3 Домашнее задание 1

Задача 1. Пусть G — группа, $g \in G, \operatorname{ord}(g) = m$ и $k \in \mathbb{Z}$. Найдите порядок элемента g^k.

Решение 1. Пусть $\operatorname{ord}(g^k) = d$. Тогда заметим, что $m \mid dk$. Пусть не так, $dk = qm + r$ $(0 < r < m)$. Но тогда $g^{dk} = g^{qm} \cdot g^r = g^r = 1$, противоречие с тем, что $\operatorname{ord}(g) = d$.

Тогда по определению порядка, d – минимальное натуральное, такое что $(g^k)^d = g^{kd} = 1$. Иными словами d минимально и kd делится на m. Понятно, что d должно делиться на $\frac{m}{(k,m)}$, где (k, m) – НОД чисел k, m. Поскольку нам нужно минимальное d, берем $\frac{m}{(k,m)}$.

Ответ: $\operatorname{ord}(g^k) = \frac{m}{(k,m)}$.

Задача 2. Найдите все подгруппы в группе D_4.

Решение 2. Из семинара мы знаем, что $D_4 = \{r^k s^m \mid k \in \{0, 1, 2, 3\}, m \in \{0, 1\}\}$. Понятно, что в каждой подгруппе H есть e. По теореме Лагранжа, порядок подгруппы делит порядок группы, а так как $|D_4| = 8$, то $|H| \in \{1, 2, 4, 8\}$. Переберем порядок подгруппы:

1. $H = \{e\}$
2. $H = \{e, r^2\}, H = \{e, s\}, H = \{e, r^2 s\}, H = \{e, r^3 s\}, H = \{e, rs\}$, так как $(r^2)^{-1} = r^2, s^{-1} = s, (r^2 s)(r^2 s) = (r^2 s)r(sr^{-1}) = (r^2 s)(sr^{-2}) = e, (rs)(rs) = (rs)(sr^{-1}) = e$.
4. $H = \{e, r, r^2, r^3\}, H = \{e, r^2, s, r^2 s\}, H = \{e, rs, r^3 s, r^2\}$, так как $(r^3 s)(rs) = (r^3 s)(sr^{-1}) = r^2$. Понятно, что других вариантов нет, т.к. иначе в H попали бы r, s по отдельности, а они порождают D_4.
8. $H = D_4$

Задача 3. Существует ли в группе $GL_4(\mathbb{Q})$ матрица порядка 4, все элементы которой — ненулевые числа?

Решение 3. Да. Рассмотрим матрицы:

$$A_1 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}, B_1 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}, B_2 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

И составим из них матрицу:

$$A = \begin{pmatrix} A_1 & B_1 \\ B_2 & A_1 \end{pmatrix}$$

Перемножим их блочно:

$$A^2 = \begin{pmatrix} & & & -4 \\ & & 4 & \\ & 4 & & \\ -4 & & & \end{pmatrix}, A^4 = \begin{pmatrix} 16 & & & \\ & 16 & & \\ & & 16 & \\ & & & 16 \end{pmatrix}$$

Теперь нужно просто домножить все элементы A_1, B_1, B_2 на $\frac{1}{2}$, тогда $A^4 = E$. Итоговая матрица:

$$A = \frac{1}{2} \begin{pmatrix} A_1 & B_1 \\ B_2 & A_1 \end{pmatrix}$$

Задача 4. Пусть $G = S_n$ и H — подгруппа всех подстановок, которые оставляют элемент n на месте. Опишите левые и правые смежные классы G по H.

Решение 4. Сначала поймем, что $|H| = (n-1)!, |G| = n!$, поэтому $[G : H] = n$. Теперь разберемся с левыми смежными классами. По определению, это все такие $gH = \{g \circ h \mid h \in H\}$. Утверждается, что в качестве g можно брать циклы вида (i, n), где $1 \leq i \leq n$.

Покажем, почему для различных $i_1, i_2, \sigma_1, \sigma_2$ ($\sigma_1, \sigma_2 \in H$) справедливо:

$$(i_1, n)\sigma_1 \neq (i_2, n)\sigma_2$$

Пусть не так. Понятно, что $i_1 = i_2$, потому что под действием σ_1, σ_2 элемент n остается на месте, а затем переходит в i_1 и i_2 соответственно. Теперь домножаем слева на (i_1, n) и получаем:

$$(i_1, n)(i_1, n)\sigma_1 = (i_1, n)(i_2, n)\sigma_2 \Leftrightarrow \sigma_1 = \sigma_2$$

Так как различных транспозиций n, $n \cdot |H| = n! = |G|$. Отлично, получается все левые смежные классы можно описать как $(i, n)H$.

Теперь для правых смежных классов. Утверждается, что здесь также можно брать циклы вида (i, n). Проверим, что получаются разные классы. Пусть $\sigma_1(i_1, n) = \sigma_2(i_2, n)$. Заметим, что если $i_1 \neq i_2$, то $(\sigma_1 \circ (i_1, n))(i_1) = n$, но $(\sigma_2 \circ (i_2, n))(i_1) \neq n$. Тогда $i_1 = i_2, \sigma_1 = \sigma_2$, следовательно получаются разные классы. Их также $n \cdot |H| = |G|$.

Задача 5. Докажите, что порядок конечной группы G нечетен тогда и только тогда, когда из любого ее элемента можно извлечь корень (то есть для любого $x \in G$ найдется $y \in G$, для которого $x = y^2$).

Решение 5. Сначала докажем $\Leftarrow$. Представим орграф, где ребро $a \to b$ есть тогда и только тогда, когда $a^2 = b$ ($a, b \in G$). Заметим, что теперь граф разбился на простые циклы. Почему? Исходящая степень каждой вершины $out_v = 1$, поэтому $\sum in_v = \sum out_v = |G|$. Тогда $\forall v : in_v = 1$, если не так, то существует вершина с $in_v = 0$, но такого не может быть, так как мы из каждой вершины провели ровно одно ребро.

Тогда наш граф — это просто множество простых циклов. Возьмем произвольный элемент $x \in G$. Пусть длина цикла, в котором содержится x, равна k. Тогда $x^{2^k} = x \Leftrightarrow x^{2^k - 1} = e$, из чего следует, что $\operatorname{ord}(x) \mid 2^k - 1$, следовательно $\operatorname{ord}(x) \equiv 1 \pmod 2$. Поскольку элемент был взят произвольно, $\forall x \in G : \operatorname{ord}(x) \equiv 1 \pmod 2$.

Из задачи 10 семинара мы знаем, что если $|G|$ четно, то найдется элемент порядка 2. В нашем случае все элементы имеют нечетные порядки, следовательно $|G|$ нечетно, что и требовалось.

Теперь докажем $\Rightarrow$. Для начала заметим, что $\forall g \in G : \operatorname{ord}(g) \equiv 1 \pmod 2$, потому что порядок подгрупы делит порядок группы $|G|$, $\operatorname{ord}(g) = |\langle g \rangle|$ а $|G| \equiv 1 \pmod 2$. Тогда $\forall g \in G \; \exists k \in \mathbb{Z}_{\geq 0} : g^{2k+1} = e$. Отсюда $g^{2k+2} = (g^{k+1})^2 = g$, следовательно для любого элемента определен корень, что и требовалось.