Лекції з загальної алгебри, 2 курс, 4 семестр, математика, частина 3

Анна Вишнякова

Харківський національний університет ім. В.Н.Каразіна

Харків, 2020

Норвезький математик в 1872 році доказав ряд результатів про структуру довільних скінчених груп. Зараз ці результати вважаються класичними, і їх зазвичай формулюють у вигляді трьох теорем Силова.

Перша теорема Силова. Нехай G – група, p – просте число, і $|G| = p^n m$, де $n, m \in \mathbb{N}$ і НСД$(m, p) = 1$. Тоді
1. Для кожного $k = 1, 2, \ldots, n$ існує $H < G$, така що $|H| = p^k$.
2. Для кожної $H < G$, $|H| = p^k$, існує така підгрупа $\tilde{H} < G$, що $|\tilde{H}| = p^n$ і $H < \tilde{H}$.

Друга теорема Силова. Нехай G – група, p – просте число, і $|G| = p^n m$, де $n, m \in \mathbb{N}$ і НСД$(m, p) = 1$. Тоді усі силовські підгрупи G є спряженими: для довільних $H_1 < G, H_2 < G$, таких що $|H_1| = |H_2| = p^n$, існує елемент групи $g \in G$, такий що $H_1 = g\, H_2\, g^{-1}$.

Третя теорема Силова. Нехай G – група, p – просте число, і $|G| = p^n m$, де $n, m \in \mathbb{N}$ і НСД$(m, p) = 1$. Нехай N – кількість силовських p-підгруп групи G. Тоді $N \Big| |G|$ і $N \equiv 1 (\mod p)$.

Доведення теорем Силова. Нехай $X = \{H < G \mid |H| = p^n\}$ – множина силовських p-підгруп групи G (ми вже довели, що ця множина не є пустою). Тоді група G діє на множині X спряженням, а саме розглянемо $(\cdot,\cdot) : G \times X \to X$, яке задається формулою $(g, H) = gHg^{-1}$, $(g \in G, H \in X)$.

Перевіримо, що вказана формула задає відображення $G \times X \to X$.
1) Для довільних $g \in G, H \in X$ виконується $gHg^{-1} < G$ (перевірте це!).
2) Припустимо, що для $g \in G, h_1, h_2 \in H$ виконується $gh_1g^{-1} = gh_2g^{-1}$, тоді $h_1 = h_2$. Тобто, $|gHg^{-1}| = |H| = p^n$.
Отже, вказана формула задає відображення $G \times X \to X$.

Перевіримо, що вказана формула задає дію групи G на множині X.
1) Для довільних $g, h \in G$, $H \in X$ маємо

$$(g,(h,H)) = (g, hHh^{-1}) = ghHh^{-1}g^{-1} = ghH(gh)^{-1} = (gh,H).$$

2) $(e,H) = eHe^{-1} = H$.
Отже, вказана формула задає дію групи G на множині X.

Нехай $P \in X$. Тоді $\mathrm{St}\,(P) < G$, і при цьому $P \subset \mathrm{St}\,(P)$ (так як $\forall p \in P$ виконується $pPp^{-1} \subset P$, і при цьому $|pPp^{-1}| = |P|$, звідки $pPp^{-1} = P$). Отже, $P < \mathrm{St}\,(P) < G$, при цьому $|P| = p^n$, $|G| = p^n m$, звідки $|\mathrm{St}\,(P)| = p^n l$, $l \Big| m$.

Ми хочемо довести, що орбіта P містить усі силовські підгрупи.

Ми маємо

$$|O(P)| = \frac{|G|}{|\mathrm{St}\ (P)|} \ \Rightarrow\ p \nmid |O(P)|.$$

Нехай $H < G$, $|H| = p^k$, $k \in \mathbb{N}$. Тоді H діє на $O(P)$ спряженням. Пояснимо це. Оскільки група G діє на множині X спряженням, а $H < G$, то H діє на множині X спряженням. При цьому для довільного $h \in H$ і довільного $\tilde{P} \in O(P)$ виконується

$$h\tilde{P}h^{-1} = hgPg^{-1}h^{-1} = (hg)P(hg)^{-1} \in O(P).$$

Ми перевірили, що H діє на $O(P)$ спряженням.

Таким чином, множина $Y = O(P)$ є диз'юнктним об'єднанням орбіт дії групи H на Y.

Тобто, існують $y_1, y_2, \ldots, y_l \in Y$, такі що $Y = \bigsqcup_{j=1}^{l} O(y_j)$, звідки $|Y| = \sum_{j=1}^{l} |O(y_j)| = \sum_{j=1}^{l} \frac{|H|}{|\mathrm{St}\ (y_j)|}$. Але $|H| = p^k$, і для кожного $j = 1, 2, \ldots, l$ маємо $\mathrm{St}\ (y_j) < H$, звідки отримуємо $\frac{|H|}{|\mathrm{St}\ (y_j)|} = p^{t_j},\ 0 \leq t_j \leq k$.

Ми довели раніше, що $p \nmid |O(P)|$, у нас $Y = O(P)$, тобто $p \nmid |Y|$, але ми маємо

$$|Y| = \sum_{j=1}^{l} p^{t_j}, \quad 0 \leq t_j \leq k.$$

Питання: коли це можливо?

Відповідь: існує $j = 1, 2, \ldots, l$ такий що $t_j = 0$. Таким чином, існує $\tilde{P} \in Y$ (отже, $\tilde{P}$ є силовською підгрупою групи G, отже $|\tilde{P}| = p^n$), така що

$$\forall h \in H: \quad h\tilde{P}h^{-1} = \tilde{P}. \tag{1}$$

Перевіримо, що $H\tilde{P} = \{h\tilde{p} \mid h \in H, \tilde{p} \in \tilde{P}\} < G$. Для довільних $h_1, h_2 \in H$, $\tilde{p}_1, \tilde{p}_2 \in \tilde{P}$ ми маємо $h_1\tilde{p}_1h_2\tilde{p}_2 = h_1(\tilde{p}_1h_2)\tilde{p}_2$. З (1) ми отримуємо $\forall h \in H: \quad h\tilde{P} = \tilde{P}h$, тобто існує $h_3 \in H$ таке що $\tilde{p}_1h_2 = h_3\tilde{p}_1$. Тобто маємо

$$h_1\tilde{p}_1h_2\tilde{p}_2 = h_1(\tilde{p}_1h_2)\tilde{p}_2 = h_1h_3\tilde{p}_1\tilde{p}_2 \in H\tilde{P},$$

тобто множина $H\tilde{P}$ є замкненою відносно множення. Очевидно, що $e \in H\tilde{P}$.

Крім того для довільних $h \in H$, $\tilde{p} \in \tilde{P}$ ми маємо $(h\tilde{p})^{-1} = \tilde{p}^{-1}h^{-1}$, і нам відомо, що існує $h_0 \in H$, таке, що $\tilde{p}^{-1}h^{-1} = h_0\tilde{p}^{-1} \in H\tilde{P}$. Тобто, $H\tilde{P} < G$.

Із (1) випливає, що $\tilde{P} \lhd H\tilde{P}$.

Ми хочемо довести, що порядок $H\tilde{P}$ є степенем p. Для цього нам потрібно довести, що $H\tilde{P}/\tilde{P} \approx H/(H \cap \tilde{P})$. Для доведення розглянемо довільний клас суміжності фактор-групи $H\tilde{P}/\tilde{P}$. Для довільних $h \in H$, $\tilde{p} \in \tilde{P}$ ми маємо $[h\tilde{p}] = h\tilde{p}\tilde{P} = h\tilde{P} = [h]$.

$$[h_1\tilde{p}_1] = [h_2\tilde{p}_2] \Leftrightarrow h_1\tilde{p}_1\tilde{P} = h_2\tilde{p}_2\tilde{P} \Leftrightarrow h_1\tilde{P} = h_2\tilde{P}$$
$$\Leftrightarrow h_2^{-1}h_1 \in \tilde{P} \Leftrightarrow h_2^{-1}h_1 \in \tilde{P} \cap H \Leftrightarrow h_1\tilde{P} \cap H = h_2\tilde{P} \cap H.$$

Ми довели, що $H\tilde{P}/\tilde{P} \approx H/(H \cap \tilde{P})$.

Кількість елементів в H є степенем p, звідки кількість елементів в $H \cap \tilde{P}$ є степенем p, тобто

$$|H/(H \cap \tilde{P})| = p^s,\ s = 0, 1, 2, \ldots, k \ \Leftrightarrow\ |H\tilde{P}/\tilde{P}| = p^s,$$

Крім того, $|\tilde{P}| = p^n$, звідки

$$|H\tilde{P}| = p^{n+s},\ s = 0, 1, 2, \ldots, k \ \Rightarrow\ |H\tilde{P}| = p^n = |\tilde{P}|$$

$$\Rightarrow\ H\tilde{P} = \tilde{P} \ \Rightarrow\ H \subset \tilde{P}.$$

Ми довели першу теорему Силова.

Нехай в попередніх міркуваннях $H = P \in X$, тобто H – силовська підгрупа G. Ми довели, що

$$\exists \tilde{P} \in X,\ \exists g \in G: \quad P \subset g\tilde{P}g^{-1} \ \Rightarrow\ P = g\tilde{P}g^{-1}.$$

Ми довели другу теорему Силова.

Нехай $H = P \in X$. Тоді одна з орбіт відносно P містить 1 елемент (саму підгрупу P), усі інші орбіти мають більше за один елемент. Порядки цих орбіт кратні p (вони дорівнюють індексам власних підгруп P).
Ми довели третю теорему Силова. $\square$