ЛЕКЦИЯ 22
СЪСЕДНИ КЛАСОВЕ. ТЕОРЕМА НА ЛАГРАНЖ. СЛЕДСТВИЯ.

Определение. *Нека G е мултипликативна група и A, B са нейни непразни подмножества. Произведение AB на тези подмножества наричаме подмножеството на G, което се дефинира с равенството*

$$AB = \{g \in G \mid g = ab,\ a \in A \text{ и } b \in B\}.$$

Ако групата е адитивна сумата на $A+B$ се дефинира чрез равенството

$$A + B = \{g \in G \mid g = a + b,\ a \in A \text{ и } b \in B\}.$$

Забележка. *По-принцип*

$$AB \neq \{ab \mid a \in A \text{ и } b \in B\},$$

защото в дясната част може да има повторения, т. е. възможно е $ab = a_1b_1$, където $a, a_1 \in A$ и $b, b_1 \in B$, $a \neq a_1$, $b \neq b_1$. Ако обаче всичките произведения ab, $a \in A$, $b \in B$ са различни тогава равенството

$$AB = \{ab \mid a \in A \text{ и } b \in B\},$$

е вярно.

Твърдение 1. *Операцията произведение (сума) на подмножества на дадена група е асоциативна.*

Доказателство:

Нека A, B и C са подмножества на групата G. Нека $g \in (AB)C$. Тогава

$$g = g_1c,\ g_1 \in AB \text{ и } c \in C.$$

От $g_1 \in AB$ имаме

$$g_1 = ab,\ a \in A \text{ и } b \in B$$

следователно $g = (ab)c$, но $(ab)c = a(bc)$. Следователно $g = a(bc) \in A(BC)$. Доказахме, че

$$(AB)C \subseteq A(BC).$$

Обратното включване се доказва по същия начин.

Следствие. *Произведението на краен брой подмножества на дадена група не зависи от начина, по който са поставени скобите.*

Твърдение 2. *Нека G е група и H е подгрупа на G. Тогава $HH = H$.*

Доказателство:

Всеки елемент на HH е произведение на два елемента на подгрупата H следователно $HH \subseteq H$. От друга страна $HH \supseteq eH = H$, така че $HH = H$.

Определение. *Нека G е група и H е нейна подгрупа. За всеки елемент $g \in G$, произведението gH се нарича ляв съседен клас на групата G по подгрупата H. Елементът g се нарича представител на съседния клас gH.*

Твърдение 3. *Всеки ляв съседен клас по дадена подгрупа е равномощен на тази подгрупа.*

Доказателство:

Нека $H = \{e, h, f, \dots\}$. Тогава $gH \subseteq \{ge, gh, gf, \dots\}$. Понеже от $ga = gb$ следва $a = b$ в $\{ge, gh, gf, \dots\}$ няма повторения. Поради това имаме

$$gH = \{ge, gh, gf, \dots\}.$$

Разглеждаме изображението

$$\begin{aligned} e &\xrightarrow{\varphi} ge, \\ h &\xrightarrow{\varphi} gh, \\ f &\xrightarrow{\varphi} gf, \\ &\dots\dots\dots \end{aligned}$$

Ясно е че φ изобразява подгрупата H върху съседния клас gH. Понеже елементите $ge, gh, gf, \dots$ са различни, φ изобразява различните елементи в различни. И така, φ е 1-1 изображение между H и gH. Следователно

$$|gH| = |H|.$$

Твърдение 4.

$$g \in gH.$$

Доказателство:

Следва от равенството $g = ge$ и $e \in H$.

Следствие. *Вярно е равенството*

$$G = \bigcup_{g \in G} gH.$$

Твърдение 5. *Нека G е група и H е нейна подгрупа. Тогава*

$$gH = H \Leftrightarrow g \in H.$$

Доказателство:

1) Нека $gH = H$. Понеже $g \in gH$ имаме $g \in H$.

2) Нека $g \in H$. Тъй като всеки елемент на gH е произведение на два елемента от H имаме $gH \subseteq H$. За да докажем и обратното включване разглеждаме произволно $t \in H$. От очевидното равенство

$$t = g(g^{-1}t),$$

следва $t \in gH$ понеже $g^{-1}t \in H$. Доказахме и включването $H \subseteq gH$ и поради това $H = gH$.

Забележка. *От Твърдение 5 става ясно, че всяка подгрупа е ляв съседен клас и че елементите на подгрупата и само те са представители на този съседен клас. Твърдение 5 може да се разглежда като усилване на Твърдение 2.*

Твърдение 6.

$$aH = bH \Leftrightarrow a^{-1}b \in H. \quad (*)$$

Доказателство:

Очевидно е че равенството $aH = bH$ е еквивалентно на равенството $H = a^{-1}bH$. Поради това (*) следва от Твърдение 5.

Твърдение 7. *Ако $b \in aH$, тогава $bH = aH$.*

Доказателство:

От $b \in aH$ следва, че $b = ah$, където $h \in H$. Поради това $a^{-1}b = h \in H$. Съгласно Твърдение 6 $aH = bH$

Забележка. *Съгласно Твърдение 4 представителите на даден ляв съседен клас принадлежат на този съседен клас. От Твърдение 7 виждаме, че всеки елемент на даден ляв съседен клас е представител на този съседен клас.*

Твърдение 8. *Два леви съседни класа по дадена подгрупа или съвпадат или не се пресичат.*

Доказателство:

Нека H е подгрупа на дадена група и $aH \cap bH \neq \emptyset$. Тогава съществува $c \in aH \cap bH$.

$$\text{От } c \in aH \text{ и Твърдение 7 имаме } cH = aH.$$

$$\text{От } c \in bH \text{ и Твърдение 7 имаме } cH = H.$$

Следователно $aH = bH$.

Твърдение 9. *Нека G е група и H е нейна подгрупа. Елементите a, $b \in G$ принадлежат на един и същ ляв съседен клас по подгрупата H, тогава и само тогава, когато $a^{-1}b \in H$ (при адитивни операции $(-a) + b \in H$).*

Доказателство:

1) Нека $a, b \in cH$. Съгласно Твърдение 7 имаме $aH = cH$ и $bH = cH$, т. е. $aH = bH$. От Твърдение 6 сега получаваме $a^{-1}b \in H$.

2) Нека $a^{-1}b \in H$. Съгласно Твърдение 6, $aH = bH$. Съгласно Твърдение 4, $a \in aH$ и $b \in bH$. Следователно елементите a и b принадлежат на съседния клас $aH = bH$.

Определение. *Нека G е група и H е подгрупа на G. Броят на различните съседни класове на H в G се нарича индекс на подгрупата на H в групата G и се бележи с $[G : H]$.*

Теорема (на Лагранж). *Нека G е крайна група и H е подгрупа на G. Тогава $|G| = |H|.[G : H]$. Следователно $|H|$ и $[G : H]$ делят $|G|$.*

Доказателство:

Съгласно следствието от Твърдение 4 имаме

$$G = \bigcup_{g \in G} gH. \qquad (**)$$

След като в (**) оставим по едно копие от повтарящите се съседни класове, получаваме

$$G = g_1H \cup g_2H \cup \cdots \cup g_kH,$$

където съседните класове в дясната част са различни и $k = [G : H]$. Съгласно Твърдение 8, $g_iH \cap g_jH = \emptyset$, $i \neq j$. Следователно

$$|G| = |g_1H| + |g_2H| + \cdots + |g_kH|.$$

От последното равенство и Твърдение 3 следва

$$|G| = k|H|.$$

Следствие 1. *Нека G е крайна група. Тогава редът на всеки елемент от G дели реда на G.*

Доказателство:

Редът на подгрупата $\langle g\rangle$ дели $|G|$. Но редът на $\langle g\rangle$ е равен на $|g|$. Следователно $|g|$ дели |G|.

Следствие 2. *Нека G е крайна група и $|G| = n$. Тогава $g^n = e$, за всяко $g \in G$.*

Доказателство:

Нека $|g| = k$. От Следствие 1 следва, че k дели n. Следователно $n = k.s$ и

$$g^n = g^{ks} = (g^k)^s = e.$$

Задача 1. *Да се докаже, че ако редът на една група е просто число тогава тази група е циклична.*

Задача 2. *Да се докаже, че ако една крайна група има повече от един елемента и няма собствени подгрупи, тогава редът на тази група е просто число.*

Определение. *Нека G е група и H е подгрупа. Тогава произведението Hg, $g \in G$ се нарича десен съседен клас на групата G по подгрупата H. Елементът g се нарича представител на този съседен клас.*

Всички свойства на левите съседни класове, с изключение на Твърдение 6 и Твърдение 9 са верни и за десните съседни класове и се доказват по същия начин. Вместо Твърдение 6, за десните съседни класове имаме

$$Ha = Hb \Leftrightarrow ba^{-1} \in H.$$

Доказателството е същото, както доказателството на Твърдение 6. Твърдение 9 трябва да се преформулира по следния начин:

Елементите a и b принадлежат на един и същ десен съседен клас по подгрупата H, тогава и само тогава, когато $ba^{-1} \in H$.

Задача 3. *Да се докаже, че изображението*

$$gH \to Hg^{-1}$$

задава 1-1 изображение между левите съседни класове и десните съседни класове на H.

Примери.

1. Разглеждаме пълната линейна група $\mathrm{GL}_n(F)$ и нейната подгрупа $\mathrm{SL}_n(F)$. Съласно Твърдение 9 матриците A и B са в един съседен клас по подгрупата $\mathrm{SL}_n(F)$ тогава и само тогава, когато $A^{-1}B \in \mathrm{SL}_n(F)$, което означава, че $\det(A^{-1}B) = 1 \Leftrightarrow \det(A) = \det(B)$. Следователно в един съседен клас на $\mathrm{GL}_n(F)$ по $\mathrm{SL}_n(F)$ са тези и само тези матрици, които имат равни детерминанти.

2. Нека G е мултипликативна група на полето на комплексните числа. Тогава
$$H = \{z \in \mathbb{C} \mid |z| = 1\}$$
е подгрупа на G. Съгласно Твърдение 9 числата z_1 и z_2 са в един и същ съседен клас по H тогава и само тогава, когато $|z_1^{-1}z_2| = 1$, т. е. $|z_1| = |z_2|$. Следователно съседните класове по подгрупата H се състоят от комплексни числа с равни модули (геометрично съседните класове ще бъдат концентрични окръжности).

3. Разглеждаме адитивната група на $\mathbb{Z}$ и подгрупата $2\mathbb{Z}$ на четните числа. В тази ситуация, съгласно Твърдение 9, две цели числа m и n ще бъдат в един и същ съседен клас тогава и само тогава, когато $(-m + n) \in 2\mathbb{Z}$, т. е. или когато и двете числа са четни, или когато и двете числа са нечетни. Следователно съседните класове са два. Единият от тях се образува от четните числа, т. е. $2\mathbb{Z}$, а другият от нечетните.