Билеты по алгебре
II семестр

Тамарин Вячеслав

31 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. $\operatorname{ord} g$

Лемма 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 $g^i = g^j \Longrightarrow g^{i-j} = e$. 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, $r = 0$. □

Лемма 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 $k_1 = k_2 + sn \Longrightarrow g^{k_1} = g^{k_2} \cdot g^{sn} = g^{k_2}$. Из свойств элементов $\mathbb{Z}/n$ и f следуют необходимые условия гомоморфизма. Также заметим, что это биекция.
- Пусть $\operatorname{ord} g = \infty$. Построим гомоморфизм $f\colon f(1) = g \Longrightarrow f(n) = g(1)^n = g^n$. Он сюръективен, 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 $g^n = e$

Лемма 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 $G \cong \mathbb{Z}/n$. □

Лемма 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 $n = m$. □

Вопрос 4 Подгруппы циклических подгрупп. Прообраз подгрупп.

Теорема 2

Пусть G циклическая и $H < G$. Тогда H тоже циклическая.

Более того, если $|G| = n$, то $\forall d\ n \vdots d\colon \exists! H \leqslant \mathbb{Z}/n\colon\ |H| = d$.

Доказательство

Рассмотрим два случая.

- $G \simeq \mathbb{Z}$.

  Лемма 5

  Пусть H — подгруппа в $\mathbb{Z}$. Тогда H циклическая.

  Доказательство

  Докажем, что $H = \langle n \rangle = n\mathbb{Z}$. Если $H = \{0\}$, то $n = 0$. Пусть m — минимальный натуральный делитель числа n. Заметим, что все $km \in H$, поэтому $\langle m \rangle = m\mathbb{Z} \subseteq H$. Пусть $x \in H,\ x \notin \langle m \rangle$. Тогда $x = km + r,\ 0 < r < m \Longrightarrow r = x - km \in H$, следовательно, m не наименьший. Противоречие.

- $G \simeq \mathbb{Z}/n$. Рассмотрим гомоморфизм, $\pi\colon \mathbb{Z} \to \mathbb{Z}/n$, $\pi(x) = \overline{x}$.

  Лемма 6

  Пусть $f\colon G_1 \to G_2$ — гомоморфизм групп, $H \leqslant G_2$. Тогда $f^{-1}(H) \leqslant G_1$.

  Доказательство

  1. $f(e) = e \Longrightarrow f^{-1}(e) = e,\ e \in H \Longrightarrow e \in f^{-1}(H)$
  2. $a = f^{-1}(x),\ x \in H \Longrightarrow f(a^{-1}) = x^{-1} \in H$
  3. $f(a), f(b) \in H \Longrightarrow f(ab) = f(a)f(b) \Longrightarrow ab \in f^{-1}(H)$

  Мы знаем, что $H \leqslant G = \mathbb{Z}/n$. По прошлой лемме $\pi^{-1}(H) \leqslant \mathbb{Z}$, поэтому $\pi^{-1}(H)$ циклическая. Из этого следует, что и H циклическая.

  Докажем существование и единственность подгруппы порядка d, если $n \vdots d$. Рассмотрим элемент $\frac{n}{d} \in \mathbb{Z}/n$, его порядок равен d, поэтому порожденная им группа будет иметь такой же порядок.

  Пусть $H = \langle x \rangle,\ \operatorname{ord} x = d$. Если отождествить этот элемент с числом, $d = \frac{n}{(n,x)}$. Тогда $\frac{n}{d} = (n, x) \Longrightarrow x \vdots \frac{n}{d} \Longrightarrow H \subseteq \langle \frac{n}{d} \rangle$. Кроме этого в обоих группах d элементов, следовательно, они совпали.

Вопрос 5 Классы смежности. Теорема Лагранжа. Следствия.

Определение 6: Отношение эквивалентности по подгруппе

Пусть $H \leqslant G$. Определим отношение эквивалентности $\sim_H$: $g_1 \sim_H g_2 \iff \exists h \in H : g_1 = g_2 h$.

Комментарий. Это отношение эквивалентности.

- $g = ge \implies g \sim_H g$
- $g_1 \sim_H g_2 \implies \exists h \in H : g_1 = hg_2 \implies h^{-1} g_1 = g_2 \implies g_2 \sim_H g_1$
- $g_1 \sim_H g_2 \sim_H g_3 \implies \exists h_1, h_2 \in H : g_1 = hg_2,\ g_2 = h_2 g_3 \implies g_1 = h_1 h_2 g_3 \implies g_1 \sim_H g_3$

Определение 7: Класс эквивалентности относительно $\sim_H$

Пусть G — группа, $H \leqslant G$, $g \in G$. Тогда множество $gH = \{gh \mid h \in H\}$ называется классом эквивалентности относительно $\sim_H$. gH — левый смежный класс g по подгруппе H.

Определение 8: Индекс

Множество всех левых смежных классов будем обозначать G/H. Количество элементов в G/H называется индексом H в G и обозначается $[G : H]$.

Следствие 2

Группа G разбивается в дизъюнктное объединение левых смежных классов $G = \bigsqcup_{gH \in G/H} gH$.

Утверждение. *Пусть H — подгруппа G и $g \in G$. Тогда отображение $H \to gH$, заданное по правилу $h \to gh$ — биекция.*

Определение 9: Порядок группы

Порядок группы G — число элементов в G.

Теорема 3: Теорема Лагранжа

Пусть G — группа, $H \leqslant G$. Пусть порядок H и индекс $[G : H]$ конечны. Тогда

$$|G| = |H| \cdot [G : H].$$

Доказательство

По следствию $G = \bigsqcup_{gH \in G/H} gH$, всего таких классов $[G : H]$, $|gH| = |H|$. Из чего и получаем нужное равенство.

Следствие 3

Пусть G — конечная группа, $H \leqslant G$. Тогда $|G| \vdots |H|$.

Следствие 4

Пусть G — конечная группа, $g \in G$. Тогда $|G| \vdots \operatorname{ord} g$.

Следствие 5

Пусть G — конечная группа порядка n, $g \in G$. Тогда $g^n = e$.

Следствие 6

Пусть G — конечная группа порядка $p \in \mathbb{P}$. Тогда $G \simeq \mathbb{Z}/p$.

Следствие 7

Пусть G — конечная группа порядка 4. Тогда $G \simeq \mathbb{Z}/4$ или $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

Следствие 8

Пусть $n \in \mathbb{N}$, $a \in \mathbb{Z}/n^*$. Тогда $a^{\varphi(n)} = 1$.

Вопрос 6 Количество элементов данного порядка в циклической группе. Тождество для функции Эйлера. Критерий цикличности. Конечные подгруппы в мультипликативной группе поля.

Лемма 7

Пусть $n \in \mathbb{N}$. Тогда $n = \sum\limits_{d|n} \varphi(d)$.

Доказательство

Рассмотрим группу $\mathbb{Z}/n$. Если $n \vdots d$, то в этой группе есть единственная подгруппа порядка d, в которой лежат все элементы порядка d. Эта группа циклическая, следовательно, таких элементов $\varphi(d)$. Тогда

$$n = |\mathbb{Z}/n| = \sum_{d|n} |\{x \in \mathbb{Z}/n \mid \operatorname{ord} x = d\}| = \sum_{d|n} \varphi(d).$$

Лемма 8

Пусть H — конечная группа, в которой число элементов $x^d = e$ не больше d. Тогда H — циклическая.

Доказательство

Пусть $|H| = n$. Пусть $x \in H$, $\operatorname{ord} x = d$. Тогда $\forall y \in \langle x \rangle \colon y^d = e$. Таких d штук. С другой стороны, в H не более d элементов, что $y^d = e$.

Рассмотрим $z \in H$, $\operatorname{ord} x = d$. Он удовлетворяет $z^d = e$, поэтому $z \in \langle x \rangle$. Но в циклической $\langle x \rangle$ ровно $\varphi(d)$ элементов порядка d. Тогда

$$n = \sum_{d|n} |\{x \in H \mid \operatorname{ord} x = d\}| \leqslant \sum_{d|n} \varphi(d) = n.$$

Следовательно, неравенство обращается в равенство, поэтому верно и неравенство для n. Значит, элементов порядка n в H ровно $\varphi(n)$. Тогда H порождена одним из них.

Теорема 4: Конечные подгруппы в мультипликативной группе поля

Пусть H — конечная подгруппа в K^*, K — поле. Тогда H циклическая.

Доказательство

Решений уравнения $x^d - 1 = 0$ в поле K не более d. Поэтому их не более d в подгруппе H. По предыдущей лемме H циклическая.

Следствие 9

Пусть $p \neq 2 \in \mathbb{P}$. Тогда группа $\mathbb{Z}/p^* \simeq \mathbb{Z}/(p-1)$.

Определение 10: Первообразный корень по модулю

Если $n \in \mathbb{N}$, число $a \colon \langle a \rangle = \mathbb{Z}/n^*$ называется первообразным корнем по модулю n.

Вопрос 7 Представление перестановки в виде произведения независимых циклов. Порядок перестановки. Обратная перестановка и ее циклическая запись.

Определение 11: Цикл

Пусть $\{a_1, \dots a_k\} \subset \{1, \dots n\}$. Цикл $(a_1, \dots, a_k)$ — такой элемент c из S_n, что

$$c(x) = \begin{cases} x, & x \notin \{a_1, \dots a_k\} \\ a_{i+1}, & x = a_i \wedge 1 \leqslant i < k \\ a_1, & x = a_k \end{cases}.$$

Замечание. Порядок $(a_1, \dots, a_k)$ равен k.

Определение 12: Неподвижная точка

Пусть $\sigma \in S_n$. Неподвижная точка — такой $x \in \{1, \dots, n\}$, что $\sigma(x) = x$.

Обозначение. $\mathrm{Fix}(\sigma)$ — множество всех неподвижных точек относительно σ.

Определение 13: Носитель

Носитель перестановки $\sigma \in S_n$ — множество $\{1, \dots, n\} \setminus \mathrm{Fix}(\sigma)$.

Обозначение. $\operatorname{supp} \sigma$.

Определение 14: Независимость перестановок

Перестановки $\sigma_1, \sigma_2 \in S_n$ называются независимыми, если $\operatorname{supp} \sigma_1 \cap \operatorname{supp} \sigma_2 = \varnothing$.

Свойства. *Две независимые перестановки коммутируют.*

Теорема 5: Разложение в произведение циклов

Пусть $\sigma \in S_n$. Тогда существует единственный с точностью до порядка набор независимых циклов $c_1, \dots, c_k$, $c_i \neq \mathrm{id}$, что $\sigma = c_1 \dots c_k$.

Доказательство

Рассмотрим все различные орбиты $\Omega_1, \Omega_2, \dots \Omega_s$. Определим перестановки c_i, $i \in \{1, \dots s\}$:

$$c_i = \begin{cases} \sigma(x), & x \in \Omega_i \\ x, & x \notin \Omega_i \end{cases}.$$

Докажем, что c_i — независимые циклы.

- $\operatorname{supp} c_i \subseteq \Omega_i$, поэтому все c_i различны.
- Докажем, что $c_i = \left(x, \sigma(x), \dots \sigma^{l-1}(x)\right), \quad l = |\Omega_i|, x \in \Omega_i$.
  - $\sigma^k(x) = x,\ k > 0 \Longrightarrow |\Omega_i| \leqslant k$
  - $\sigma^{k_1}(x) = \sigma^{k_2}(x),\ 0 \leqslant k_2 < k_1 < l \Longrightarrow \sigma^{k_2 - k_1}(x) = x \Longrightarrow |\Omega_i| \leqslant k_2 - k_1 < l$. Из чего следует, что все элементы Ω_i различны.
  - Рассмотрим элемент $\sigma^l(x) \in \{x, \sigma(x), \dots \sigma^{l-1}(x)\}$. По прошлому пункту он не может совпасть ни с кем кроме x.

  Получили, что c_i — цикл.

Докажем, что $\sigma = c_1 \dots c_s$. Пусть $x \in \Omega_i$, тогда $\sigma(x) \in \Omega_i$.

$$c_1 \dots c_s(x) = c_1 \dots c_{i-1} c_i(x) = c_1 \dots c_{i-1}(\sigma(x)) = \sigma(x).$$

Теперь докажем единственность. Пусть $\sigma = c_1 \dots c_k$. $\operatorname{supp} c_i = \Omega_j$. Порядок следования элементов в c_i определяется действием на этой орбите, так как остальные циклы независимы и не влияют на жту орбиту.

Теорема 6: Порядок перестановки

Пусть $\sigma \in S_n$ и $\sigma = c_1 \dots c_k$. Обозначим d_i за длину c_i. Тогда $\operatorname{ord} \sigma = (d_1, \dots d_k)$

Доказательство

Так как независимые перестановки коммутируют, $\sigma^d = \prod c_i^d$. Так как c_i^d тоже независимы, чтобы $\sigma^d = id$, нужно $c_i^d = id$. То есть требуется $d \vdots d_i$.

Теорема 7: Обратная перестановка в циклической записи

Пусть $c = (a_1, \dots a_k)$. Тогда $c^{-1} = (a_k, \dots a_1)$.
Если $\sigma = c_1 c_2 \dots c_s$, где c_i — независимые циклы, то $\sigma^{-1} = c_1^{-1} c_2^{-1} \dots c_s^{-1}$.

Доказательство

Так как c_i^{-1} тоже независимы, они коммутируют, поэтому можем поставить в нужном порядке.