Обозначения

- **S** перестановочная
- **C** циклическая
- **D** диэдральная (группа симметрий правильного n-угольника)
- **Z** по сложению

Вычеты

- Критерий: $[a]_n$ - обратимый $\iff a, n-$ взаимно простые
- Группа $\mathbb{Z}_n^*$ - группа обратимых вычетов по модулю n. $|\mathbb{Z}_n^*| = \varphi(n)$, $\varphi(n)-$ функция Эйлера - количество взаимно простых с данным числом и меньших его.
- Теорема Эйлера: НОД $(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 (mod\ n)$
- Малая теорема Ферма: p - простое, тогда $a \neq 0 (mod\ p) \Rightarrow a^{p-1} \equiv 1\ (mod\ p)$
- Группа $\mathbb{Z}_n$ по сложению - остатки по модулю n. a - элемент этой группы, тогда $ord(a) = \frac{\text{НОК(a, n)}}{a} = \frac{n}{\text{НОД(a, n)}}$

Свойства групповых операций

- Закон сокращения: Пусть G - группа $\forall a \in G\ x = y \Leftrightarrow ax = ay \Leftrightarrow xa = ya$
- Формула обратного произведения: $(xy)^{-1} = y^{-1}x^{-1}$

Порядки элементов

- Пусть G - группа, тогда $\forall g, h \in G\ |ghg^{-1}| = |h|$, кроме того, $|gh| = |hg|$.
- Пусть $\forall g \in G\ g^2 = e$. Тогда G - абелева.

Подгруппы и классы смежности

- Критерий подгруппы. Непустое $H \subset G$ - подгруппа группы $G \Leftrightarrow \forall a, b \in H\ ab^{-1} \in H$
- Пересечение подгрупп - подгруппа
- Левый смежный класс. Пусть $H < G$ тогда левый смежный класс $gH = \{x \in G : x = gh, h \in H\}$. Тут g фиксировано и отвечает за свой класс смежности. Аналогично определяется правый класс смежности $Hg = \{x \in G : x = hg, h \in H\}$
- Смежные классы не пересекаются, либо совпадают, то есть смежные классы задают отношение эквивалентности на группе.
- Критерий принадлежности классу смежности. Для левого класса: $x, y \in GH \Leftrightarrow y^{-1}x \in H$.

  Для правого класса: $x, y \in GH \Leftrightarrow xy^{-1} \in H$.
- Смежные классы не подгруппы в общем случае!
- $(G : H)$ - индекс группы - количество смежные классов по данной подгруппе H. Во всех классах смежности одинаковое количество элементов.

Теорема Лагранжа, ее следствие и применения

- Теорема Лагранжа (мега-имба). Пусть G - группа, $H < G$. Тогда $|G| = (G : H) \cdot |H|$. То есть количество элементов в группе равно количеству элементов в подгруппе, помноженному на количество смежных классов по этой подгруппе.
- Следствие 1: Порядок подгруппы делит порядок группы.
- Следствие 2: $|G| = p -$ простое. Тогда в G нет несобственных подгрупп (то есть подгруппы только $\{e\}, G$)

- Следствие 3: Порядок элемента делит порядок группы — OVERPOWERED
- Следствие 4: $|G| = p -$ простое $\Rightarrow G -$ абелева (доказывается через группу, порожденную одним элементом)
- Следствие 5: Пусть $|G| = n, \forall g \in G: \ g^n = e$ (так как порядок элемента делит порядок группы)

Изоморфизм

Изоморфизм - биекция из одной группы в другую, сохраняющая операцию, то есть $\varphi(xy) = \varphi(x)\varphi(y)$

- Необходимое условие существования изоморфизма - порядки элементов совпадают. Проверка на изоморфизм - построить биекцию (можно табличкой)
- Способы доказать, что изоморфизма нет: проверить количество элементов (должны быть равны), проверить порядки элементов, проверить на абелевость (сказать, что одна - абелева, а вторая - нет).

Прямое произведение групп

Прямое произведение групп - все выполняется покомпонентно.

- НОД$(p, q) = 1$, тогда $C_p \times C_q \cong C_{pq}$.
- $ord(g, h) =$ НОК$(ord(g), ord(h))$

Перестановки

Если перестановка π представима в виде произведения циклов длины $l_0, l_1, ..., l_n$, то $ord(\pi) =$ НОК$(l_0, l_1, ..., l_n)$.
Четность перестановки. Эквивалентные определения:

1. Перестановка содержит четное число инверсий
2. Перестановка представима в видел произведения четного числа транспозиций
3. Перестановка представима в виде произведения циклов длины 3
4. $n + k -$ четно, где k - число циклов (вместе с тривиальными)

- Любой цикл длины 3 представим в виде 2-х транспозиций.
- Цикл длины n представим в виде n транспозиций. $(a_1, a_2, a_3, ..., a_n) = (a_1, a_n) \circ (a_1, a_{n-1}) \circ ... \circ (a_1, a_2)$
- Умножение на транспозицию изменяет количество циклов на ± 1.
- Четные перестановки образуют подгруппу A_n. $|A_n| = \frac{n!}{2}$
- Перестановки сопряжены тогда и только тогда, когда у них совпадают длины циклов.

Гомоморфизм

Гомоморфизм - отображение, сохраняющее операцию $\varphi : G \to H$, $\varphi(xy) = \varphi(x) \cdot \varphi(y)$.
Ядро $Ker\varphi = \{g \in G : \varphi(g) = e_H\}$ Ядро - подгруппа G
Образ $Im\varphi = \{h \in H : \exists g \in G \ \varphi(g) = h\}$ Образ - подгруппа H.

- Композиция гомоморфизмов - гомоморфизм
- $\varphi : G \to H$ - гомоморфизм, тогда $\varphi(e)$ - нейтральный в H,
  $\varphi(a^{-1}) = \varphi(a)^{-1}$
- $|G| = |Im\varphi| \cdot |Ker\varphi|$ (G - группа аргументов гомоморфизма, как в определении выше) - следствие из теоремы Лагранжа.
- В обозначениях того же определения: если $K < H$, тогда $\varphi^{-1}(H)$ - подгруппа G.

Нормальные подгруппы, фактор-группа

$H \lhd G \Leftrightarrow \forall g \in G : gH = Hg$, то есть правый смежный класс совпадает с левым смежным классом по нормальной подгруппе

- Ядро любого гомоморфизма - нормальная подгруппа.
- Любая нормальная подгруппа является ядром некоторого гомоморфизма. Фактор-группа - группа из смежных классов по ядру, то есть смежные классы мы воспринимаем как элементы фактор группы. (свойства классов смежности есть выше).
- Любая подгруппа абелевой группа - нормальная
- ОСНОВНАЯ ТЕОРЕМА ГОМОМОРФИЗМА: $Im\varphi \cong G/Ker\varphi$ - образ изоморфен фактору группы по ядру.
- Подгруппа индекса 2 всегда нормальна Пусть $\psi : G \to G$ - автоморфизм (то есть изоморфизм в самого себя) и H - нормальная подгруппа G. Тогда $\psi(H)$ - нормальна и $G/H \cong G/\psi(H)$
- $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

Сопряжения

Пусть G - группа. Тогда элемент b сопряжен с a посредством g, если $b = g^{-1}ag$. Сопряжение - отношение эквивалентности.
Образуются классы сопряженности, отвечающие отношению эквивалентности.

- Нормализатор $N_x = \{y|yx = xy\}\,, y = x^{-1}yx$, то есть все те y, которые сопряжены с собой посредством x. Ну либо же все те y, которые коммутируют с x.
- Нормализатор - подгруппа
- $|N_x| \cdot |\,[x]\,| = |G|, \quad [x] -$ класс сопряженности по x.

Диэдральная группа

Диэдральная группа D_n - группа симметрий правильного n - угольника.

- Количество элементов: $|D_n| = 2n$
- Элементы: id, n-1 поворот, n осевых симметрий: n - нечетно, тогда все осевые симметрии - из вершины к середине противоположной стороны. n - четно, тогда n/2 симметрий по серединам сторон, n/2 симметрий по вершинам.
- Осевую симметрию можно получить сопряжением одной осевой симметрии поворотом: $x = srs^{-1}$, r - симметрия, s - поворот.
- Также $s^{-1} = rsr$
- D_n не изоморфна $C_n \times C_2$, так как она не абелева.

Действия групп

Действие группы G на множестве X - гомоморфизм $G \to S(x)$, то есть каждому элементу из группы мы сопоставляем некоторую перестановку на множестве.

- Действие левыми сдвигами (группа действует сама на себя) $g(x) : x \mapsto gx$
- Действие сопряжением (группа действует сама на себя) $g(x) : x \mapsto g^{-1}xg$. Тут $Stab_x = N_x$ и $Orb(x) = [x]$
- Орбита действия: $Orb(x) = \{y \in X : \exists g \in G : g(x) = y\}$
- Стабилизатор: $Stab(x) = \{g\ inG : g(x) = x\}$ - все элементы G, которые оставляют x на месте.
- Стабилизатор - подгруппа
- Орбиты - классы эквивалентности

- $|Orb(x)| = (G : Stab_x)$
- По теореме Лагранжа $|G| = |Orb(x)| \cdot |Stab_x|$
- Стабилизаторы элементов одной орбиты сопряжены.
- Центр группы $Z(G) = \{z \in G | \forall g \in G : zg = gz\}$ - те элементы, которые коммутируют со всеми. Центр - ядро при действием сопряжением.
- Если G - p-группа (ее порядок равен p^n, p - простое). Тогда центр $Z(G)$ - нетривиален, то есть в нем больше 1 элемента.
- Лемма Бернсайда: #орбит $= \frac{1}{|G|} \sum_{g \in G} |X^g|$, где X^g - это точки, неподвижные под действием g.

Группы симметрий правильный многогранников

$Cube \cong S_4$ (доказывается через диагонали) $|Cube| = |Oct| = 24$
$Tetra \cong A_4, |Tetra| = 12$, $Dodec \cong Iso \cong A_5, |Dodec| = 60$

Fun Facts

- Если $p > 2 -$ простое, тогда уравнение $x^2 \equiv 1 \mod p$ имеет только 2 решения: 1 и -1. (доказывается через $(x-1)(x+1) \equiv 0 \mod p$)
- $\sum_{d|n} \varphi(d) = n$, где $\varphi(d) -$функция Эйлера.
- Мультипликативность функции Эйлера: НОД$(p, q) = 1 \Rightarrow \varphi(pq) = \varphi(p) \cdot \varphi(q)$
- Необходимое и достаточное условие квадратичного вычета: a - кв.вычет по модулю p - простого $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \mod p$
- Конечно порожденная абелева группа изоморфна прямому произведению циклических