Съседни класове. Теорема на Лагранж. Следствия.

Нека G е група, а H е нейна подгрупа. Нека $x \in G$ е произволен елемент. Множеството

$$xH = \{xh \mid h \in H\} \subseteq G$$

се нарича *ляв съседен клас на G по H с представител елемента x*. Аналогично, дефинираме множеството

$$Hx = \{hx \mid h \in H\} \subseteq G$$

се нарича *десен съседен клас на G по H с представител x*. Тривиални примери за съседни класове получаваме при $H = G$, където $xG = G$ за $\forall x \in G$, както и при $H = \{1\}$, при което имаме $xH = \{x\}$. В общия случай $xH \neq xH$ и $xH \neq H$ и съседните класове не са подгрупи на G.

Свойства:

Ще покажем свойства само на левите съседни класове, които по аналогичен начин се превеждат и за десните. Нека G е група, $H \leq G$ и $x \in G$. Тогава:

1. Всеки елемент на G се съдържа в някой ляв съседен клас на G по H. Наистина, за произволно $x \in G$ имаме, че $x = xe$ и $e \in H$. Следователно $x \in xH$.

2. $xH = H \Leftrightarrow x \in H$. Необходимост: От свойство 1 имаме, че $x \in xH$, но $xH = H$ и следователно $x \in H$. Достатъчност: Нека $x \in H$. Тогава за проиволен елемент $y \in xH$ е в сила, че $y = xh$ за някой елемент $h \in H$. Сега от $x \in H$ и $h \in H$ следва, че трябва $y \in H$ и оттук получаваме включването $xH \subseteq H$. От друга страна, за произволен елемент $h \in H$ имаме $h = eh = (xx^{-1})h = x(x^{-1}h)$. Сега от $h \in H$ и $x \in H$ следва, че трябва $x^{-1}h \in H$. Оттук пък получаваме, че $x(x^{-1}h) \in xH$, т.е. че

$h \in xH$. По този начин доказахме и обратното включване $H \subseteq xH$ и следователно $H = xH$.

3. Нека $x, y \in G$. Тогава $y \in xH \Leftrightarrow xH = yH$. (В частност това означава, че всеки елемент $y \in xH$ е представител на същия съседен клас.) Необходимост: Нека $y \in xH$, т.е. $y = xh$ за някой елемент $h \in H$. За произволен елемент $u \in yH$ имаме, че $u = yh_1$ за някой елемент $h_1 \in H$. Сега имаме $u = yh_1 = (xh)h_1 = x(\underbrace{hh_1}_{\in H})$, което означава, че $u \in xH$ и по този начин $yH \subseteq xH$. За произволен елемент $v \in xH$ имаме, че $v = xh_2$ за някой елемент $h_2 \in H$. Имайки предвид, че $y = xh$, от което следва, че $x = yh^{-1}$, получаваме $v = xh_2 = (yh^{-1})h_2 = y(\underbrace{h^{-1}h_2}_{\in H})$, което означава, че $v \in yH$, откъдето следва и обратното включване $xH \subseteq yH$. Така $xH = yH$. Достатъчност: Нека $xH = yH$. Тогава $y \in yH = xH$ и директно $y \in xH$.

4. Нека $x, y \in G$. Тогава $xH = yH \Leftrightarrow x^{-1}y \in H$ (или еквивалентно $y^{-1}x \in H$, което следва и от факта, че $x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H$). Необходимост: Нека $xH = yH$. Тогава от свойство 3 следва, че $y \in xH$, което означава, че $y = xh$ за елемент $h \in H$. Но тогава $x^{-1}y = h \in H$. Достатъчност: Нека $x^{-1}y \in H$ и $x^{-1}y = h \in H$. Това ни дава, че $y = xh$ и $x = yh^{-1}$. За всеки елемент $u \in xH$ имаме, че $u = xh_1$ за някакъв елемент $h_1 \in H$. Сега, $u = (yh^{-1})h_1 = y(\underbrace{h^{-1}h_1}_{\in H})$, откъдето следва включването $xH \subseteq yH$. За всеки елемент $v \in yH$ имаме, че $v = yh_2$ за някакъв елемент $h_2 \in H$ и така $v = (xh)h_2 = x(\underbrace{hh_2}_{\in H})$, откъдето пък следва обратното включване $yH \subseteq xH$. Окончателно това ни дава, че $xH = yH$.

5. Ако $x, y \in G$, то или $xH = yH$, или $xH \cap yH = \varnothing$. Наистина, ако $xH = yH$, то първият случай е изпълнен и няма какво да доказваме. Нека сега $xH \neq yH$ и да допуснем, че $xH \cap yH \neq \varnothing$. Тогава $\exists z \in xH \cap yH$, т.е. $z \in xH$ и едновременно с това $z \in yH$. Тогава според свойство 3 имаме, че $xH = zH$ и $yH = zH$, което ни дава противоречието $xH = yH$. Следователно остава да е вярно $xH \cap yH = \varnothing$.

Оттук се вижда, че ако $x \in G$, xH е левият съседен клас на G по H и имаме, че $xH \neq H$, то $H = eH$ и $xH \cap eH = \varnothing$. По този начин $e \notin xH$ и xH няма как да е подгрупа на G.

6. За всеки елемент $x \in G$ е в сила $|xH| = |H|$, т.е. броят на елементите

на xH е равен на реда на H. Наистина, да разгледаме изображението

$$\varphi : H \longrightarrow xH,$$

дефинирано с $\varphi(h) = xh$ за всеки елемент $h \in H$. За всеки елемент $y \in xH$ имаме, че $y = xh$ за някакъв елемент $h \in H$. Следователно $y = \varphi(h)$, т.е. всеки елемент от xH е образ на елемент от H под действието на φ и по този начин φ е сюрективно. Нека сега $h_1, h_2 \in H$ са такива, че $h_1 \neq h_2$. Ако допуснем, че $\varphi(h_1) = \varphi(h_2)$, получаваме равенството $xh_1 = xh_2$, което след ляво умножение с x^{-1} дава противоречието $h_1 = h_2$. Следователно остава да е вярно, че от $h_1 \neq h_2$ следва $\varphi(h_1) \neq \varphi(h_1)$, което означава, че φ е инективно изображение. По този начин φ е биекция, а xH и H са равномощни множества, което означава точно, че $|xH| = |H|$.

7. Нека L е множеството на всички леви съседни класове на G по H, а R е множеството на всички десни съседни класове на G по H. Тогава $|L| = |R|$, т.е. броят на левите е равен на броя на десните съседни класове. За да го докажем разглеждаме изображението

$$\varphi : L \longrightarrow R,$$

дефинирано с равенството $\varphi(xH) = Hx^{-1}$ за всеки елемент $x \in G$. Ще докажем, че φ е биективно. Първо, всеки елемент от R има вида Hy за елемент $y \in G$. Тогава $\exists y^{-1} \in G$ и разглеждаме левият съседен клас на G по H с представител y^{-1}, т.е. $y^{-1}H \in L$. Тогава $\varphi(y^{-1}H) = H(y^{-1})^{-1} = Hy$, откъдето следва че φ е сюрективно. Нека сега $x_1H, x_2H \in L$ са два леви съседни класа, такива че $x_1H \neq x_2H$. Ако допуснем, че $\varphi(x_1H) = \varphi(x_2H)$, получаваме че $Hx_1^{-1} = Hx_2^{-1}$. От еквивалента на свойство 4 за десни съседни класове имаме, че $x_1^{-1}(x_2^{-1})^{-1} \in H$, т.е. $x_1^{-1}x_2 \in H$. Сега, отново от свойство 4, този пътприложено за леви съседни класове, получаваме че трябва $x_1H = x_2H$, което е противоречие. Следователно $Hx_1^{-1} \neq Hx_2^{-1}$ и φ е инективно. Окончателно, φ е биекция, откъдето следва, че $|L| = |R|$.

Числото $|L| = |R|$, което току-що разгледахме се нарича *индекс на подгрупата H в G*. Означаваме го с $|G : H|$.

Примери:

1. За тривиалните подгрупи на G имаме: при $H = G$ имаме $|G : H| = |G : G| = 1$ тъй като $xG = G$ за $\forall x \in G$ и съществува единствен ляв и

единствен десен съседен клас; при $H = \{e\}$ имаме $|G : H| = |G|$, т.к. получаваме различен съседен клас $gH = \{g\}$ за всеки различен елемент $g \in G$.

2. Нека разгледаме адитивната група на целите числа $G = \mathbb{Z}$. Ако $H \leq G$ е нейна подгрупа, то знаем, че $H = m\mathbb{Z}$ за $m = 0, 1, 2, \ldots$. Нека $x \in G$. тогава ляв съседен клас на G по H с представител x е $x + H = \{x+h \mid h \in H\} = \{x+mz \mid z \in \mathbb{Z}\}$. Така $x+H$ се състои от всички числа, сравними с x по модул m. Т.к. всевъзможните остатъципри деление с m са $0, 1, \ldots, m-1$, то плучаваме, че всички съседни класове на G по H са $0 + m\mathbb{Z} = m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$. Те са m на брой и следователно индексът на H в G е $|G : H| = m$.

3. Нека $G = GL_n(F) = \{A \in F_{n\times n} \mid \det A \neq 0\}$, а $H = SL_n = \{A \in F_{n\times n} \mid \det A = 1\}$. Нека $x \in G$. Всеки елемент $y \in xH$ има вида $y = xh$ за някакъв елемент $h \in H$. Тогава $\det y = \det(xh) = \det x \det h = \det x$. Обратно, ако $g \in G$ и $\det g = \det x$, то $\det(x^{-1}g) = \dfrac{1}{\det x} \det g = 1$. Това означава, че $x^{-1}g \in H$, което дава, че $g \in xH$. По този начин открихме, за за всеки елемент $x \in G$ левият съседен клас на G по H е $xH = \{g \in G \mid \det g = \det x\}$. Аналогично и $Hx = \{g \in G \mid \det g = \det x\}$, което означава, че $xH = Hx$, т.е. за всеки елемент $x \in G$ левите и десните съседни класове съвпадат, въпреки че групата $G = GL_n(F)$ не е абелева. Още повече, индексът на H в G е равен на броят на случаите, в които детерминантата на една матрица е ненулева, т.е. $|G : H| = |F\backslash\{0\}| = |F^*| = \infty$.

Нека G е крайна група, а H е нейна подгрупа. Тогава различните леви съседни класове на G по H са краен брой: $x_1H, \ldots, x_kH$, където $k = |G : H|$ е индексът на H в G. От свойство 1 имаме, че всеки елемент на G се съдържа в някой от тези съседни класове x_iH за $i = 1, \ldots, k$. Следователно

$$G = x_1H \cup x_2H \cup \cdots \cup x_nH$$

. От свойство 5 имаме, че различните съседни калсове са непресичащи се, т.е. $x_iH \cap x_jH = \varnothing$ при $i \neq j$ и следователно

$$|G| = |x_1H| + |x_2H| + \cdots + |x_kH|.$$

От свойство 6 имаме, че за всяко $x \in G$ е изпълнено $|xH| = |H|$ което ни дава

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{k \text{ пъти}} = k|H|.$$

По този начин доказахме, че

$$|G| = |G : K||H|,$$

което всъщност гласи

Теоремата на Лагранж. *Ако G е крайна група и H е произволна нейна подгрупа, то*

$$|G| = |G : H||H|.$$

Нека сега видим няколко следствия от тази теорема.

Следствие 1. *Ако G крайна група и H е подгрупа на G, то редът на H дели реда на G и индекса на H дели реда на G*

Следствие 2. *Ако G е крайна група от ред $|G| = n$ и $a \in G$ е произволен елемент, то $|a|$ дели $|G|$. В частност $a^n = e$.*

Доказателство. Нека $|a| = r$ за $r \in \mathbb{N}$, т.е. r е най-малкото естествено число, за което $a^r = e$. Нека $H = \langle a \rangle$ е цикличната подгрупана G, породена от a. Тогава $|H| = |\langle a \rangle| = |a| = r$. От Следствие 1 имаме, че $|H|$ дели $|G|$, т.е. $r = |a|$ дели $|G| = n$. Оттук веднага следва и че $a^n = e$. □

Следствие 3. *Ако G е крайна група от ред p – просто число, то $G \cong \mathbb{C}_p$.*

Доказателство. Т.к. $|G| = p \geq 2$, то съществува елемент $a \in G$, такъв че $a \neq e$. Разглеждаме цикличната група $\langle a \rangle$, породена от a. Според Следствие 1 $|\langle a \rangle|$ дели $|G| = p$ и т.к. числото p е просто, а $a \neq e \Rightarrow |\langle a \rangle| \geq 2$, то следва, че $|\langle a \rangle| = p = |G|$. Т.к. $\langle a \rangle \leq G$, то достигаме до извода, че $G = \langle a \rangle$, т.е. G е крайна циклична група от ред p, а според класификацията на цикличните групи знаем, че в такъв случай $G \cong \mathbb{C}_p$. □

Следствие 4. *Ако $G \neq \{e\}$ е група и G няма подгрупи различни от $\{e\}$ и G, т.е. ако няма нетривиални подгрупи, то $G \cong \mathbb{C}_p$ за някое просто число p.*

Доказателство. Нека $a \in G$ е такъв, че $a \neq e$. Тогава $\langle a \rangle \leq G$ и $\langle a \rangle \neq \{e\}$, откъдето следва, че $\langle a \rangle = G$ и G е циклина група. Ако допуснем, че G е безкрайна,то според класификацията на цикличните групи $G \cong \mathbb{Z}$. Тук обаче достигаме до противоречие, т.к. $\mathbb{Z}$ има нетривиални

погрупи, откъдето следва, че ако $G \cong \mathbb{Z}$, то и G има нетривиални подгрупи. Следователно остава групата G да е крайна и $|G| = p$ за $p \in \mathbb{N}$ и от класификацията на цикличните групи знаем, че $G \cong \mathbb{C}_p$. Ако p не е просто число, то съществува число $d \in \mathbb{N}, d \neq 1$, такова че $d \mid p$ и $\mathbb{C}_d \leq \mathbb{C}_p$ е нетривиална подгрупа на $\mathbb{C}_p$, което би означавало, че G също притежава нетривиални подгрупи. Това противоречие доказва, че числото p трябва да е просто, с което следствието е доказано. $\square$