

# Определения и формулировки по алгебре II семестр

Тамарин Вячеслав

6 июня 2020 г.

# Оглавление

Вопрос 1	Подгруппа, порожденная множеством. Явное описание. Примеры образующих в $D_n$ и $GL_n(K)$ . Понятие циклической группы. . . . .	2
i	Подгруппа, порожденная множеством . . . . .	2
ii	Примеры образующих в $D_n$ и $GL_n(K)$ . . . . .	2
Вопрос 2	Порядок элемента. Эквивалентное определение. Соотношение $g^n = e$ и порядок элемента $g$ . Порядок элемента в группе $\mathbb{Z}/n$ . . . . .	2
Вопрос 3	Классификация циклических групп. Порядок элемента в циклической группе. Критерий для определения порядка, если известно отношение $g^n = e$ . . . . .	3
Вопрос 4	Подгруппы циклических подгрупп. Прообраз подгрупп. . . . .	3
Вопрос 5	Классы смежности. Теорема Лагранжа. Следствия. . . . .	3
Вопрос 6	Количество элементов данного порядка в циклической группе. Тождество для функции Эйлера. Критерий цикличности. Конечные подгруппы в мультипликативной группе поля. . . . .	4
Вопрос 7	Представление перестановки в виде произведения независимых циклов. Порядок перестановки. Обратная перестановка и ее циклическая запись. . . . .	5
Вопрос 8	Разложение в произведение транспозиций. Знак перестановки. Знак как гомоморфизм. Знак и число транспозиций в разложении. . . . .	5
Вопрос 9	Разные способы вычисления знака перестановки. Знак обратной перестановки. Знакопеременная группа. Задача о пятнадцати. . . . .	6
Вопрос 10	Образующие $S_n$ . Сопряжение. Цикленный тип и сопряженность. Класс сопряженности произвольной перестановки. . . . .	6
Вопрос 11	$S_n$ порождена двумя образующими. Образующие $A_n$ — два типа. . . . .	7
Вопрос 12	Прямое произведение. Порядок элемента в прямом произведении. Прямое произведение и подгруппы. Образующие прямого произведения. Критерий разложимости в прямое произведение. . . . .	7
Вопрос 13	Лемма про возведение в степень по модулю $p^\alpha$ . Строение группы $\mathbb{Z}/p^\alpha$ при простом $p$ . Ответ в зависимости от разложения $p$ на множители. . . . .	7
Вопрос 14	Доказательство теоремы Рабина . . . . .	8
Вопрос 15	Сюръективный гомоморфизм и образующие. Сюръективный гомоморфизм и порядок. Нормальная подгруппа. Переформулировки. Примеры. . . . .	8
Вопрос 16	Фактор-группа. Корректность. Универсальное свойство фактора. Теорема об изоморфизме. Примеры. Простые группы. . . . .	8
Вопрос 17	Действие группы на множестве. Примеры. Действия и гомоморфизмы. Описание группы самосовмещений тетраэдра. Теорема Кэли. . . . .	9
Вопрос 18	Инвариантное подмножество. Орбита. Стабилизатор. Связь орбиты и стабилизатора. Следствие про делимость. Вычисление орбиты. Пример. . . . .	9
Вопрос 19	Теорема Коши. Ограничение числа образующих у подгруппы в $S_n$ . . . . .	9
Вопрос 20	Лемма Шрайера. Понятие о цепочке стабилизаторов и о сильном порождающем множестве. Алгоритм проверки принадлежности элемента, если известна полная цепочка стабилизаторов. . . . .	10
Вопрос 21	Лемма Бренсайда. Пример с раскраской квадрата. . . . .	10

## Вопрос 1 Подгруппа, порожденная множеством. Явное описание. Примеры образующих в $D_n$ и $GL_n(K)$ . Понятие циклической группы.

### i Подгруппа, порожденная множеством

#### Определение 1: Подгруппа, порожденная множеством

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

**Обозначение.**  $\langle X \rangle$ .

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

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

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

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

#### Определение 2: Группа, порожденная множеством

Группа  $G$  называется порожденной множеством  $X$ , если  $\langle X \rangle = G$ . Если  $X$  конечно, имеет место обозначение  $G = \langle x_1, \dots, x_n \rangle$ . 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  $\exists g \in G: G = \langle g \rangle$ .

### ii Примеры образующих в $D_n$ и $GL_n(K)$

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

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

**Образующие  $GL_n(K)$**  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.**  $\text{ord } g$

#### Лемма 1

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

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

#### Лемма 2

Пусть  $G$  — группа,  $g \in G$ . Тогда существует такой единственный гомоморфизм  $f: \mathbb{Z} \rightarrow G$ ,  $f(1) = g$ .

**Теорема 1: Об изоморфности циклической группы**

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

**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  $\text{ord } k = \frac{n}{(n,k)}$ .

**Следствие 1: Порядок элемента в циклической группе**

$G$  — группа,  $g \in G$ ,  $\text{ord } g = n$ . Тогда  $\text{ord } g^k = \frac{n}{(n,k)}$ .

**Лемма 4: Критерий определения порядка**

Пусть  $g \in G$ :  $g^n = e$  и  $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ . Тогда если  $g^{\frac{n}{p_i}} \neq e$   $\forall i$ , то  $n = \text{ord } g$ .

**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  $\forall d \mid n$ :  $d$ :  $\exists! H \leq \mathbb{Z}/n$ :  $|H| = d$ .

*Доказательство*

Рассмотрим два случая.

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

**Лемма 5**

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

- $G \simeq \mathbb{Z}/n$ . Рассмотрим гомоморфизм,  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n$ ,  $\pi(x) = \bar{x}$ .

**Лемма 6**

Пусть  $f: G_1 \rightarrow G_2$  — гомоморфизм групп,  $H \leq G_2$ . Тогда  $f^{-1}(H) \leq G_1$ .

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

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

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

**Вопрос 5 Классы смежности. Теорема Лагранжа. Следствия.****Определение 6: Отношение эквивалентности по подгруппе**

Пусть  $H \leq G$ . 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.

- $g = ge \implies g \sim_H g$
- $g_1 \sim_H g_2 \implies \exists h \in H: g_1 = hg_2 \implies h^{-1}g_1 = g_2 \implies g_2 \sim_H g_1$
- $g_1 \sim_H g_2 \sim_H g_3 \implies \exists h_1, h_2 \in H: g_1 = hg_2, g_2 = h_2g_3 \implies g_1 = h_1h_2g_3 \implies g_1 \sim_H g_3$

**Определение 7: Класс эквивалентности относительно  $\sim_H$** 

Пусть  $G$  — группа,  $H \leq G$ ,  $g \in G$ . 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  $H \rightarrow gH$ , заданное по правилу  $h \rightarrow gh$  — биекция.

**Определение 9: Порядок группы**

Порядок группы  $G$  — число элементов в  $G$ .

**Теорема 3: Теорема Лагранжа**

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

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

**Следствие 3**

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

**Следствие 4**

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

**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  $n = \sum_{d|n} \varphi(d)$ .

**Лемма 8**

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

**Теорема 4: Конечные подгруппы в мультипликативной группе поля**

Пусть  $H$  — конечная подгруппа в  $K^*$ ,  $K$  — поле. Тогда  $H$  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  $a: \langle a \rangle = \mathbb{Z}/n^*$  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

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

*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.**  $\text{Fix}(\sigma)$  — множество всех неподвижных точек относительно  $\sigma$ .

**Определение 13: Носитель**

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

**Обозначение.**  $\text{supp } \sigma$ .

**Определение 14: Независимость перестановок**

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

**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  $c_1, \dots, c_k$ ,  $c_i \neq \text{id}$ , что  $\sigma = c_1 \dots c_k$ .

**Теорема 6: Порядок перестановки**

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

**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  $\sigma^{-1} = c_1^{-1} c_2^{-1} \dots c_s^{-1}$ .

## Вопрос 8 Разложение в произведение транспозиций. Знак перестановки. Знак как гомоморфизм. Знак и число транспозиций в разложении.

**Определение 15: Транспозиция**

Цикл вида  $(ij)$ ,  $i \neq j$  называется транспозицией.

**Утверждение.** Любая перестановка раскладывается в произведение транспозиций.

**Определение 16: Инверсия**

Пара  $i < j$  образует инверсию, если  $\sigma(i) > \sigma(j)$ .

**Определение 17: Четность и знак перестановки**

Четность перестановки — четность числа инверсий  $Inv(\sigma)$  в ней.

Знак перестановки — число

$$\operatorname{sgn}(\sigma) = (-1)^{Inv(\sigma)} = \prod_{i>j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

**Пример 1**

$$\operatorname{sgn}(1, 2) = -1$$

**Утверждение.** Отображение  $\operatorname{sgn} : S_n \rightarrow \{\pm 1\}$  является гомоморфизмом групп.

**Лемма 9**

$g \in S_n$ . Тогда  $g(1, 2)g^{-1} = (g(1), g(2))$ . Знак любой транспозиции равен  $-1$ .

**Теорема 8**

Пусть  $\sigma = \tau_1 \dots \tau_k$ ,  $\tau_i$  — транспозиция. Тогда  $\operatorname{sgn} \sigma = (-1)^k$ .

**Вопрос 9 Разные способы вычисления знака перестановки. Знак обратной перестановки. Знакопеременная группа. Задача о пятнадцати.**

**Утверждение.**  $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$

**Утверждение.** Пусть  $\sigma = c_1 \dots c_n$ ,  $c_i$  — независимые циклы. Тогда  $\operatorname{sgn} \sigma = (-1)^{\text{кол-во } c_i \text{ четной длины}} = (-1)^{n-k}$ , где  $k$  — количество орбит  $\sigma$ .

**Определение 18: Знакопеременная группа**

Знакопеременная группа  $A_n$  — группа

$$A_n = \{\sigma \in S_n \mid \sigma \text{ — четная}\} = \ker(\operatorname{sgn}).$$

$$|A_n| = \frac{n!}{2}.$$

**Вопрос 10 Образующие  $S_n$ . Сопряжение. Цикленный тип и сопряженность. Класс сопряженности произвольной перестановки.**

**Утверждение.** Пусть  $g_1, \dots, g_k$  — образующие  $S_n$ . Набор  $h_1, \dots, h_l \in G$  порождает  $G$  тогда и только тогда, когда все  $g_i$  выражаются через  $h_j$ .

**Утверждение.**  $S_n$  порождена перестановками  $(12), \dots, (1n)$ .

**Утверждение.** Пусть  $g \in S_n$ ,  $c = (a_1, \dots, a_k) \in S_n$ . Тогда

$$g c g^{-1} = (g(a_1), \dots, g(a_k)).$$

**Утверждение.** Пусть  $\sigma = c_1 \dots c_k$ , где  $c_k$  — независимые циклы. Тогда для любого  $g \in S_n$  :

$$g \sigma g^{-1} = (g c_1 g^{-1}) \dots (g c_k g^{-1}).$$

**Определение 19: Цикленный тип**

Пусть  $g \in S_n$ . Цикленный тип перестановки  $g$  — набор упорядоченных пар  $(1, k_1), \dots, (n, k_n)$ , где  $k_i$  — число орбит элемента  $i$  относительно  $g$ .

**Определение 20: Сопряженный элемент**

Пусть  $g, h \in G$ . Сопряженный элемент к  $h$  при помощи  $g$  — такой элемент  $ghg^{-1}$ . Два элемента  $h_1, h_2$  сопряжены, если  $\exists g \in G: gh_1g^{-1} = h_2$ .

**Теорема 9**

$\sigma_1, \sigma_2 \in S_n$ , сопряжены тогда и только тогда, когда у них одинаковые цикленные типы.

**Вопрос 11**  $S_n$  порождена двумя образующими. Образующие  $A_n$  — два типа.

**Утверждение.** Группа  $S_n$  порождена перестановками  $(12), (1 \dots n)$ .

**Утверждение.** Группа  $A_n$  порождена перестановками  $(123), \dots (12n)$ .

**Утверждение.** Группа  $A_n$  порождена перестановками  $(123), (12 \dots n)$ , если  $n$  нечетно, и  $(123), (23 \dots n)$ , если четно.

**Вопрос 12** Прямое произведение. Порядок элемента в прямом произведении. Прямое произведение и подгруппы. Образующие прямого произведения. Критерий разложимости в прямое произведение.

**Утверждение.** Пусть  $(g, h) \in G \times H$ . Тогда  $\text{ord}(g, h) = \text{НОК}(\text{ord } g, \text{ord } h)$ .

**Теорема 10**

Пусть  $G = \langle g_1, \dots, g_k \rangle$ ,  $H = \langle h_1, \dots, h_l \rangle$ . Тогда  $(g_1, e), \dots, (g_k, e), (e, h_1), \dots, (e, h_l)$  — образующие  $G \times H$ .

**Определение 21: Разложение в произведение подгрупп**

Группа  $G$  раскладывается в произведение своих подгрупп  $G_1, G_2$ , если отображение  $f: G_1 \times G_2 \rightarrow G$ ,  $f(g, h) = gh$ , является гомоморфизмом.

**Обозначение.**  $G = G_1 \times G_2$ .

**Теорема 11: Критерий разложимости в прямое произведение подгрупп**

Пусть  $G_1, G_2 \leq G$ .  $G_1 \times G_2 = G$  тогда и только тогда, когда

- $G_1 \cap G_2 = \{e\}$
- $g_1 \in G_1, g_2 \in G_2 \implies g_1 g_2 = g_2 g_1$
- $\langle G_1, G_2 \rangle = G$ .

*Замечание.* Последнее условие равносильно тому, что  $\forall g \in G \exists g_1 \in G_1, g_2 \in G_2: g = g_1 g_2$ , при условии первого пункта.

**Вопрос 13** Лемма про возведение в степень по модулю  $p^\alpha$ . Строение группы  $\mathbb{Z}/_{p^\alpha}^*$  при простом  $p$ . Ответ в зависимости от разложения  $p$  на множители.

**Лемма 10**

Пусть  $p \in \mathbb{P}$ , если  $p$  нечетно, то  $s \geq 1$ , если  $p = 2$ , то  $s \geq 2$ . Тогда

$$x \equiv 1 + cp^s \pmod{p^{s+1}} \implies x^p \equiv 1 + cp^{s+1} \pmod{p^{s+2}}.$$

**Утверждение.**

- Пусть  $p \in \mathbb{P}$  и  $p$  нечетно. Тогда  $\mathbb{Z}/_{p^\alpha}^*$  изоморфна циклической группе

$$\mathbb{Z}/_{p^{\alpha-1}(p-1)} \cong \mathbb{Z}/_{p-1} \times \mathbb{Z}/_{p^{\alpha-1}}.$$

- Если  $p = 2$ :

$$\begin{aligned} \alpha = 1 & \text{ группа } \mathbb{Z}/_{p^\alpha}^* \text{ тривиальна} \\ \alpha \geq 2 & \mathbb{Z}/_{p^\alpha}^* \cong \mathbb{Z}/_2 \times \mathbb{Z}_{2^{\alpha-2}}. \end{aligned}$$



**Теорема 12: Ответ в зависимости от разложения**

Пусть  $n = 2^k p_1 d \alpha_1 \dots p_s^{\alpha_s}$ . Тогда

$k = 0, 1$

$$\mathbb{Z}/_n^* \cong \prod_{i=1}^s \mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)}$$

$k \geq 2$

$$\mathbb{Z}/_n^* \cong \mathbb{Z}/_2 \times \mathbb{Z}/_{2^{k-2}} \times \prod_{i=1}^s \mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)}$$

**Вопрос 14 Доказательство теоремы Рабина****Теорема 13: Рабин**

Пусть  $n$  нечетное составное число,  $n > 9$ . Тогда  $S(n) \leq \frac{\varphi(n)}{4}$ , где  $S(n)$  — множество свидетелей простоты в тесте Миллера-Рабина.

**Вопрос 15 Сюръективный гомоморфизм и образующие. Сюръективный гомоморфизм и порядок. Нормальная подгруппа. Переформулировки. Примеры.**

**Утверждение.** Пусть дан сюръективный гомоморфизм  $f: G \rightarrow H$ ,  $\ker f = \langle g_1, \dots, g_k \rangle$ ,  $H = \langle h_1, \dots, h_l \rangle$ . Если взять  $h'_i \in G$  такие, что  $g(h'_i) = h_i$ , то группа  $G$  будет порождена  $h'_1, \dots, h'_l, g_1, \dots, g_k$ .

**Лемма 11**

Пусть  $f: G \rightarrow H$  — гомоморфизм. Тогда  $f(g_1) = f(g_2)$  тогда и только тогда, когда  $g_1 \in g_2 \ker f$ .

**Утверждение.** Пусть  $G$  конечна,  $f: G \rightarrow H$  — сюръективный гомоморфизм. Тогда  $|G| = |\ker f| \cdot |H|$ .

**Определение 22: Нормальная подгруппа**

Подгруппа  $H \leq G$  называется нормальной, если для любых  $g \in G$  и  $h \in H$  выполнено следующее:  $ghg^{-1} \in H$ .

**Обозначение.**  $H \trianglelefteq G$ .

**Утверждение (Переформулировки).** Пусть  $H \leq G$ . Следующие утверждения эквивалентны:

- $\forall g \in G: gHg^{-1} \subseteq H$
- $\forall g \in G: gHg^{-1} = H$
- $\forall g \in G: gH = Hg$
- $\forall g \in G: gH \subseteq Hg$

**Вопрос 16 Фактор-группа. Корректность. Универсальное свойство фактора. Теорема об изоморфизме. Примеры. Простые группы.****Определение 23: Фактор-группа**

Пусть  $H \trianglelefteq G$ . Определим на множестве смежных классов  $G/H$  структуру группы:  $g_1 H g_2 H = g_1 g_2 H$ .

**Теорема 14: Универсальное свойство фактора**

Пусть  $G, G_1$  — группы,  $H \leq G$ . Тогда для любого гомоморфизма  $f: G \rightarrow G_1$ , такого, что  $H \leq \ker f$ , существует единственный гомоморфизм  $\varphi: G/H \rightarrow G_1$  такой, что  $f = \pi \circ \varphi$ .

**Теорема 15: Теорема об изоморфизме**

Пусть  $f: G \rightarrow G_1$  — гомоморфизм. Тогда  $G/\ker f \cong \text{Im } f$ . Этот изоморфизм переводит  $g \ker f$  в  $f(g)$ .

**Определение 24: Простая группа**

Группа  $G$  называется простой, если в  $G$  нет нормальных подгрупп отличных от  $G$  и  $\{e\}$ .

**Вопрос 17 Действие группы на множестве. Примеры. Действия и гомоморфизмы. Описание группы самосовмещений тетраэдра. Теорема Кэли.****Определение 25: Действие группы на множестве**

Действие группы  $G$  на множестве  $X$  — отображение  $\cdot : G \times X \rightarrow X$ , удовлетворяющее аксиомам:

- $\forall x \in X : e \cdot x = x$
- $\forall x \in X, g, h \in G : (gh) \cdot x = g \cdot (h \cdot x)$

Обозначение.  $G \curvearrowright X$

**Теорема 16**

Пусть заданы группа  $G$  и множество  $X$ . Тогда для каждого действия  $G \curvearrowright X$  существует гомоморфизм, переводящий  $g \rightarrow T_g$ , где  $T_g(x) = gx$  — биекция, заданная домножением на  $g$ .

**Теорема 17: Кэли**

Любая группа  $G$  вкладывается в  $S_G$ . Если  $|G| = n$ , то есть подгруппа  $H \leq S_n \cong G$ .

**Вопрос 18 Инвариантное подмножество. Орбита. Стабилизатор. Связь орбиты и стабилизатора. Следствие про делимость. Вычисление орбиты. Пример.****Определение 26: Инвариантное подмножество**

Пусть  $G \curvearrowright X$ . Подмножество  $Y \subseteq X$  называется инвариантным относительно данного действия, если для всех  $g \in G$  выполнено  $g(Y) = Y$ .

**Определение 27: Орбита**

Орбита элемента  $x$  — множество элементов, которые можно получить при помощи группы  $G$ :

$$O_x = G \cdot x := \{y \in X \mid \exists g \in G : g \cdot x = y\}.$$

**Определение 28: Стабилизатор**

Стабилизатор точки  $x$  — множество элементов группы  $G$ , оставляющих ее на месте:

$$\text{Stab}_x = G_x := \{g \in G \mid g \cdot x = x\}.$$

**Теорема 18: О связи орбиты и стабилизатора**

Пусть  $G \curvearrowright X$  и задана точка  $x \in X$ . Тогда для любой точки  $y \in O_x$  множество  $\{h \in G \mid hx = y\}$  является левым смежным классом группы  $G$  по стабилизатору  $\text{Stab}_x$ .

Обратно, для любого элемента  $h \in g\text{Stab}_x$  верно, что  $hx = gx$ . В частности, корректно определены отношения, задающие биекцию между  $O_x \longleftrightarrow G/\text{Stab}_x$ , заданные так

$$y \in O_x \rightarrow \{h \in G \mid hx = y\} \quad g\text{Stab}_x \rightarrow gx \in O_x.$$

**Следствие 10: про делимость**

Пусть  $G$  — конечная группа, действующая на множестве  $X$ . Если задан элемент  $x \in X$ , то  $|G| = |O_x| \cdot |\text{Stab}_x|$ .

**Вопрос 19 Теорема Коши. Ограничение числа образующих у подгруппы в  $S_n$ .**

**Теорема 19: Коши**

Пусть  $G$  — конечная группа,  $|G| : p \in \mathbb{P}$ . Тогда в группе  $G$  есть элемент порядка  $p$ .

**Теорема 20: Об ограничении числа образующих**

Пусть  $G \leq S_n$ . Тогда существует набор образующих из не более чем  $\frac{n(n-1)}{2}$  элементов.

## Вопрос 20 Лемма Шрайера. Понятие о цепочке стабилизаторов и о сильном порождающем множестве. Алгоритм проверки принадлежности элемента, если известна полная цепочка стабилизаторов.

**Теорема 21: Лемма Шрайера**

Пусть группа  $G = \langle S \rangle$  действует на множестве  $X$ . Пусть  $x \in X$  и для всех  $y \in O_x$  задан  $h_y \in G$  такой, что  $h_y x = y$ . Если  $x = y$ ,  $h_x = e$ . Тогда

$$\text{Stab}_x = \langle h_{(sy)}^{-1} s h_y \rangle \text{ по всем } y \in O_x \text{ и } s \in S.$$

**Определение 29: База**

Пусть группа  $G$  действует на множестве  $X$ . Назовем набор  $(b_1, \dots, b_k)$  базой, если для всех  $g \in G$  выполнено  $(\forall i: gb_i = bi) \implies g = e$ .

**Определение 30: Дерево Шрайера**

Пусть  $G$  — группа с конечным множеством образующих  $S$  действует на множестве  $X$ . Дерево Шрайера для элемента  $x \in X$  относительно множества  $S$  — дерево (ребра направлены к корню), вершины которого соответствуют элементам орбиты  $O_x$  ( $x$  — корень), на ребрах стоят пометки из элементов  $S$ , что ребро из  $u$  в  $v$  с меткой  $s$  проведено, если  $su = v$ .

**Определение 31: Полная цепочка стабилизаторов**

Пусть  $G$  действует на множестве  $X$ , дана база  $B = (b_1, \dots, b_k)$ . Полной цепочкой стабилизаторов относительно базы  $B$  будем называть цепочку подгрупп

$$G = G_0 \geq G_1 \geq \dots \geq G_k = \{e\},$$

обладающую свойствами:

1.  $G_{i+1} = \text{Stab}_{b_{i+1}}^{G_i}$ , при  $0 \leq i \leq k-1$
2.  $G_i$  заданы с помощью образующих  $S_i$
3.  $\forall i \geq 0$  задано  $T_i$  — дерево Шрайера для  $b_{i+1}$  относительно  $S_i$
4. дополнительно  $G_i = G_{i+1}$

**Определение 32: Сильное порождающее множество**

Пусть группа  $G$  действует на множестве  $X$  и задана база  $B$ . Тогда множество  $S$  называется сильным порождающим множеством относительно  $B$ , если  $S \cap G_i$  — образующие для  $G_i$ .

## Вопрос 21 Лемма Бренсайда. Пример с раскраской квадрата.

**Определение 33: Множество орбит**

Пусть группа  $G$  действует на множестве  $X$ . Множество всех орбит относительно этого действия будем обозначать  $X/G$ .

**Определение 34: Множество неподвижных точек**

Пусть так же задан элемент  $g \in G$ . Тогда обозначим за  $\text{Fix}(f)$  — множество неподвижных точек элюента  $g$ :

$$\text{Fix}(g) = \{x \in X \mid gx = x\}.$$

**Теорема 22: Бренсайд**

Пусть конечная группа  $G$  действует на конечном множестве  $X$ . Тогда

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$