Съседни класове. Теорема на Лагранж.

Определение 1. *Нека G е група, H е подгрупа на G и $a \in G$. Множеството*

$$aH := \{ah \,|\, h \in H\}$$

се нарича ляв съседен клас на G относно H с представител a, а

$$Ha = \{ha \,|\, h \in H\}$$

е десният съседен клас на G относно H с представител a.

Твърдение 2. *Нека G е група, H е подгрупа на G и $a, b \in G$.*

(i) Определяме $a \sim_{LH} b$, ако $a^{-1}b \in H$. Тогава $\sim_{LH}$ е релация на еквивалентност, чиито класове на еквивалентност са левите съседни класове aH на G относно H.

(ii) Полагаме $a \sim_{RH} b$, ако $ba^{-1} \in H$ Тогава $\sim_{RH}$ е релация на еквивалентност, чиито класове на еквивалентност са десните съседни класове Ha на G относно H.

Доказателство. (i) Ясно е, че $a \sim_{LH} a$, защото $a^{-1}a = e \in H$. Ако $a \sim_{LH} b$, то $a^{-1}b \in H$, откъдето $(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a \in H$ и $b \sim_{LH} a$. Ако $a \sim_{LH} b$ и $b \sim_{LH} c$, то $a^{-1}b \in H$ и $b^{-1}c \in H$. Следователно $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}ec = a^{-1}c \in H$ и $a \sim_{LH} c$. Това доказва, че $\sim_{LH}$ е релация на еквивалентност.

Класовете на еквивалентност на $\sim_{LH}$ са

$$C_a = \{b \in G \,|\, a \sim_{LH} b\} = \{b \in G \,|\, a^{-1}b \in H\} = \{b \in G \,|\, b \in aH\} = aH.$$

(ii) Аналогично, $a \sim_{RH} a$, защото $aa^{-1} = e \in H$. Предположението $a \sim_{RH} b$ означава, че $ba^{-1} \in H$ и води до $(ba^{-1})^{-1} = (a^{-1})^{-1}b^{-1} = ab^{-1}$, което е еквивалентно на $b \sim_{RH} a$. Ако $a \sim_{RH} b$ и $b \sim_{RH} c$, то $ba^{-1} \in H$, $cb^{-1} \in H$, откъдето $(cb^{-1})(ba^{-1}) = ca^{-1} \in H$ и $a \sim_{RH} c$. Това доказва, че $\sim_{RH}$ е релация на еквивалентност.

Нейните класове на еквивалентност са

$$C_a = \{b \in G \,|\, a \sim_{RH} b\} = \{b \in G \,|\, ba^{-1} \in H\} = \{b \in G \,|\, b \in Ha\} = Ha.$$

□

Съгласно взаимната еднозначност на съответствието между релациите на еквивалентност и разбиванията на множество, Твърдение 2 дава следното

Следствие 3. *Нека G е група, а H е подгрупа на G. Тогава*

(i) $G = \cup_{a \in G} aH$ е разбиване в обединение на леви съседни класове, така че от $aH \cap bH \neq \emptyset$ следва $aH = bH$.

(ii) $G = \cup_{a \in G} Ha$ *е разбиване в обединение на десни съседни класове, така че от* $Ha \cap Hb \neq \emptyset$ *следва* $Ha = Hb$.

(iii) следните условия са еквивалентни:

$$aH = bH \Leftrightarrow a \sim_{LH} b \Leftrightarrow a^{-1}b \in H \Leftrightarrow b = ah \quad \text{за някое} \quad h \in H;$$

(iv)следните условия са еквивалентни:

$$Ha = Hb \Leftrightarrow a \sim_{RH} b \Leftrightarrow ba^{-1} \in H \Leftrightarrow b = ha \quad \text{за някое} \quad h \in H.$$

От свойствата на левите и десните съседни класове получаваме също следното

Следствие 4. *Нека* G *е група,* H *е подгрупа на* G *и* $a \in G$. *Тогава:*

(i) $aH = H$ *тогава и само тогава, когато* $a \in H$;

(ii) $Ha = H$ *тогава и само тогава, когато* $a \in H$;

(iii) aH *е подгрупа на* G *тогава и само тогава, когато* $aH = H$;

(iv) Ha *е подгрупа на* G *тогава и само тогава, когато* $Ha = H$.

Доказателство. (i) По определение, $eH = \{eh = h \,|\, h \in H\} = H$ за неутралния елемент e на H, така че $aH = H = eH$ е равносилно на $e \sim_{LH} a$ и се свежда до $e^{-1}a = a \in H$.

(ii) Аналогично, $He = \{he \,|\, h \in H\} = H$, откъдето $Ha = H = He$ е еквивалентно на $e \sim_{RH} a$ и означава $ae^{-1} = a \in H$.

(iii) По предположение, H е подгрупа на G. Ако aH е подгрупа на G, то неутралният елемент e на G принадлежи на aH и съществува $h \in H$ с $ah = e$. Оттук, $a = h^{-1} \in H$ и $aH = H$ съгласно (i).

(iv) Когато Ha е подгрупа на G, неутралният елемент e на G принадлежи на Ha и съществува $h \in H$ с $ha = e$. В резултат, $a = h^{-1} \in H$ и $Ha = H$ съгласно (ii).

□

Твърдение 5. *Нека* G *е група,* H *е подгрупа на* G *и* $a \in G$. *Тогава*

(i) лявата транслация $L_a : H \to aH$, $L_a(h) = ah$, $\forall h \in H$ *е взаимно еднозначно съответствие между групата* H *и левия съседен клас* aH;

(ii) дясната транслация $R_a : H \to Ha$, $R_a(h) = ha$, $\forall h \in H$ *е взаимно еднозначно съответствие между групата* H *и десния съседен клас* Ha.

В частност, ако подгрупата H *на* G *е крайна, то всеки ляв и десен съседен клас на* G *относно* H *има същият брой елементи* $|aH| = |H| = |Ha|$ *както* H.

Доказателство. (i) Изображението L_a е инективно, защото от

$$ah_1 = L_a(h_1) = L_a(h_2) = ah_2 \quad \text{за} \quad h_1, h_2 \in H$$

следва $h_1 = h_2$ след ляво умножение с $a^{-1} \in G$. Всеки елемент на aH е от вида $ah = L_a(h)$ за някое $h \in H$, така че L_a е сюрективно, а оттам и биективно изображение на H върху aH.

(ii) Съответствието R_a е инективно, защото дясното умножение с a^{-1} на предположението

$$h_1a = R_a(h_1) = R_a(h_2) = h_2a \quad \text{за} \quad h_1, h_2 \in H$$

дава $h_1 = h_2$. Всеки елемент на десния съседен клас Ha е от вида $ha = R_a(h)$ за някое $h \in H$, така че R_a е сюрективно, а оттам и биективно съответствие.

□

Твърдение 6. *Нека G е група, а H е подгрупа на G. Тогава съответствието*

$$aH \mapsto Ha^{-1}, \quad \forall a \in G$$

между левите и десните съседни класове на G относно H е взаимно еднозначно.

В частност, всяка крайна група G има един и същи брой леви и десни съседни класове относно подгрупа H. Този брой се нарича индекс на H в G и се бележи с $[G : H]$.

Доказателство. Ако $Ha^{-1} = Hb^{-1}$ за $a, b \in G$, то $a^{-1} \sim_{RH} b^{-1}$. По определение, това означава, че $b^{-1}(a^{-1})^{-1} = b^{-1}a \in H$ и е еквивалентно на $b \sim_{LH} a$. Оттук $aH = bH$ и съответствието $aH \mapsto Ha^{-1}$ между левите и десните съседни класове на G относно H е инективно. Споменатото съответствие е сюрективно, а оттам и биективно, защото всеки десен съседен клас Hb е образ на $b^{-1}H$, съгласно $H(b^{-1})^{-1} = Hb$.

□

Теорема 7. (Теорема на Lagrange:) *Ако G е крайна група, а H е нейна подгрупа, то*

$$|G| = |H|[G : H]$$

за реда $|G|$ на G, реда $|H|$ на H и индекса $[G : H]$ на H в G.

Доказателство. Да означим $k := [G : H]$. Тогава съществуват елементи $a_1, \ldots, a_k \in G$, така че

$$G = a_1H \cup a_2H \cup \ldots \cup a_kH$$

е разбиване в обединение на два по два непресичащи се леви съседни класове на G относно H. Левите транслации $L_{a_i} : H \to a_iH$ са взаимно еднозначни изображения на множества, така че $|a_iH| = |H|$ за произволно $1 \leq i \leq k$ и броят на елементите на G е

$$|G| = |a_1H| + |a_2H| + \ldots + |a_kH| = k|H| = [G : H]|H|.$$

□

Понеже индексът $[G : H]$ на H в G е естествено число, от Теоремата на Lagrange получаваме следното

Следствие 8. *Ако G е крайна група, то редът $|H|$ на всяка подгрупа H на G дели реда $|G|$ на G.*

Следствие 9. *Ако G е крайна група, то редът $\mathrm{ord}(g)$ на всеки неин елемент $g \in G$ дели реда $|G|$ на G.*

Доказателство. Редът $\mathrm{ord}(g)$ на $g \in G$ съвпада с реда $|\langle g \rangle|$ на цикличната подгрупа $\langle g \rangle$, породена от g. Следствие 9 се получава непосредствено от Следствие 8.

□

Следствие 10. *Всяка крайна група G от прост ред p е циклична от ред p.*

Доказателство. Редът на произволен елемент $a \in G \setminus \{e\}$, различен от неутралния елемент $e \in G$ е естествен делител на $|G| = p$, различен от 1. Следователно a е от ред $\mathrm{ord}(a) = p$ и цикличната подгрупа $\langle a \rangle$ на G, породена от a е от ред $|\langle a \rangle| = |G|$. Оттук, подмножеството $\langle a \rangle \subseteq G$ съвпада с множеството $\langle a \rangle = G$ и групата G е циклична.

□

Следствие 11. *Ако единствените подгрупи на група G са тривиалната $\{e\}$ и G, то G е крайна циклична група от прост ред p.*

Доказателство. Ако $a \in G \setminus \{e\}$, то цикличната група $\langle a \rangle$, породена от a е различна от $\{e\}$ и съвпада с G. Следователно $G = \langle a \rangle$ е циклична група.

Ако цикличната група $G = \langle a \rangle$ е безкрайна, то $a \in G$ е от безкраен ред и за произволно естествено число $n > 1$ подгрупата $\langle a^n \rangle$ е различна както от $\{e\}$, така и от $G = \langle a \rangle$, защото допускането $a = (a^n)^m$ изисква $1 = nm$ при $\mathrm{ord}(a) = \infty$ и води до противоречие. Това доказва, че $G = \langle a \rangle$ е крайна циклична група.

Ако редът на $G = \langle a \rangle$ е съставно естествено число mn, то $\langle a^n \rangle$ е подгрупа на $G = \langle a \rangle$ от ред $m \neq 1, mn$. Следователно $\langle a^n \rangle$ е различна от $\{e\}$ и G. Това доказва, че ако единствените подгрупи на G са $\{e\}$ и G, то G е циклична от прост ред p.

□

Следствие 12. *Ако G е крайна група и $K \subset H$ са подгрупи на G, то*

$$[G : K] = [G : H][H : K]. \tag{1}$$

Доказателство. От Теоремата на Lagrange за G и H имаме $|G| = [G : H]|H|$. Същата теорема за H и K дава $|H| = [H : K]|K|$. Следователно

$$|G| = [G : H][H : K]|K|.$$

Комбинирайки с Теоремата на Lagrange $|G| = [G : K]|K|$ за G и K получаваме (1)

□