Билеты по алгебре
II семестр

Тамарин Вячеслав

21 мая 2020 г.

Оглавление

Вопрос 1 Подгруппа, порожденная множеством. Явное описание. Примеры образующих в D_n и $\mathrm{GL}_n(K)$. Понятие циклической группы.

i Подгруппа, порожденная множеством

Определение 1: Подгруппа, прожденная множеством

G — группа, $X \subset G$. Наименьшая группа $H \leqslant G$, содержащая X называется подгруппой, порожденной X.

Обозначение. $\langle X \rangle$.

Замечание. Эта группа всегда существует и совпадает с $\bigcap_{X \subset L \leqslant G} L = \langle X \rangle$

Утверждение (Явное описание порожденной подгруппы)**.**

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n} \mid x_i \in X,\ \varepsilon_i = \pm 1\}.$$

Для $n = 1$ считаем, что такое произведение равно нейтральному элементу.

Доказательство.

$\boxed{\supseteq}$ Любой элемент $x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n}$ должен принадлежать подгруппе, порожденной X, из чего следует это включение.

$\boxed{\subseteq}$ Заметим, что заданное множество — подгруппа G: произведение двух элементов и обратный элемент имеют такой же вид, нейтральный — случай с $n = 0$. Поэтому это множество — подгруппа G, содержащая X. Так как $\langle X \rangle$ — минимальная группа с этим свойством, получаем нужное включение.

□

Определение 2: Группа, порожденная множеством

Группа G называется порожденной множеством X, если $\langle X \rangle = G$. Если X конечно, имеет место обозначение $G = \langle x_1, \ldots, x_n \rangle$. Все x_i называются образующими G. Если для группы G существует такой конечный набор, она называется конечно порожденной.

Определение 3: Циклическая подгруппа

G — группа, $g \in G$. Подгруппа вида $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ называется циклической подгруппой, порожденной g.

Определение 4: Циклическая группа

Группа G называется циклической, если она порождена одним элементом, то есть $\exists g \in G \colon G = \langle g \rangle$.

ii Примеры образующих в D_n и $\mathrm{GL}_n(K)$

Образующие D_n Заметим, что одним элементом эта группа порождена быть не может, так как она не абелева.

Утверждение. *Поворот f_φ на угол $\varphi = \frac{2\pi}{n}$ и симметрия f_l относительно одной из разрешенных прямых. Тогда $\langle f_\varphi, f_l \rangle = D_n$.*

Доказательство. Любой поворот на $\frac{2\pi k}{n}$ можно получить повтором f_φ^k. Докажем, что

$$\left| \left\{ f_l^\varepsilon f_\varphi^k \;\middle|\; \varepsilon \in \{0, 1\},\ k \in \{0, \ldots, n-1\} \right\} \right| = 2n.$$

Пусть $f_l^{\varepsilon_1} f_\varphi^{k_1} = f_l^{\varepsilon_2} f_\varphi^{k_2}$. Тогда $f_l^{\varepsilon_1 - \varepsilon_2} f_\varphi^{k_1 - k_2} = \mathrm{id}$.

Если $\varepsilon_1 = \varepsilon_2$, $f_\varphi^{k_1 - k_2} = \mathrm{id} \Longrightarrow k_1 = k_2$. Иначе $f_l^\varepsilon = f_\varphi^k$, но поворот не может быть равен симметрии, так как при симметрии на месте остается только прямая, а при повороте либо одна точка, либо все пространство. □

Образующие $\mathrm{GL}_n(K)$ Здесь образующими будут матрицы элементарных преобразований: транспозиций (которые можно выразить через оставшиеся), псевдоотражения (домножение на число) и трансвекции (прибавление одной строки к другой, умноженной на число).

Вопрос 2 Порядок элемента. Эквивалентное определение. Соотношение $g^n = e$ и порядок элемента g. Порядок элемента в группе $\mathbb{Z}/n$

Определение 5: Порядок элемента

Порядок элемента $g \in G$ — количество элементов в подгруппе $\langle g \rangle$.

Обозначение. $\operatorname{ord} g$

Lemma 1. *Пусть $g \in G$. Если $\operatorname{ord} g$ конечен, то $\operatorname{ord} g = n$, где n — наименьшее натуральное число, что $g^n = e$, иначе такого n не существует.*

Доказательство.

- Пусть $g^n = e$. Докажем, что $\operatorname{ord} g \leqslant n$. Рассмотрим $\{e, g, g^2, \ldots, g^n, \ldots\}$. Начиная с g^n элементы повторяются. А именно
$$g^m = g^{nq+r} = g^r.$$
Следовательно, различных элементов группы $\langle g \rangle$ всего n.

- Пусть $\operatorname{ord} g = \infty$ и $g^n = e$ при $n \in \mathbb{N}$. но в группе $\langle g \rangle$ не более n элементов. Противоречие.

- Пусть $m = \operatorname{ord} g < \infty$. Рассмотрим $\{e, g, \ldots g^m\}$. Здесь $m + 1$ элемент, поэтому там есть два равных. Пусть $g^i = g^j \implies g^{i-j} = e$. Но тогда $|\langle g \rangle| \leqslant i - j$. Значит, $i = m, j = 0$, $g^m = e$. Также получаем, что до этого ни один $g^k = e$, поэтому, m и есть минимальное.

□

Утверждение. *Пусть $g \in G$, $g^n = e$, $n \in \mathbb{N}$. Тогда $n \,\vdots\, \operatorname{ord} n$.*

Доказательство. Поделим с остатком $n = q \cdot \operatorname{ord} g + r$, $0 \leqslant r < \operatorname{ord} g$. Тогда $e = g^n = g^r$. Если $r \neq 0$, то $g^r \neq e$. Следовательно, $r = 0$. □

Lemma 2. *Пусть G — группа, $g \in G$. Тогда существует такой единственный гомоморфизм $f\colon \mathbb{Z} \to G$, $f(1) = g$.*

Доказательство. Такой гомоморфизм существует (как задан в условии, все условия выполняются). Заметим, что $g(n) = g(1)^n = g^n$. Поэтому он задан однозначно. □

Теорема 1: Об изоморфмности циклической группы

Пусть $g \in G$ Если $\operatorname{ord} g = n$, то $\langle g \rangle$ изоморфна группе $\mathbb{Z}/n$. Если $\operatorname{ord} g = \infty$, то $\langle g \rangle$ изоморфна $\mathbb{Z}$.

Доказательство.

- Пусть $\operatorname{ord} g = n$. Построим $f\colon \mathbb{Z}/n \to G$ так $f(\overline{k}) = g^k$. Проверим корректность: пусть $k_1 \equiv k_2 \pmod n$, то есть $k_1 = k_2 + sn \implies g^{k_1} = g^{k_2} \cdot g^{sn} = g^{k_2}$. Из свойств элементов $\mathbb{Z}/n$ и f следуют необходимые условия гомоморфизма. Также заметим, что это биекция.

- Пусть $\operatorname{ord} g = \infty$. Построим гомоморфизм $f\colon f(1) = g \implies f(n) = g(1)^n = g^n$. Он сюрьективен, проверим инъективность: пусть $\ker f \neq 0$, тогда $\exists k \in \mathbb{N}\colon g^k = e$, а тогда $\langle g \rangle$ конечна. Противоречие.

□

Вопрос 3 Классификация циклических групп. Порядок элемента в циклической группе. Критерий для определения порядка, если известно отношение $g^n = e$

Lemma 3 (Порядок элемента $\mathbb{Z}/n$)**.** *Пусть* $k \in \mathbb{Z}/n$*. Тогда* $\operatorname{ord} k = \frac{n}{(n,k)}$.

Доказательство.

$$\operatorname{ord} k = \min d\colon dk \equiv 0 \pmod n \implies d = \min\left\{t\frac{n}{(n,k)}\right\}.$$

Наименьшим значением будет то, когда $t = 1$: $\frac{n}{(n,k)}$. □

Следствие 1 (Порядок элемента в циклической группе)**.** G — группа, $g \in G$, $\operatorname{ord} g = n$. Тогда $\operatorname{ord} g^k = \frac{n}{(n,k)}$.

Доказательство. Из прошлой леммы это доказано для $\mathbb{Z}/n$, а мы знаем, что $G \cong \mathbb{Z}/n$. □

Lemma 4 (Критерий определения порядка)**.** *Пусть* $g \in G\colon g^n = e$ *и* $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$*. Тогда если* $g^{\frac{n}{p_i}} \neq e \quad i$*, то* $n = \operatorname{ord} g$.

Доказательство. Пусть $m = \operatorname{ord} g$.

$$g^n = e \Longrightarrow n \vdots m.$$

Тогда, если $n \neq m$,

$$\exists p_i\colon n \vdots p_i^{\alpha_i} \wedge p_i^{\alpha_i} \nmid m.$$

Следовательно, $\frac{n}{p_i} \mid m \Longrightarrow \frac{n}{p_i} = mk$. Но тогда $g^{mk} = e$. Противоречие. Поэтому $n = m$. □