Действие на група върху множество

Сайт:	learn.fmi.uni-sofia.bg	Разпечатано от:	Мартин Попов
Курс:	Алгебра 2, поток 1, летен семестър 2021/2022	Дата:	Thursday, 24 March 2022, 21:21
Книга:	Действие на група върху множество		

Съдържание

1. Определение и примери

Определение:

Нека $(G, *)$ е група и $M \neq \emptyset$ е непразно множество. Казваме, че групата G действа върху множеството M, когато на произволни елементи $g \in G$ и $x \in M$ е съпоставен елемент $gx = g(x) \in M$ който принадлежи на множеството M и са изпълнени равенствата:

- $e(x) = x, \forall x \in M,$
- $(g * h)(x) = g(h(x)), \forall g, h \in G, \forall x \in M.$

Забележка: Някои автори дефинират действие на група върху множество от дясната страна, като на елементите $g \in G$ и $x \in M$ се съпоставя елемент $x^g \in M$, и са изпълнени свойствата $x^e = x$ и $x^{g_1 g_2} = (x^{g_1})^{g_2}$. Разглеждайки такова действие се получава разлика в някои от свойствата, като навсякъде където при нашите разглеждания се получат леви съседни класове, при дясното действие ще се получат десни съседни класове.

Основен пример за действие е начина на дефиниране на симетричната група.

Основен пример .

Ако $M \neq \emptyset$ е непразно множество с $S(M)$ се бележи множеството от всички биективни изображения на множеството M и по дефиниция имаме $\varphi(x) \in M$, $\forall \varphi \in S(M)$. Ако $\varphi, \psi \in S(M)$ е изпълнено :

- $id(x) = x, \forall x \in M,$
- $(\psi \circ \varphi)(x) = \psi(\varphi(x)), \forall x \in M$.

Получава се, че групата $S(M)$ действа върху множеството M.

Пример.1

Нека V е линейно пространство над полето F и с $F^* = F \setminus \{0\}$ да сме отбелязали множеството от ненулевите елементи на полето, което е група относно умножението в полето. Една от основните операции при линейното пространство е умножение на вектор със скалар,

$$\lambda \in F^* \ , \ x \in V \to \lambda x \in V.$$

Следните аксиоми от дефиницията на линейно пространство

- $1.x = x \ , \ \forall x \in V$
- $(\lambda . \mu)x = \lambda(\mu . x) \ , \ \forall x \in V$

показват, че имаме действие на групата F^* върху множеството V.

1.1. Примери 1

Пример 2.

Нека да разгледаме групата от обратимите матрици $G = GL_n(\mathbb{R})$ и $M = \mathbb{R}^n$ е множеството от n-мерните вектори. Ако $A \in GL_n(\mathbb{R})$ и $X \in \mathbb{R}^n$ разглеждаме произведението, което има в резултат също n-мерен вектор

$$A \in GL_n(\mathbb{R}),\ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n \quad \longrightarrow \quad A(X) = A.\, X = A. \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$$

От линейната алгебра е известно, че са изпълнени свойствата $EX = X$, където E е единичната матрица и $(AB)X = A(BX)$. По този начин се получава, че това съответствие задава действие на пълната линейна група върху множеството от n-мерните вектори.

Забележка:

Видяхме, че действието на група върху множество представлява изображение $\tau : G \times M \to M,\ \ \tau(g, x) = g(x) \in M,$ за което са изпълнени свойствата $\tau(e, x) = x$ и $\tau(g_1 g_2, x) = \tau(g_1, \tau(g_2, x)), \forall x \in M.$ В някои случаи е по-удобно да се разглежда действието, записано по такъв начин като функция, в която първият аргумент е от групата G, а вторият аргумент е от множеството M .

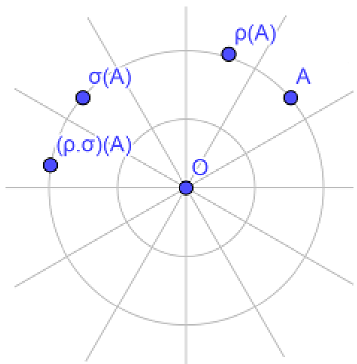
Пример 3.

Нека да разгледаме действие на целите числа $\mathbb{Z}$ върху множеството от реални числа $\mathbb{R}$, изразявайки се в умножаване по степен на числото 2. В този случай е удачно да се използва функционален запис на действието $\eta(z, x) = 2^z.\, x$. Ясно е, че са изпълнени равенствата за действие на група $\eta(0, x) = 2^0.\, x = x$, както и $\eta(z_1 + z_2, x) = 2^{z_1 + z_2} x = 2^{z_1}.\, (2^{z_2} x) = \eta(z_1, \eta(z_2, x))$

1.2. Примери 2

Пример 4.

Нека $M = \mathbb{R}^2$ е множеството на точките в Евклидовата равнина и нека G е групата от всички ротации в равнината относно фиксирана точка O. Ротациите на точките в равнината са биективни изображения на множеството от точки, освен това множеството на ротациите относно една фиксирана точка образуват група, защото композицията на ротации около една и съща точка пак е ротация около същата точка, следователно $G < S(\mathbb{R}^2)$. Съобразява се, че са изпълнени условията за действие на групата G от всички ротации около точка O, върху множеството от всички точки в Евклидовата равнина $\mathbb{R}^2$.



Пример 5.

Когато е фиксиран центъра на ротацията, тогава всяка ротация може да се опише чрез нейния ъгъл. При фиксирано начало O и описвайки ротациите чрез ъгъла (записан в радиани), можем да получим действие на адитивната група на реалните числа $(\mathbb{R}, +)$ върху множеството на точките в Евклидовата равнина $\mathbb{R}^2$. В този случай е по-удачно да се използа функционалния запис на действието и нека чрез ρ_α да записваме ротацията на ъгъл α около началната точка O. Тогава :

$$\tau : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2, \;\; \tau(\alpha, A) = B, \text{ където } \; B = \rho_\alpha(A).$$

За произволна точка A от равнината са изпълнени равенствата:

$$\begin{aligned} &\tau(0, A) = \rho_0(A) = A, \\ &\tau(\alpha+\beta, A) = \rho_{\alpha+\beta}(A) = \rho_\alpha(\rho_\beta(A)) = \tau(\alpha, \tau(\beta, A)) \end{aligned} .$$

Забележка: В последните два примера имаме действие на две различни групи $G < S(\mathbb{R}^2)$ и $\mathbb{R}$ върху едно и също множество $M = \mathbb{R}^2$ -точките от Евклидовата равнина, като и двете действия показват еднакви зависимости в равнината.

1.3. Основно свойство

Твърдение:

Нека групата G действа върху множеството M ($\forall g \in G,\ \forall x \in M \rightarrow g(x) \in M$). За $g \in G$, дефинираме изображението

$$\phi_g : M \rightarrow M,\ \phi_g(x) = g(x).$$

Тогава ϕ_g е биективно изображение на M, т.е. $\phi_g \in S(M)$ и $(\phi_g)^{-1} = \phi_{g^{-1}}$.

Доказателство:

Проверяваме, че ϕ_g е инективно и сюрективно съответствие:

- *Инекция:* Нека $x_1, x_2 \in M$, тогава

$$\begin{array}{rcl} \phi_g(x_1) = \phi_g(x_2) & \Leftrightarrow & g(x_1) = g(x_2) \Leftrightarrow \\ & \Leftrightarrow & g^{-1}(g(x_1)) = g^{-1}(g(x_2)) \Leftrightarrow \\ & \Leftrightarrow & (g^{-1}g)(x_1) = (g^{-1}g)(x_2) \Leftrightarrow \\ & \Leftrightarrow & e(x_1) = e(x_2) \Leftrightarrow \\ & \Leftrightarrow & x_1 = x_2 \end{array}$$

- *Сюрекция:* Ако $y \in M$ е произволен елемент, тогава е изпълнено $y = e(y)$ и затова $y = e(y) = (gg^{-1})(y) = g(g^{-1}(y))$, получихме, че y принадлежи на образа $\phi_g(M)$ и следователно $\phi_g(M) = M$ и изображението е сюрекция.

По този начин получаваме, че ϕ_g е биекция и принадлежи на симетричната група $\phi_g \in S(M)$.

За произволен елемент $x \in M$ проверяваме:

$$\left. \begin{array}{l} (\phi_g \circ \phi_{g^{-1}})(x) = g(g^{-1}(x)) = e(x) = x \\ (\phi_{g^{-1}} \circ \phi_g)(x) = g^{-1}(g(x)) = e(x) = x \end{array} \right\} \Rightarrow (\phi_g)^{-1} = \phi_{g^{-1}}$$

$\square$

2. Действието като хомоморфизъм на групи

В предишното твърдение установихме, че използвайки действието на група G върху множество M, всеки елемент от групата $g \in G$ определя биекция $\phi_g \in S(M)$ в множеството M. От следващата теорема ще видим, че на всяко действие на групата G върху множество M, може да се съпостави хомоморфизъм от групата G в симетричната група $S(M)$ и това съответствие е биективно. По този начин се получава, че действието на група върху множество описва (илюстрира) хомоморфизъм от G в $S(M)$.

2.1. Теорема

Теорема:

Нека G е група и M е непразно множество, тогава:

а) Двете твърдения са еквивалентни:

(1) Групата G действа върху множеството M, чрез съответствието $g, x \longrightarrow\ g(x) = \phi_g(x) \in M,\ \forall x \in M,\ \forall g \in G$.

(2) Изображението $\Phi : G \to S(M),$ където $\Phi(g) = \phi_g \in S(M)$ е хомоморфизъм на групи.

б) Съществува биективно съответствие между всички действия на групата G върху множеството M и всички хомоморфизми от вида $\Phi : G \to S(M)$.

Доказателство: а)

$(1) \Rightarrow (2):$ Нека групата G действа върху множеството M, тогава в предишното твърдение за всеки елемент от групата $g \in G$, определихме изображението $\phi_g : M \to M,\ \phi_g(x) = g(x)$, за което доказахме, че е биекция и принадлежи на симетричната група $S(M)$. Използвайки тези биекции можем да дефинираме изображение от групата G в симетричната група $S(M)$, по следния начин:

$$\Phi : G \to S(M),\ \text{където } \Phi(g) = \phi_g \in S(M).$$

За произволен елемент $x \in M$ пресмятаме

$$(\Phi(g_1 g_2))(x) = \phi_{g_1 g_2}(x) = (g_1 g_2)(x) = g_1(g_2(x))$$
$$(\Phi(g_1) \circ \Phi(g_2))(x) = \Phi(g_1)(\Phi(g_2)(x)) = \phi_{g_1}(\phi_{g_2}(x)) = g_1(g_2(x))$$

Следователно $\Phi(g_1 g_2) = \Phi(g_1) \circ \Phi(g_2)$, откъдето получаваме, че това изображение е хомоморфизъм на групи.

$(2) \Rightarrow (1):$ Нека $\Phi : G \to S(M)$ е хомоморфизъм на групи, като $\Phi(g) = \phi_g \in S(M)$ е биекция в M. За произволни елементи $g \in G$ и $x \in M$ дефинираме изображението

$$g,\ x \to\ g(x) = \phi_g(x) = (\Phi(g))(x) \in M.$$

Проверяваме дали са изпълнени условията от определението за действие на група:

- от $\Phi(e) = \phi_e = id_M$ получаваме $e(x) = \phi_e(x) = id_M(x) = x$

- от Φ хомоморфизъм имаме $\phi_{g_1 g_2} = \Phi(g_1 g_2) = \Phi(g_1) \circ \Phi(g_2) = \phi_{g_1} \circ \phi_{g_2}$, откъдето получаваме

$(g_1 g_2)(x) = \phi_{g_1 g_2}(x) = (\phi_{g_1} \circ \phi_{g_2})(x) = \phi_{g_1}(\phi_{g_2}(x)) = g_1(g_2(x))$

Получихме, че така дефинираното изображение е действие на групата G върху множеството M

б) В точка а) на всеки хомоморфизъм $\Phi : G \to S(M)$ съпоставихме действие на групата G върху множеството M и видяхме, че всяко действие на групата G върху множеството M може да се получи от такъв тип хомоморфизъм. Това означава, че разглежданото съпоставяне на хомоморфизъм (от G в $S(M)$) и действие (на групата G в множеството M) е сюрективно изображение.

За да покажем, че това съпоставяне е инективно изображение, да разгледаме два различни хомоморфизма: $\Phi : G \to S(M)$ и $\Psi : G \to S(M)$ и съответните им действия:

хомоморфизъм	действие на G върху M
$\Phi : G \to S(M) \quad \Rightarrow$	$G \times M \to M$ при което: $g, x \longrightarrow \phi_g(x) = (\Phi(g))(x) \in M$
$\Psi : G \to S(M) \quad \Rightarrow$	$G \times M \to M$ при което: $g, x \longrightarrow \psi_g(x) = (\Psi(g))(x) \in M$

Изпълнено е:

$$\begin{array}{ccc} \Phi \neq \Psi & \Leftrightarrow & \exists\, t \in G\ :\ \Phi(t) = \phi_t \neq \psi_t = \Psi(t) \in S(M) \\ & & \Updownarrow \\ & & \exists\, y \in M\ :\ \phi_t(y) \neq \psi_t(y) \\ & & \Updownarrow \\ & & \text{действията, определени от } \Phi \text{ и } \Psi \text{ са различни} \end{array}$$

Пот този начин установихме, че имаме биективно съответствие между всички действия на групата G върху множеството M и всички хомоморфизми от вида $\Phi : G \to S(M)$.

$\square$

2.2. "Точно" действие

От доказаната теорема видяхме, че когато е зададено действие на G върху множество M, тогава съществува хомоморфизъм $\Phi: G \to S(M)$. Ядрото на този хомоморфизъм се състои от всички елементи на групата G, за които е изпълнено $\Phi(g) = id_M$ и следователно

$$\mathtt{Ker}(\Phi) = \{g \in G | g(x) = x, \forall x \in M\} \lhd G$$

Когато $\mathtt{Ker}(\Phi) = \{e\}$, тогава казваме, че действието е точно (faithful).

Примери за точно действие: От показаните примери в началото, "точно" е действието на примери с номера 1,...,4.

Пример за действие, което не е точно: Пример 5 от началото е действие на група върху множество, което не е точно. Действието е $\tau: \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2, \;\; \tau(\alpha, A) = \rho_\alpha(A),$ в което ротациите в равнината ρ_α се описват чрез реалното число α, задаващо мярката на ъгъла на ротация около началната точка O. Ядрото на хомоморфизма, задаващ това действие представлява множеството от всички числа, кратни на 2π и имаме $\mathtt{Ker}(\tau) = < 2\pi >$.

Образът е съвкупността от всички ротации

$$\mathtt{Im}(\tau) = G = \{\rho_\alpha \mid \text{ротация с център } O \text{ на ъгъл } \alpha\}.$$

Поради тази причина действието (от пример 4) на групата G от всички ротации около началната точка O съответства на описаното действие $\tau: \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2.$ (от пример 5) Съответствието се състои в това, че образите на хомоморфизмите, съставени от тези две действия са една и съща група $G < S(\mathbb{R}^2)$.

2.3. Теорема на Кейли

Теорема (Кейли):
Всяка група G е изоморфна на подгрупа на симетричната група $S(G)$ и в частност, всяка крайна група от ред $|G| = n$ е изоморфна на подгрупа на S_n.

Доказателство:
Ще разгледаме действие на групата G върху множеството $M = G$ от собствените си елементи чрез умножаване отляво $g(x) = g.\, x$.
Непосредствено се проверява, че са изпълнени равенствата от дефиницията на действие:

- $e(x) = e.\, x = x,$
- $(g_1 g_2)(x) = (g_1 \,.\, g_2).\, x = g_1 \,.\, (g_2 \,.\, x) = g_1(g_2(x)).$

От доказаното в предишната теорема следва , че съществува хомоморфизъм $\Psi : G \to S(G)$, който съответства на това действие $\Psi(g)(x) = gx$. Ядрото на този хомоморфизъм се състои от тези елементи $g \in G$ на групата, за които е изпълнено

$$\Psi(g) = id \iff gx = g(x) = id(x) = x,\ \forall x \in G \iff g = e.$$

Това означава, че ядрото се състои само от единичния елемент $\mathtt{Ker}(\Psi) = \{e\}.$ От теоремата за хомоморфизмите получаваме, че $G/\{e\} \cong \mathtt{Im}(\Psi)$ известно е, че $G/\{e\} = G$, откъдето получаваме търсения изоморфизъм $G \cong G_1 = \mathtt{Im}(\Psi) < S(G)$.

В случая когато групата е крайна и има n елемента и $S(G) = S_n$, тогава получаваме $G \cong G_1 < S_n.$

□

3. Орбити и стабилизатори

При разглеждане на действие на група G върху множество M основно се интересуваме от орбитите, на които се разбива множеството M, както и от зависимостите им със стабилизаторите на елементите, които се явяват подгрупи на групата G.

3.1. Релация в множеството M

Нека G действа върху множеството M. В множеството M разглеждаме релацията "$\sim$", определена по следното правило:

$$a \sim b, \text{ когато } \exists\, g \in G, \text{ за който } g(a) = b.$$

Твърдение:
Ако групата G действа върху множеството M, тогава въведената в множеството M релация $a \sim b \Leftrightarrow g(a) = b, \text{ за } g \in G$ е релация на еквивалентност.

Доказателство:
Проверяваме, че са изпълнени изисванията за релация на еквивалентност:

- За произволен елемент $a \in M$ е изпълнено $a = e(a)$, следователно $a \sim a$;
- Ако е изпълнено $a \sim b$, тогава съществува елемент от групата, такъв че $g(a) = b$. Като действаме с обратния елемент получаваме $g^{-1}(g(a)) = g^{-1}(b)$. По този начин установихме, че $a = e(a) = g^{-1}(b)$ и следователно $b \sim a$, т.е. релацията е симетрична;
- Ако е изпълнено $a \sim b$ и $b \sim c$, тогава съществуват елементи g, h от групата, за които е изпълнено $g(a) = b$ и $h(b) = c$.
  Получаваме:

  $$(h.g)(a) = h(g(a)) = h(b) = c \implies a \sim c.$$

  Следователно въведената релация е транзитивна.

Получихме, че "$\sim$" е релация на еквивалентнтост.

$\square$

3.2. Орбити - свойства

Множеството M се разбива на класове на еквивалентност относно въведената релация $"\sim"$ получена от действието на групата G върху множеството. Тези класове на еквивалентност се наричат орбити под действието на групата G.

Определение:

Нека групата G действа върху множеството M, орбита на елемента $x \in M,$ наричаме множеството :

$$\mathcal{O}(x) = \{g(x) \mid g \in G\} = \{y \in M \mid x \sim y\} \subset M.$$

Свойството, че $"\sim"$ е релация на еквивалентност и $\mathcal{O}(x)$ са класовете на еквивалентност показват, че са в сила следните свойства за орбитите:

Свойство 1. $x \in \mathcal{O}(x), \ \forall x \in M;$

Свойство 2. $y \in \mathcal{O}(x) \ \Leftrightarrow \ x \in \mathcal{O}(y);$

Свойство 3.

$$\mathcal{O}(x) \cap \mathcal{O}(y) = \begin{cases} \emptyset, & \text{когато } y \notin \mathcal{O}(x) \\ \mathcal{O}(x) = \mathcal{O}(y), & \text{когато } y \in \mathcal{O}(x) \end{cases}$$

Свойство 4. Множеството M е обединение на непресичащи се орбити и ако $I = \{y_1, \ldots, y_s, \ldots\}$ е множество, в което сме взели по един представител от всички различни орбити, тогава

$$M = \bigcup_{x \in M} \mathcal{O}(x) = \bigcup_{y \in I} \mathcal{O}(y).$$

Свойство 5. Когато M е крайно множество и $I = \{y_1, \ldots, y_s\}$ е подмножество на M, в което сме взели по един представител от всички различни орбити, тогава

$$|M| = |\mathcal{O}(y_1)| + \ldots + |\mathcal{O}(y_s)|.$$

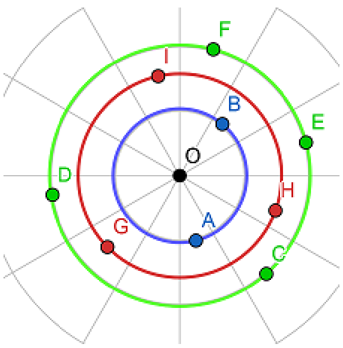
3.3. Орбити - примери

Пример 1.
Нека G е мултипликативна група и $H < G$ е нейна подгрупа. Разглеждаме действието "умножение отляво" на подгрупата H върху множеството $M = G$, състоящо се от всички елементи на групата

$$h(x) = hx \in G, \ \forall x \in G, \ \forall h \in H.$$

При това действие, орбитата на един елемент $x \in G$ по дефиниция е $\mathcal{O}(x) = \{hx | \ h \in H\},$ което съвпада точно с определението на десен съседен клас на подгрупата H, а именно $\mathcal{O}(x) = Hx.$

Пример 2:
Ако разгледаме отново M е множеството на точките в равнината $\mathbb{R}^2$ и групата G от всички ротации в равнината относно фиксирана точка O. Орбитите при това действие представляват множеството от всички концентрични окръжности относно центъра на ротациите. Само орбитата на началната точка се състои само от една точка $\mathcal{O}(O) = \{O\}.$



Пример 3:
Нека $\varphi \in S_n$ е произволен елемент от симетричната група и да разгледаме действието на цикличната подгрупа $H =< \varphi >$ върху множеството $M = \{1, 2, \ldots, n\}$. За да намерим орбитата, определена от едно число $i_1 \in M$ ще трябва последователно да пресмятаме
$i_2 = \varphi(i_1), \ldots, i_s = \varphi^{s-1}(i_1), \ldots$. Тази редица използвахме при намиране представянето на елемента φ като произведение на независими цикли и така определяхме цикъла, който съдържа числото i_1 - ако първото повторение на числа в редицата е $i_{k+1} = i_1$, то търсения цикъл е $(i_1, \ldots, i_k)$ и от дефиницията на орбита получаваме, че $\mathcal{O}_H(i_1) = \{i_1, \ldots, i_k\}$. Следователно, от представянето на елемента φ като произведение на независими цикли непосредствено се получава и разбиването на множеството $M = \{1, 2, \ldots, n\}$ като обединение на орбити при действие на групата $H =< \varphi >$:

$$\varphi = (i_1^{(1)}, \ldots, i_{k_1}^{(1)}) \circ \ldots \circ (i_1^{(s)}, \ldots, i_{k_s}^{(s)}),$$
$$\text{и } \ j_1, \ldots, j_p \text{ неподвижни точки за } \varphi$$
$$\Downarrow$$
$$\mathcal{O}_H(i_1^{(1)}) = \{i_1^{(1)}, \ldots, i_{k_1}^{(1)}\}, \ldots, \mathcal{O}_H(i_1^{(s)}) = \{i_1^{(s)}, \ldots, i_{k_s}^{(s)}\}.$$
$$\mathcal{O}_H(j_1) = \{j_1\}, \ldots, \mathcal{O}_H(j_p) = \{j_p\}$$
$$\Downarrow$$
$$M = \mathcal{O}_H(i_1^{(1)}) \cup \ldots \cup \mathcal{O}_H(i_1^{(s)}) \cup \mathcal{O}_H(j_1) \cup \ldots \cup \mathcal{O}_H(j_p)$$

3.4. Стабилизатор

Определение:
Нека групата G действа върху множеството M и $x \in M$. Стабилизатор на x наричаме множеството от всички елементи на G, които оставят x на място, т.е.

$$St_G(x) = St(x) = \{g \in G \mid g(x) = x\} \subset G.$$

Пример:
Нека разгледаме действието на S_n върху множеството от числата $M = \{1, \dots, n\}$.
Тогава стабилизатора на числото n се състои от пермутациите, които не разместват числото n и следователно, принадлежат на подгрупата S_{n-1}. По този начин се получава $St(n) = \{\varphi \in S_n | \, \varphi(n) = n\} = S_{n-1} < S_n$

Твърдение:
Нека групата G действа върху множеството M, и нека $\Phi : G \to S(M)$, е хомоморфизмът породен от действието, където $\Phi(g)(x) = g(x)$. Тогава е изпълнено:

- а) $St(x) < G, \ \ \forall x \in M;$
- б) $\mathtt{Ker}(\Phi) = \bigcap_{x \in M} St(x).$

Доказателство:
а) Нека $x \in M$, знаем че $e(x) = x$, следователно $e \in St(x)$.
Ако $g_1, g_2 \in St(x)$, тогава

$$\begin{aligned} &(g_1 g_2)(x) = g_1(g_2(x)) = g_1(x) = x, \\ &g_1(x) = x \ \Rightarrow x = (g_1^{-1} g_1)(x) = g_1^{-1}(x) \end{aligned} ,$$

следователно $g_1 \,.\, g_2$ и g_1^{-1} са елементи от стабилизатора, откъдето получаваме, че стабилизаторът на елемента x е подгрупа $St(x) < G$.

б) Нека $h \in \mathtt{Ker}(\Phi)$, което означава че образът на този елемент при хомоморфизма, описващ действието, е идентитета на множеството M и затова имаме $\Phi(h) = id_M$, откъдето получаваме, че $h(x) = id_M(x) = x, \forall x \in M.$ Получава се, че елементът $h \in \mathtt{Ker}(\Phi)$ принадлежи на стабилизаторите $h \in St(x) \forall x \in M$, следователно $\mathtt{Ker}(\Phi) \subset \bigcap_{x \in M} St(x).$

Обратно, ако $t \in \bigcap_{x \in M} St(x) \Rightarrow t(x) = x, \forall x \in M$, откъдето получаваме, че изображението $\Phi(t)$ съвпада с идентитета на множеството M. Затова от $t \in \mathtt{Ker}(\Phi)$, следва че е изпълнено включването $\bigcap_{x \in M} St(x) \subset \mathtt{Ker}(\Phi).$ По този начин установяваме, че $\mathtt{Ker}(\Phi) = \bigcap_{x \in M} St(x).$

□

3.5. Връзката орбита и стабилизатор

Теорема:
Нека групата G действа върху множеството M и $x \in M$ е произволен елемент :

а) Ако $y = g(x) \in \mathcal{O}(x)$ и $t \in G$, тогава е изпълнено

$$t(x) = y \Longleftrightarrow t \in gSt(x);$$

б) Има биективно съответствие между точките на орбитата $\mathcal{O}(x)$ и множеството от всички леви съседни класове на подгрупата $St(x)$.
в) Ако $|G : St(x)| < \infty$, тогава $|\mathcal{O}(x)| = |G : St(x)| = \dfrac{|G|}{|St(x)|}$.

Доказателство:

а) Нека $y = g(x) \in \mathcal{O}(x)$, и за елемента $t \in G$ също е изпълнено $t(x) = y$, прилагаме g^{-1} към равенството $g^{-1}(t(x)) = g^{-1}(y) = x$ следователно $g^{-1}t \in St(x)$. По този начин получаваме, че t принадлежи на левия съседен клас на стабилизатора $t \in g.\, St(x)$.

Обратно, нека $p = gh_1 \in gSt(x), h_1 \in St(x)$ е произволен елемент от левия съседен клас и за него пресмятаме $p(x) = g(h_1(x)) = g(x)$, откъдето се получава, че елемента удовлетворява условието $p(x) = y$.

б) Нека $LC_G(St(x)) = \{gSt(x) | g \in G\}$ е множеството от всички леви съседни класове на стабилизатора на x. Да разгледаме изображението

$$\eta : LC_G(St(x)) \to \mathcal{O}(x), \text{ където } \eta(gSt(x)) = g(x) \in \mathcal{O}(x),$$

Използвайки доказаното в т. а) установяваме, че това е коректно дефинирано и биективно изображение:

- *η е коректно:* От доказаното в т. а) имаме,

$$t \in g.\, St(x) \Leftrightarrow t.\, St(x) = g.\, St(x) \Rightarrow t(x) = g(x) \in \mathcal{O}(x) \Rightarrow \eta(g.\, St(x)) = \eta(t.\, St(x))$$

  и изображението не зависи от конкретния представител, с който е записан съседния клас;
- *η е инективно*: следва пак от т а):

$$\eta(gSt(x)) = \eta(tSt(x)) \Rightarrow t(x) = g(x) \in \mathcal{O}(x) \Rightarrow t.\, St(x) = g.\, St(x)$$

- *η е сюрективно:* Ако вземем произволен елемент от орбитата $y \in \mathcal{O}(x)$, тогава съществува елемент $g \in G$, за който е изпълнено $y = g(x) = \eta(g.\, St(x))$, следователно y принадлежи на образа на η.

в) Ако множеството $LC_G(St(x))$ от левите съседни класове е крайно, от изоморфизма в т. б) получаваме, че индексът на подгрупата е равен на броя на точките в орбитата, а ако групата G е крайна може да се приложи теоремата на Лагранж:

$$|\mathcal{O}(x)| = |LC_G(St(x)| = |G : St(x)| = \frac{|G|}{|St(x)|}.$$

$\square$

3.6. Пример

Пример:

Да разгледаме действието на групата $H = < \sigma >$ върху множеството $M = \{1, \ldots, 8\}$, където $\sigma = (1, 3, 5, 7) \circ (2, 4, 8) \in S_8$. Редът на елемента σ е 12 и групата е циклична с 12 елемента. Орбитите, на които се разбива множеството са:

$$\mathcal{O}(1) = \{1, 3, 5, 7\}, \ \ \mathcal{O}(2) = \{2, 4, 8\}, \ \ \mathcal{O}(6) = \{6\}.$$

За да пресметнем стабилизаторите, използваме, че

$$\sigma^k = (1, 3, 5, 7)^k \circ (2, 4, 8)^k$$

.

Редът на цикъла $(1, 3, 5, 7)$ е 4 и затова стабилизаторите на елементите $1, 3, 5, 7$ съдържат елементи от вида σ^{4t} и се получава

$$St(1) = \{id, \sigma^4, \sigma^8\} = St(3) = St(5) = St(7)$$

Аналогично, за да принадлежи елемента σ^k на стабилизатора на числото 2, трябва 3 да е делител на степента k:

$$St(2) = \{id, \sigma^3, \sigma^6\ , \sigma^9\} = St(4) = St(8)$$

Изпълнено е, че $\{\sigma, \sigma^4, \sigma^7, \sigma^{10}\}$ е съседен клас на $St(2)$ и от $4 = \sigma(2) \in \mathcal{O}(2)$ получаваме и

$$4 = \sigma(2); \ 4 = \sigma^4(2); \ \ 4 = \sigma^7(2); \ \ 4 = \sigma^{10}(2)$$

Аналогично, от $5 \in \mathcal{O}(1)$ и $5 = \sigma^2(1)$, може да се получи $5 = \sigma^6(1); \ \ 5 = \sigma^{10}(1).$

3.7. Стабилизатори на елементи от една орбита

Следващото твърдение е много полезно при решаване на някои конкретни задачи за действие на група, което ни показва, че стабилизаторите на точките от една орбита са спрегнати помежду си подгрупи на G:

Твърдение:

Нека групата G действа върху множеството M, $x \in M$ и $y = g(x) \in \mathcal{O}(x)$, тогава $St(y) = gSt(x)g^{-1}$.

Доказателство:

Нека $y = g(x) \in \mathcal{O}(x)$, тогава имаме

$$\begin{array}{rl} \text{Ако } h \in St(x) \Rightarrow & ghg^{-1}(y) = ghg^{-1}(gx) = gh(x) = g(x) = y \\ & \Downarrow \\ & ghg^{-1} \in St(y) \end{array}$$

По този начин се получава $gSt(x)g^{-1} \subset St(y)$.

За обратното включване нека от равенството $y = g(x)$ да получим $g^{-1}(y) = x$ и да вземем произволен елемент $t \in St(y)$, тогава:

$$\begin{array}{rl} y = t(y) \Rightarrow & x = g^{-1}(y) = g^{-1}(t(y)) = g^{-1}t(g(x)) \Rightarrow \\ \Rightarrow & h_1 = g^{-1}tg \in St(x) \Rightarrow \\ \Rightarrow & t = g(g^{-1}tg)g^{-1} = gh_1g^{-1} \in g(St(x))g^{-1} \end{array}$$

Получихме включването $St(y) \subset gSt(x)g^{-1}$ и окончателно получаваме $St(y) = gSt(x)g^{-1}$.

По този начин се получава че стабилизаторите на елементите в орбитата $\mathcal{O}(x)$ са всички подгрупи, които са спрегнати с $St(x)$.

□

3.8. Транзитивно действие

Определение:

Казваме, че групата G действа транзитивно върху множеството M, ако за всяка двойка елементи $x, y \in M$ съществува елемент $g \in G$, така че $y = g(x)$.

Като сравним това определени с дефиницията за орбита , установяваме че групата G действа транзитивно върху множеството M, когато всички елементи от множеството са от една орбита при това действие $M = \mathcal{O}(x)$.

Пример на транзитивно действие е действието на симетричната група S_n върху множеството $\{1, \dots, n\}$.

Следствие:

Ако крайната група G действа транзитивно върху множеството M, тогава $|M| \mid |G|$.

3.9. Брой елементи в M

Теорема:

Ако групата G действа върху крайното множество M, и $x_1, \ldots, x_s$ са по един представител от всички орбити при това действие, тогава

$$|M| = |G : St(x_1)| + \ldots + |G : St(x_s)|$$

В случая, когато G е крайна група, е изпълнено:

$$|M| = |G|. \sum_{i=1}^{s} \frac{1}{|St(x_i)|}.$$

Доказателство:

От доказаното свойство, че множеството M е обединение на непресичащи се орбити и $x_1, \ldots, x_s$ са по един представител от всички орбити, и като приложим полученото от предната теорема и теоремата на Лагранж, получаваме:

$$\begin{aligned} |M| = \quad & |\mathcal{O}(x_1)| + \ldots + |\mathcal{O}(x_s)| = \\ = \quad & |G : St(x_1)| + \ldots + |G : St(x_s)| = \\ = \quad & \frac{|G|}{|St(x_1)|} + \ldots + \frac{|G|}{|St(x_s)|} \end{aligned}$$

□

4. Спрягането като действие

Използвайки спрягането в една група G, можем да дефинираме следното съответствие:

$$g \in G, x \in G \quad \rightarrow \quad g[x] = gxg^{-1} \in G$$

Проверяваме, че то изпълнява условията за действие на групата G върху множеството $M = G$ от собствените си елементи:

$$e[x] = exe^{-1} = x$$
$$(g_1 g_2)[x] = (g_1 g_2)x(g_1 g_2)^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1} = g_1[g_2[x]]$$

Забележка: Ако групата G е Абелева, тогава за произволен елемент g действието спрягане е идентитета $g[x] = gxg^{-1} = x$ и всички елементи остават неподвижни при това действие.

4.1. Център на група

При това действие съществена роля играе центърът на групата.

Определение:

Център на група, наричаме множеството от всички елементи, които комутират с всеки елемент от групата:

$$\mathbf{Z}(G) = \{a \mid a.x = x.a,\ \forall x \in G\}$$

Лема:

Нека G е група, тогава $\mathbf{Z}(G) \lhd G$ и групата G е Абелева група, тогава и само тогава, когато $G = \mathbf{Z}(G)$.

Доказателство:

Нека $a, b \in \mathbf{Z}(G)$, и $x, g \in G$ са произволни елементи от групата:

$$\begin{aligned} (ab)x = a(bx) = a(xb) = (xa)b = x(ab), &\quad \Rightarrow ab \in \mathbf{Z}(G) \\ ax = xa \Rightarrow x = a^{-1}xa \Rightarrow xa^{-1} = a^{-1}x &\quad \Rightarrow a^{-1} \in \mathbf{Z}(G) \\ (gag^{-1})x = (gg^{-1})ax = xa = xa(gg^{-1}) = x(gag^{-1}) &\quad \Rightarrow gag^{-1} \in \mathbf{Z}(G) \end{aligned}$$

Следователно центърът е нормална подгрупа $\mathbf{Z}(G) \lhd G$.

Ако групата G е Абелева група, тогава за произволни елементи от групата имаме $ab = ba$, следователно всеки елемент принадлежи на центъра. Обратно, ако всеки елемент от групата принадлежи на центъра, тогава той комутира със всеки друг елемент и затова групата е Абелева.

□

4.2. Свойства

Определение:

Клас спрегнати елементи на елемента $a \in G$ се нарича множеството

$$C(a) = \{gag^{-1} \mid g \in G\}.$$

Определение:

Централизатор на елемента $a \in G$ се нарича множеството

$$\mathbf{Z}(a) = \{g \mid gag^{-1} = a\} = \{g \mid ga = ag\}.$$

При така дефинираното действие чрез спрягане на групата върху елементите си, орбитата на елемента a представлява точно класа спрегнати елементи $\mathcal{O}(a) = C(a),$ а централизатора е стабилизатора на елемента при при това действие $St(a) = \mathbf{Z}(a).$

Следващото твърдение задава връзката на центъра на групата с действието спрягане.

Лема:

Нека G е група $\Psi : G \to S(G)$ е хомоморфизма, който се поражда от разглеждането на спрягането като действие на група $\Psi(g) : x \to g[x] = gxg^{-1}$. Тогава:

$$\text{а) } \mathbf{Z}(G) = \mathtt{Ker}(\Psi) = \bigcap_{a \in G} \mathbf{Z}(a)$$

$$\text{б) } a \in \mathbf{Z}(G) \Longleftrightarrow C(a) = \{a\}.$$

Доказателство:

а) Ясно е, ако $a \in \mathbf{Z}(G)$ е произволен елемент от центъра, тогава всички равенства $ax = xa, (\forall x \in G)$, записани във вида $axa^{-1} = x, (\forall x \in G)$ ни показват, че $\Psi(a) = id$ и $\mathbf{Z}(G) \subset \mathtt{Ker}(\Psi).$

Ако g е елемент от ядрото на хомоморфизма, тогава образът му е единичния елемент (т.е. идентитета) при това действие и $\Psi(g) = id = \Psi(e)$, т.е. $g[x] = x = e[x],\ \forall x$. От това получаваме $gxg^{-1} = x$, и $gx = xg,\ (\forall x)$ и $g \in \mathbf{Z}(G)$, следователно $\mathtt{Ker}(\Psi) \subset \mathbf{Z}(G).$

Равенството $\mathbf{Z}(G) = \bigcap_{a \in G} \mathbf{Z}(a)$ следва от доказаното свойство за стабилизаторите.

б) От схемата, лесно се вижда, че твърдението е изпълнено

$$\begin{array}{ccc} a \in \mathbf{Z}(G) & \Leftrightarrow & ax = xa, (\forall x \in G) \\ & & \Updownarrow \\ C(a) = \{a\} & \Leftrightarrow & a = xax^{-1}, (\forall x \in G) \end{array}.$$

$\square$

4.3. Формула за класовете

Теорема: [*формула за класовете спрегнати елементи]*

Нека G е, крайна група и $x_1, \ldots, x_s$ са по един представител на онези спрегнати класове, които имат повече от един елемент. Тогава броя на спрегнатите елементи във всеки клас спрегнати елементи дели реда на групата {($|C(x_i)| \mid |G|$)} и е изпълнено:

$$|G| = |\mathbf{Z}(G)| + |C(x_1)| + \ldots + |C(x_s)|,$$

$$|G| = |\mathbf{Z}(G)| + \frac{|G|}{|\mathbf{Z}(x_1)|} + \ldots + \frac{|G|}{|\mathbf{Z}(x_s)|}$$

Доказателство:

Пресмята се броят на елементите в класовете спрегнати елементи, които се явяват орбити при действието на групата чрез спрягане върху множеството от собствените си елементи. От доказаната теорема имаме, че е изпълнено $|C(x_i)| = |G : \mathbf{Z}(x_i)|$, откъдето от следствие на теоремата на Лагранж получаваме, че $|C(x_i)|$ дели реда на групата.

От Лемата за центъра имаме, че центъра $\mathbf{Z}(G) = \{a_1, \ldots, a_m\} = C(a_1) \cup \ldots \cup C(a_m)$ е обединение на тези класове, които се състоят от по един елемент.

Използваме, че централизаторите $\mathbf{Z}(x_i)$ са точно стабилизаторите при това действие и прилагаме Теорема за орбитите, за да получим търсеното равенство.

$$\begin{gathered}
G = C(a_1) \cup \ldots \cup C(a_m) \cup C(x_1) \cup \ldots \cup C(x_s) \\
\Downarrow \\
G = \mathbf{Z}(G) \cup C(x_1) \cup \ldots \cup C(x_s) \\
\Downarrow \\
|G| = |\mathbf{Z}(G)| + |C(x_1)| + \ldots + |C(x_s)|, \\
\Downarrow \\
|G| = |\mathbf{Z}(G)| + \frac{|G|}{|\mathbf{Z}(x_1)|} + \ldots + \frac{|G|}{|\mathbf{Z}(x_s)|}
\end{gathered}$$

$\square$

5. Приложение

Действието на група върху множество се прилага много често при доказване на някои от възловите теореми в алгебрата.

Като пример са дадени няколко теореми, чието доказателство лесно се получава използвайки подходящо подбрани множества и действие на група върху тях.

5.1. p- групи

Определение:

Ако група G има ред p^k, където p е просто число, тогава групата се нарича p-група.

Теорема:

Ако G е крайна група, от ред $|G| = p^k$ където p е просто число, тогава групата има нетривиален център

$$\mathbf{Z}(G) \neq \{e\}.$$

Доказателство:

Разглеждаме действието на групата върху собствените си елементи чрез спрягане и прилагаме формулата за класовете спрегнати елементи

$$|G| = |\mathbf{Z}(G)| + |C(x_1)| + \ldots + |C(x_s)|$$

Елементите $x_1, \ldots, x_s$ са по един представител на онези спрегнати класове, които имат повече от един елемент и затова $|C(x_i)| \mid p^k$, следователно $|C(x_i)| = p^{m_i},$ където $1 \leq m_i < k$.

Пресмятаме броя на елементите в центъра на групата

$$|\mathbf{Z}(G)| = |G| - |C(x_1)| - \ldots - |C(x_s)| = p^k - p^{m_1} - \ldots - p^{m_s},$$

и получаваме, че простото число p дели $|\mathbf{Z}(G)|$. Знаем, че центърът на групата е подгрупа и затова $|\mathbf{Z}(G)| = p^m,\ m \geq 1$ и групата има нетривиален център.

$\square$

Следствие:

Ако G е крайна група, от ред $|G| = p^2$ където p е просто число, тогава групата е Абелева.

Доказателство:

От доказаното в предната теорема имаме, че групата G има нетривиален център. Следователно $|\mathbf{Z}(G)| = p$ или $|\mathbf{Z}(G)| = p^2$.

Допускаме, че $|\mathbf{Z}(G)| = p$ и да изберем елемент $x \in G \setminus \mathbf{Z}(G)$ който не принадлежи на центъра на групата. На централизатора на елемента x, (който е подгрупа на G) принадлежат всички елементи от центъра на групата и освен това и самия елемент x, защото $x = x.\,x.\,x^{-1}$.

Получи се, че $|\mathbf{Z}(x)| \geq p + 1$ откъдето $|\mathbf{Z}(x)| = p^2 = |G|$. Следователно за елемента x е изпълнено $xg = gx, \forall g \in G$, т.е. x принадлежи на центъра на групата, което е в противоречие с допускането.

Получихме, че единствената възможност е $|\mathbf{Z}(G)| = p^2 = |G|$, което означава, че групата е Абелева.

$\square$

5.2. елемент от ред p

Следващата теорема обобщава доказаното твърдение, че в група от ред четно число има елемент от ред 2. Тя се явява частен случай на теорема на Силов, според която ако p е просто число и $p^k \mid |G|$, тогава в групата има подгрупа от ред p^k.

Теорема:

Ако G е крайна група, и p е просто число, което дели реда на групата $(p \mid |G|)$, тогава в групата има елемент от ред p.

Доказателство:

- *Намираме подходящо множество:* Да разгледаме множеството от вектори, имащи дължина p, с координати елементи на групата G, имащи произведение равно на единичния елемент на групата G.

$$M = \{X = (x_1, \ldots, x_p) \mid x_i \in G, \ \text{за които } x_1.x_2 \ldots x_p = e\ \}$$

Един елемент $Y = (y, \ldots, y) \in M$ от множеството има равни координати, точно когато $y^p = e$, в групата G такива са само единичния елемент и елементите от ред p.

За да пресметнем броя на елементите в множеството M, съобразяваме, че ако вземем $x_1, \ldots, x_{p-1} \in G^{p-1}$ - произволен набор от $p-1$ елемента от групата G, тогава той еднозначно може да се допълни до вектор от множеството M по следния начин

$$x_1, \ldots, x_{p-1} \in G^{p-1} \ \rightarrow \ (x_1, \ldots, x_{p-1}, (x_1. \ldots . x_{p-1})^{-1}) \in M$$

Получаваме, че броят на елементите в множеството е $|M| = |G|^{p-1}$ и се дели на простото число p.

- *Определяме група, действаща върху множеството*: Нека $\sigma = (1, 2, \ldots, p) \in S_p$, и да разлеждаме изображението

$$\sigma(x_1, \ldots, x_p) = (x_{\sigma(1)}, \ldots, x_{\sigma(p)}) = (x_2, \ldots, x_p, x_1).$$

Ясно е, че ако $(x_1, \ldots, x_p) \in M$ следва, че $\sigma(x_1, \ldots, x_p) \in M$, защото $x_1.x_2 \ldots x_p = e \ \Rightarrow \ (x_2 \ldots x_p).x_1 = e$. По този начин се получава, че цикличната група $H =< \sigma >\subset S_p$ от ред p действа върху множеството M. При това действие един елемент $X = (x_1, \ldots, x_p) \in M$ образува орбита с дължина 1, когато всички координати на вектора са равни помежду си, защото

$$\sigma(X) = X \Leftrightarrow (x_1, \ldots, x_p) = (x_2, \ldots, x_p, x_1) \Leftrightarrow x_1 = x_2 = \ldots = x_p$$

- *Използваме свойства на действието на групата върху множеството:* При дефинираното действие орбитите на елементите имат дължини 1 или p.

Ако множеството M се разбива на t орбити с дължина p и s орбити с дължина 1, тогава прилагайки формулата за броя на елементите в множеството получаваме $|M| = s + t.p$, откъдето виждаме, че $s = |M| - tp$ се дели на p. Известно ни е, че $s \geq 1$, защото $(e, \ldots, e) \in M$ и $\mathcal{O}((e, \ldots, e)) = \{(e, \ldots, e)\}$, следователно $s \geq p$, като в групата има поне $p-1$ елемента от ред p.

□