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

Анна Вишнякова

Харківський національний університет ім. В.Н.Каразіна

Харків, 2020

Дія групи на множині

Нехай G – група, X – множина, $X \neq \emptyset$.

Означення. Відображення $(\cdot,\cdot) : G \times X \to X$ називається дією групи G на множині X, якщо

$$1. \forall g, h \in G,\ \forall x \in X : (g,(h,x)) = (gh,x).$$

$$2. \forall x \in X : (e,x) = x.$$

Приклади. Наведемо два простих приклади, більш важливі для нас приклади наведемо пізніше.
1. Нехай G – група, $X = G$. Тоді група G діє на собі множенням зліва: $(g,x) = gx, \quad g \in G, x \in X$. Перевірте: це є дією групи на собі.
2. Нехай G – група, $H < G$. Тоді група H діє на множині $X = G$ множенням зліва: $(h,x) = hx, \quad h \in H, x \in X$. Перевірте: це є дією підгрупи на групі.

Нехай G – група, X – множина, $X \neq \emptyset$, і задана дія групи G на множині X, тобто задане відображення $(\cdot,\cdot) : G\times X \to X$, яке задовольняє властивості 1 і 2. Зафіксуємо довільний елемент $g \in G$ і розглянемо відображення $F_g : X \to X$, таке що $F_g(x) = (g, x),\ x \in X$.
Твердження. Для кожного $g \in G$ відображення F_g є бієкцією.

Доведення. Із властивості 2 дії групи на множині $F_e(x) = (e, x) = x,\ \forall x \in X$. Тобто $F_e = \mathrm{id}$ – тотожне відображення. Крім того, із властивості 1:

$$\forall g, h \in G, \forall x \in X : F_g \circ F_h(x) = F_g(F_h(x)) =$$

$$(g, (h, x)) = (gh, x) = F_{gh}(x).$$

Ми маємо

$$F_g \circ F_{g^{-1}} = F_{gg^{-1}} = F_e, \quad F_{g^{-1}} \circ F_g = F_{g^{-1}g} = F_e.$$

Тобто, відображення F_g має двостороннє обернене відображення, звідки воно є бієктивним. $\square$

Означення. Нехай група G діє на множині X, $x \in X$. Множина $O(x) = \{(g, x) \mid g \in G\} \subset X$ називається орбітою елемента x під дією групи. Кількість елементів в орбіті елемента x позначається $|O(x)|$

Твердження. Нехай група G діє на множині X. Довільні дві орбіти не перетинаються або збігаються:

$$\forall x, y \in X \quad O(x) \cap O(y) \neq \emptyset \;\Rightarrow\; O(x) = O(y).$$

Доведення. Припустимо, що $x, y \in X : \quad O(x) \cap O(y) \neq \emptyset$. Нехай $z \in X : \ z \in O(x) \wedge z \in O(y)$. Тобто, існують елементи групи $g, h \in G : \ (g, x) = z, \ (h, y) = z$. Звідки $(g^{-1}, (g, x)) = (g^{-1}, z)$, тобто $(g^{-1}, z) = (e, x) = x$. Аналогічно, $(h^{-1}, z) = y$.

Для довільного $w \in O(x)$ існує $\varphi \in G$, таке що $w = (\varphi, x) = (\varphi, (g^{-1}, z)) = (\varphi g^{-1}, z) = (\varphi g^{-1}, (h, y)) = (\varphi g^{-1} h, y) \in O(y)$. Тобто $O(x) \subset O(y)$. Так само, для довільного $\omega \in O(y)$ існує $\psi \in G$, таке що $\omega = (\psi, y) = (\psi, (h^{-1}, z)) = (\psi h^{-1}, z) = (\psi h^{-1}, (g, x)) = (\psi h^{-1} g, x) \in O(x)$. Тобто $O(y) \subset O(x)$. Маємо $O(x) = O(y)$. $\square$

Таким чином, множина X є диз'юнктним об'єднанням орбіт дії групи G.

Означення. Нехай група G діє на множині X, $x \in X$. Стабілізатором елемента x називається множина $\mathrm{St}(x) = \{g \in G \mid (g, x) = x\} \subset G$.

Твердження. Нехай група G діє на множині X, $x \in X$. Тоді $\mathrm{St}(x) < G$.

Доведення. Нехай $g, h \in \mathrm{St}(x)$, тоді $(g, x) = x$ і $(h, x) = x$, звідки маємо $(gh, x) = (g, (h, x)) = (g, x) = x$, отже $gh \in \mathrm{St}(x)$. Очевидно, що $e \in \mathrm{St}(x)$. Якщо $g \in \mathrm{St}(x)$, то маємо

$$(g, x) = x \Rightarrow (g^{-1}, (g, x)) = (g^{-1}, x) \Rightarrow$$

$$(g^{-1}g, x) = (g^{-1}, x) \Rightarrow (e, x) = (g^{-1}, x) \Rightarrow x = (g^{-1}, x),$$

звідки $g^{-1} \in \mathrm{St}(x)$. Ми довели, що $\mathrm{St}(x) < G$. $\square$

Теорема. Нехай група G діє на множині X, $x \in X$. Кількість елементів орбіти елемента x дорівнює кількості класів суміжності групи G по підгрупі $\mathrm{St}(x)$, тобто $|O(x)| = [G : \mathrm{St}(x)]$. Якщо група G є скінченою, то $|O(x)| = \frac{|G|}{|\mathrm{St}(x)|}$.

Доведення. Розглянемо множину правих класів суміжності групи G по підгрупі $\mathrm{St}(x)$: $\{[g] \mid g \in G\}$, де $[g] = g\ \mathrm{St}(x)$. Задамо функцію $f : \{[g] \mid g \in G\} \to O(x)$ (із множини правих класів суміжності групи G по підгрупі $\mathrm{St}(x)$ в орбіту елемента x) наступним чином: $f([g]) = (g, x)$.

Перевіримо коректність означення. Нехай $[g] = [h]$, тобто існує $\xi \in \mathrm{St}(x)$, такий що $g = h\xi$. Тоді маємо $f([g]) = (g, x) = (h\xi, x) = (h, (\xi, x)) = (h, x) = f([h])$. Коректність перевірено.

Перевіримо, що f – бієкція. Нехай $f([g]) = f([h])$, $g, h \in G$. Це означає, що $(g, x) = (h, x) \Rightarrow (h^{-1}g, x) = (h^{-1}, (g, x)) = (h^{-1}, (h, x)) = (h^{-1}h, x) = (e, x) = x$. Звідки $h^{-1}g \in \mathrm{St}(x)$, тобто $g \in h\,\mathrm{St}(x) = [h]$, звідки $[g] = [h]$. Ми довели, що f – ін'єкція.

Розглянемо довільний $y \in O(x)$. Ми маємо $y \in O(x) \Leftrightarrow \exists g \in G : y = (g, x)$. Тоді $f([g]) = y$. Ми довели, що f – сюр'єкція.

Тобто, f – бієкція, звідки множина правих класів суміжності групи G по підгрупі $\mathrm{St}(x)$ і множина елементів орбіти $O(x)$ мають однакову потужність. □

Приклад 1.

Нехай G – група, множина $X = G$. Задамо дію групи G на множині X наступним чином:

$$(g, x) = gxg^{-1}, \quad g \in G, x \in X$$

(дія групи на собі спряженням).

Перевіримо, що це є дією групи на собі.
1. Для довільних $g, h \in G$ і довільного $x \in X$ маємо $(g,(h,x)) = (g, hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh, x)$.
2. $(e,x) = exe^{-1} = exe = x$. Тобто група G діє на собі спряженням.

Приклад 2.
Нехай G – група, множина $X = \{H \mid H < G\}$. Задамо дію групи G на множині X наступним чином:

$$(g,H) = gHg^{-1}, \quad g \in G, H \in X$$

(дія групи на множині своїх підгруп спряженням). Перевірте, що це є дією групи на множині.

Силовські підгрупи скінченої групи

Нехай G – група, p – просте число, і $|G| = p^n m$, де НСД$(m, p) = 1$, $n \in \mathbb{N}$.

Означення. Силовською p-підгрупою групи G називається підгрупа $H < G$, така що $|H| = p^n$.

Теорема (Силов). Нехай G – група, p – просте число, і $|G| = p^n m$, де НСД$(m, p) = 1$, $n \in \mathbb{N}$. Тоді існує підгрупа $H < G$, така що $|H| = p^n$, тобто в групі G існує силовська p-підгрупа.

Доведення. Ми будемо доводити цю теорему індукцією по порядку групи (за умовою, що порядок групи ділиться на p).

1. База індукції $|G| = p$. Тоді G є своєю силовською підгрупою.

2. Індуктивний перехід. Припустимо, що твердження теореми виконується для усіх груп, порядок яких є меншим за $|G| = p^n m$.

Якщо група G має власну підгрупу $H < G, H \neq G$, таку що $p^n \mid |H|$, то силовська p-підгрупа для H буде і силовською p-підгрупою для G. Тобто, ми можемо припустити, що кожна власна підгрупа $H < G, H \neq G$, має властивість $p \mid \frac{|G|}{|H|}$.

Розглянемо дію групи на собі спряженням (група G діє на множині $X = G$ наступним чином: $(g, x) = gxg^{-1}, \quad g \in G, x \in X$). Ми вже доводили, що це є дією групи. Тоді вся множина $X = G$ є диз'юнктним об'єднанням орбіт. Тобто, існують $x_1, x_2, \ldots, x_s \in X : X = G = \sqcup_{j=1}^{s} O(x_j)$ (тобто, $O(x_i) \cap O(x_j) = \emptyset$ при $i \neq j, \ i, j \in \{1, 2, \ldots, s\}$), звідки

$$|G| = \sum_{j=1}^{s} |O(x_j)|.$$

Для кожного $j = 1, 2, \ldots, s$ виконується $|O(x_j)| = \frac{|G|}{|\mathrm{St}(x_j)|}$. Для кожного $j = 1, 2, \ldots, s$ можливі два випадки: $\mathrm{St}(x_j) \neq G$ або $\mathrm{St}(x_j) = G$. Якщо $\mathrm{St}(x_j) \neq G$, то, за нашим припущенням щодо власних підгруп, $p \mid \frac{|G|}{|\mathrm{St}(x_j)|}$, або $p \mid |O(x_j)|$. Якщо $\mathrm{St}(x_j) = G$, то $|O(x_j)| = \frac{|G|}{|\mathrm{St}(x_j)|} = \frac{|G|}{|G|} = 1$.

Відзначимо, що $O(e) = \{(g, e) \mid g \in G\} = \{geg^{-1} \mid g \in G\} = \{e\}$, тобто $|O(e)| = 1$. Ми отримали, що в множині $X = G$ є орбіти, які складаються з одного елемента. Нехай $t, 1 \leq t \leq s$, таке що $|O(x_1)| = |O(x_2)| = \ldots = |O(x_t)| = 1$, а $\forall j \geq (t + 1) : \quad |O(x_j)| > 1$ (за необхідності перенумеруємо елементи $x_1, x_2, \ldots, x_s$). Тоді маємо

$$|G| = \sum_{j=1}^{t} |O(x_j)| + \sum_{j=t+1}^{s} |O(x_j)| = t + \sum_{j=t+1}^{s} |O(x_j)|.$$

Як ми вже перевірили, $\forall j \geq (t+1) \ : \ p \mid |O(x_j)|$, крім того $p \mid |G|$. Висновок: $p \mid t$.

З'ясуємо, за якої умови $|O(y)| = 1$. Оскільки $y \in O(y)$ (так як $(e, y) = y$), то $|O(y)| = 1 \Leftrightarrow O(y) = \{y\}$. $O(y) = \{(g, y) \mid g \in G\} = \{gyg^{-1} \mid g \in G\} = \{y\} \Leftrightarrow gyg^{-1} = y \quad \forall g \in G \Leftrightarrow gy = yg \quad \forall g \in G$. Тобто, орбіта y містить один елемент тоді і тільки тоді, коли y належить до центру групи:

$$|O(y)| = 1 \Leftrightarrow y \in C(G) = \{z \in G \mid \forall g \in G : \ gz = zg\}.$$

Ми довели, що наша група має нетривіальний центр, при цьому $p \mid |C(G)|$.

Очевидно, що центр групи є нормальною підгрупою групи G, тобто $C(G) \triangleleft G$, при цьому $C(G)$ є абелевою групою (пояснення!).

Із основної теореми про абелеві групи, $C(G)$ є ізоморфним прямої сумі примарних циклічних груп. Оскільки $p \mid |C(G)|$, одна з цих циклічних груп має порядок p^k для деякого $k \in \mathbb{N}$. Така циклічна група має підгрупу порядку p (пояснення!). Висновок: група G має підгрупу $K < G$, таку що $|K| = p$, при цьому $K < C(G)$, тобто $K \triangleleft G$.

Розглянемо фактор-групу G/K. Маємо $|G/K| = p^{n-1}m$. За індуктивним припущенням, група G/K має підгрупу порядку p^{n-1}, $M < G/K$, $|M| = p^{n-1}$. Розглянемо канонічний гомоморфізм $f : G \to G/K$, який діє за правилом $f(g) = [g] = gK$, $g \in G$. Позначимо $S := f^{-1}(M) = \{g \in G \mid f(g) \in M\}$. Тоді $S < G$ (так як прообраз підгрупи при гомоморфізмі є підгрупою) і $K \subset S$ (так як для $k \in K$ ми маємо $f(k) = [k] = [e] \in M$). Очевидно, що гомоморфізм $f : G \to G/K$ є сюр'єктивним, за побудовою гомоморфізм $f|_S : S \to M$ є сюр'єктивним.

Ядром гомоморфізма $f: G \to G/K$ є $\mathrm{Ker}\,(f) = K$, тобто ядром гомоморфізма $f|_S$ буде $\mathrm{Ker}\,(f|_S) = K$. Для гомоморфізма $f|_S$ застосуємо твердження, що фактор-група по ядру є ізоморфною образу: $S/\mathrm{Ker}\,(f|_S) \approx M$, звідки $|S/\mathrm{Ker}\,(f|_S)| = |M|$, тобто $\frac{|S|}{|K|} = |M|$, звідки маємо $|S| = |K| \cdot |M| = p \cdot p^{n-1} = p^n$. Тобто існує $S < G$, така що $|S| = p^n$. $\square$