Семинар 17

1 Повторение

Утверждение о том, какими могут быть подгруппы группы целых чисел по сложению.

Левый смежный класс по некоторой подгруппе. Примеры. Лемма о том, что левые смежные классы либо не пересекаются, либо совпадают. Лемма о мощности левого смежного класса по подгруппе. Индекс подгруппы. Теорема Лагранжа.

Следствие 1: порядок элемента конечной группы всегда делит порядок группы. Следствие 2: элемент группы, возведенный в степень равную порядку конечной группы, равен тождественному. Малая теорема Ферма как следствие 3 теоремы Лагранжа.

Правый смежный класс. Определение нормальной подгруппы.

Примеры групп: группа диэдра. Построение изоморфизма D_3 и S_3. Формулировка теоремы Кэли.

2 Задачи

Пусть X – моноид. *Элемент* $x \in X$ называется *обратимым*, если существует $y \in X$ такой, что $xy = yx = 1$. *Элемент* $y \in X$ при этом называется *обратным к* x. Обозначим через G множество всех обратимых элементов моноида X. Рассмотрим некоторые свойства обратимых элементов.

1. Обратный элемент определён однозначно: если $y, y' \in X$ обратны к некоторому $x \in X$, то $y = y'$. В частности, определено отображение $\iota : G \to G$ *инверсии* (взятия обратного), которое элементу $g \in G$ ставит в соответствие обратный к нему элемент G. Обозначение: $\iota(g) = g^{-1}$.

2. Отображение ι *инволютивно*: $\iota \circ \iota = 1_G$. Другими словами, $(g^{-1})^{-1} = g$.

3. $1 \in G$ и $1^{-1} = 1$.

4. Пусть $x_1, \ldots, x_n \in X$. Если обратим каждый x_i, то произведение $x_1 \ldots x_n$ обратимо и $(x_1 \ldots x_n)^{-1} = x_n^{-1} \ldots x_1^{-1}$.

Доказательство. Пусть $x_i \in G$ для всех i. Докажем индукцией по n формулу $(x_1 \dots x_n)^{-1} = x_n^{-1} \dots x_1^{-1}$. База $n = 1$ тривиальна. Пусть формула верна для некоторого n. Тогда

$$(x_1 \dots x_n \underbrace{x_{n+1}) \cdot (x_{n+1}^{-1}}_{1} x_n^{-1} \dots x_1^{-1}) = (x_1 \dots x_n) \cdot (x_n^{-1} \dots x_1^{-1})$$

и $(x_1 \dots x_n) \cdot (x_n^{-1} \dots x_1^{-1}) = 1$ по предположению индукции. Аналогично,

$$(x_{n+1}^{-1} \dots x_2^{-1} \underbrace{x_1^{-1}) \cdot (x_1}_{1} x_2 \dots x_{n+1}) = (x_{n+1}^{-1} \dots x_2^{-1}) \cdot (x_2 \dots x_{n+1})$$

и $(x_{n+1}^{-1} \dots x_2^{-1}) \cdot (x_2 \dots x_{n+1}) = 1$ по предположению индукции (рассматриваем множество $x_2, \dots, x_{n+1}$ из n элементов). $\square$

Обратное верно, только если x_i коммутируют между собой: если обратимо произведение $x_1 \dots x_n$ и для всех $1 \le i, j \le n$ элементы x_i и x_j коммутируют, то каждый x_i обратим.

5. Множество обратимых элементов G является подгруппой в X.

Порядок $\mathrm{ord}(g)$ *элемента* g *группы* G:

$$\mathrm{ord}(g) = \begin{cases} \infty, & \text{если } g^n \neq 1 \ \forall n \in \mathbb{N} \\ k, & \text{если } \exists n \in \mathbb{N} : g^n = 1 \text{ и } k \text{ минимально среди всех таких } n \end{cases}.$$

Свойства порядка:

1. $\mathrm{ord}(x) = 1 \iff x = 1$ и $\mathrm{ord}(g^{-1}) = \mathrm{ord}(g)$;
2. если $|G| < \infty$, то $\mathrm{ord}(g) < \infty \ \forall g \in G$;
3. если $\mathrm{ord}(g) < \infty$, то $g^n = 1$ для всех $n \in \mathbb{Z}$, кратных $\mathrm{ord}(g)$;
4. обратно, если $\mathrm{ord}(g) < \infty$ и $g^n = 1$ для некоторого $n \in \mathbb{Z}$, то n кратно $\mathrm{ord}(g)$;
5. если $\mathrm{ord}(g) < \infty$, то $g^{-1} = g^{\mathrm{ord}(g)-1}$.

В общем случае, для $g, h \in G$ ничего нельзя сказать про порядок gh. Более того, для любых целых $n, m, k > 1$ существует группа G и элементы $g, h \in G$ такие, что

$$\mathrm{ord}(g) = n, \ \mathrm{ord}(h) = m, \ \mathrm{ord}(gh) = k.$$

Задача 1. Привести пример группы G и элементов $g, h \in G$ таких, что:

1. $\mathrm{ord}(g)$, $\mathrm{ord}(h)$ и $\mathrm{ord}(gh)$ конечны;
2. $\mathrm{ord}(g)$ и $\mathrm{ord}(h)$ конечны, но $\mathrm{ord}(gh) = \infty$.

Решение.

1. Любые два элемента любой конечной группы G подойдут.
2. Пусть $G = \mathrm{GL}_2(\mathbb{R})$, $g = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$ и $h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Тогда $\mathrm{ord}(g) = \mathrm{ord}(h) = 2$, но
$$gh = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix} \text{ и } hg = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix},$$
откуда $\mathrm{ord}(gh) = \mathrm{ord}(hg) = \infty$.

■

Задача 2. Найти порядок элемента группы:

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$;
2. $\frac{-\sqrt{3}}{2} + \frac{1}{2}i \in \mathbb{C}^\times$;
3. $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$.

Пусть $S \subseteq G$ – некоторое подмножество группы G. *Подгруппа $\langle S \rangle$, порождённая множеством S* – это множество слов в алфавите $\{s^{\pm 1} \mid s \in S\}$ (под пустым словом мы понимаем нейтральный элемент G). Другими словами,
$$\langle S \rangle = \{s_1^{\pm 1} \dots s_n^{\pm 1} \mid n \in \mathbb{Z}_{\geq 0} \text{ и } s_1, \dots, s_n \in S\}.$$
Говорят, что G *порождена* S, если $\langle S \rangle = G$.

Рассмотрим некоторые свойства порождающих множеств.

1. $\langle S \rangle$ – это наименьшая подгруппа в G, содержащая множество S.
2. Если $g \in G$, то $\langle g \rangle$ – это циклическая группа порядка $\mathrm{ord}(g)$.

Задача 3. Доказать, что группа $\mathbb{Z}_2 \times \mathbb{Z}_2$ порождается двумя элементами, но не порождается одним.

Пусть X – некоторое множество. Подгруппа $\mathrm{Sym}(X)$ в группе биекций $X \to X$, выделенная некоторым “естественным свойством”, называется *группой симметрий X*.

Пример 1.

1. Если X – это n-элементное множество, а свойство, которым выделено $\mathrm{Sym}(X)$ – тривиально, то $\mathrm{Sym}(X) = S_n$.

2. Если X – это группа, то среди биекций $X \to X$ естественно выделить гомоморфизмы (то есть изоморфизмы). Тогда $\mathrm{Sym}(X)$ называется группой *автоморфизмов* X и обозначается $\mathrm{Aut}(X)$.

Пусть V – это трёхмерное (или двумерное) евклидово пространство с выделенной прямоугольной системой координат. Если l – это плоскость (прямая) в V, проходящая через 0, то обозначим через T_l преобразование отражения V относительно l. Обозначим также через R^{ξ}_{ϕ} поворот V вокруг оси ξ, проходящей через 0, в положительном направлении (в случае плоскости повороты R_ϕ есть только вокруг нуля). Заметим, что $T_l^{-1} = T_l$ и $(R^{\xi}_{\phi})^{-1} = R^{\xi}_{-\phi}$.

Выделим группу $\mathrm{Sym}(V)$: пусть $\mathrm{Sym}(V)$ порождена всеми возможными отражениями и поворотами. Эта группа называется группой *движений* V и обозначается $\mathrm{O}(V)$. Имеется гомоморфизм $\det : \mathrm{O}(V) \to \{\pm 1\}$, определённый на порождающих по правилу $\det(R^{\xi}_{\phi}) = 1$ и $\det(T_l) = -1$. Если $g \in \mathrm{O}(V)$ и $\det(g) = 1$, то *движение* g называется *собственным*.

Если $X \subseteq V$ – некоторое подмножество, то под $\mathrm{Sym}(X)$ будем понимать такие биекции $X \to X$, которые получаются из движений $g \in \mathrm{O}(V)$ таких, что $g(X) = X$ (*сохраняющих* X). Группа $\mathrm{Sym}(X)$ называется группой движений X.

Задача 4.

1. Доказать, что любой элемент $\mathrm{O}(V^2)$ является либо поворотом, либо отражением.

2. Предъявить элемент $\mathrm{O}(V^3)$, который не является ни отражением, ни поворотом.