag}[-E_4, E_4] \rangle.$$

Вправа 3. Нехай

$$K = \mathbb{Z}[\varepsilon], \quad \varepsilon^3 = 1, \quad \varepsilon \neq 1, \quad P_3 = \langle \varepsilon \rangle, \quad C_3 = \langle (123) \rangle, \quad W_1(P_3) = P_3 \wr C_3.$$

a) 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 $T_0 = E_3$,

$$T_1 = \begin{pmatrix} \omega & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} \omega & 0 & 1 \\ 0 & \omega & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad (\omega = \varepsilon - 1).$$

в) Нехай

$$W_2(P_3) = W_1(P_3) \wr C_3 \quad \text{i} \quad H = SL(9, K) \cap W_3(P_3).$$

Показати, що

$$\mathfrak{Z}^2(H) = \langle \varepsilon E_9, \text{diag}[E_3, \varepsilon E_3, \varepsilon^2 E_3] \rangle.$$

Вправа 4. Нехай

$$p > 3, \quad P_p = \{\varepsilon\}, \quad \varepsilon^p = 1, \quad \varepsilon \neq 1,$$

$$W(P_p) = P_p \wr C_p, \quad C_p = \langle (12 \dots p) \rangle \quad \text{i} \quad H = SL(p, K) \cap W(P_p).$$

Показати, що

$$Z^2(H) = \langle \varepsilon E_p, \text{diag}[1, \varepsilon, \dots, \varepsilon^{p-1}] \rangle.$$

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

$$\begin{aligned} \det(A + B) &= \det(A + E_n - (E_n - B)) = \\ &= \det((A(E_n - B)^{-1} + (E_n - B)^{-1} - E_n)(E_n - B)) = \\ &= \det((A(E_n + B') + B')(E_n - B)) = \\ &= \det((A + B' + AB')(E_n - B)) = \det(A \circ B') \det(E_n - B) = 0. \end{aligned}$$

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 матрицях з групи P елемент у деякій фіксованій позиції (i, j) ($i \neq j$) рівний нулю, то рівний нулю і елемент матриці A^r у позиції (i, j) для будь-якого натурального числа r і кожної матриці A порядку n над кільцем K такої, що $E_n + A \in P$.

Далі через K^* будемо позначати мультиплікативну групу кільця K , $\text{rad } K$ — першій радикал кільця K , який у комутативному випадку складається з усіх нільпотентних елементів кільця K .

Теорема 22.1 ([10]). *Нехай K є комутативним кільцем характеристики p , $\text{rad } K = \{0\}$, $n \in \mathbb{N}$. 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 $\det(A \circ B) \in \text{rad } K$. 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 ($i = k+1, \dots, n$). Покажемо, що у всіх матриць з групи P елемент у позиції $(k, 1)$ також рівний нулю. Дійсно, нехай знову A' — довільна матриця з групи P , $A = A' - E_n$, B — довільна матриця з $T_0(n, K)$. 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 ($i = k+1, \dots, n$; $r \in \mathbb{N}$).

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 $M((A \circ B)^m)$ і $(M(A \circ B))^m$ 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 $(\det M(A \circ B))^m = \det(M(A \circ B))^m = 0$. Тому $\det(M(A \circ B)) \in \text{rad } K$. 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 $\det(M(A) \circ B') = \det(M(A) \circ M(B_1)) = 0$. 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 $\tilde{z} = z + \text{rad } K$ будемо позначати елемент фактор-кільця $K/\text{rad } K$ кільця K , де $z \in K$, $\tilde{T} = \|t_{ij} + \text{rad } K\|$ — матрицю над фактор-кільцем $K/\text{rad } K$ кільця K , де $T = \|t_{ij}\|$ — деяка матриця над кільцем K . Неважко встановити зв'язок між p -підгрупами групи $GL(n, K)$ та — групи $GL(n, K/\text{rad } K)$.

Теорема 22.2 ([10]). *Нехай K — комутативне кільце характеристики p^s , $n \in \mathbb{N}$. $\varphi: X \rightarrow \tilde{X}$ є гомоморфним відображенням групи $GL(n, K)$ на групу $GL(n, K/\text{rad } K)$. При цьому відображення повний прообраз будь-якої силовської p -підгрупи групи $GL(n, K/\text{rad } K)$ 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 $GL(n, K/\text{rad } K)$. Дві силовські p -підгрупи групи $GL(n, K)$ спряжені тоді і*

тільки тоді, коли їх образи при гомоморфізмі φ є спряженими силовськими р-підгрупами групи $GL(n, K/\text{rad } K)$.

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 спряженні тоді і тільки тоді, коли силовські p -підгрупи групи $GL(n, K/\text{rad } K)$ попарно спряженні.*

Теорема 22.3 ([10]). *Нехай K — комутативне кільце характеристики p^s , $n \in \mathbb{N}$. Мноожина*

$$H = \{X \in GL(n, K) \mid \tilde{X} \in UT(n, K/\text{rad } K)\}$$

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 -підгрупа 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 ($x_i \in F$, $i = 1, \dots, n$). Нехай $x_i = \alpha x_i^{(0)}$, де $\alpha \in F$ ($x'_i \in K$, $i = 1, \dots, n$). 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 ($0 \leq k < n - 1$). Покажемо, що для деякої матриці $D \in GL(n, K)$ $DX^{(k)}$ 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 $\alpha, \beta, \gamma, \delta$ — 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 $K/\text{rad } K$ — 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 $K/\text{rad } K$ — кільце Безу, то всі, з точністю до спряженості, силовські p -підгрупи групи $GL(n, K)$ вичерпуються групою $H = \{X \in GL(n, K) | \tilde{X} \in UT(n, K/\text{rad } K)\}$.*