

Содержание

1	Множества	2
1.1	Отображения	2
1.2	Операция на множествах	3
1.3	Мощность множества	3
1.4	Сравнение мощности множеств	4
2	Группы и подгруппы	4
2.1	Операции на множестве	4
2.2	Обратимость и сопряженность	5
2.3	Про группоиды, моноиды, полугруппы и группы	6
2.4	Про виды групп	6
2.5	Порядок элемента в группе	6
2.6	Таблица Кэли	7
2.7	Подгруппы	7
2.8	Нормальные подгруппы	9
2.9	Про виды различных групп	10
3	Перестановки	10
3.1	Перестановки	10
3.2	Описание элементов S_n и перестановок	12
3.3	Четность/Нечетность подстановки	12

1 Множества

Определение. *Множество* - это набор уникальных элементов.

1.1 Отображения

Определение. *Отображение* - это подмножество декартового произведения множеств A и B , такое что каждому элементу из множества A соответствует единственный элемент из множества B :

$$f : A \rightarrow B \Leftrightarrow f \subset A \times B : \forall a \in A \exists! b \in B : (a, b) \in f \Leftrightarrow$$
$$f = \{(a_1, b_1), \dots, (a_k, b_k)\}$$

Отображения бывают нескольких видов:

- *Инъективные*: разные элементы отображаются в разные образы

$$f : A \rightarrow B \Leftrightarrow \forall a_1, a_2 \in A (a_1 \neq a_2) : f(a_1) \neq f(a_2)$$

- *Сюръективные*: для каждого образа существует элемент, который отображается в этот образ.

$$f : A \rightarrow B \Leftrightarrow \forall b \in B : \exists a \in A : b = f(a)$$

Примечание: При этом единственность существования элемента a не гарантируется.

Определение. Отображение *биективно*, если оно одновременно сюръективно и инъективно.

Как это запомнить?

Рассмотрим пример из жизни. Допустим у нас есть некоторое множество *шприцов* и *нариков*. Пусть f - это отображение множества шприцов на множество нариков. Если у каждого нарика есть хотя бы по одному шприцу (у каждого нарика может быть больше одного шприца!), то f - это *инъективное* отображение. Если у разных нариков разные шприцы, то это *сюръективное* отображение. Если каждому нарику досталось по одному шприцу, то это *биекция*!

Определение. *Композицией отображений* $f : A \rightarrow B$, $g : B \rightarrow C$ называется отображение $\omega : A \rightarrow C$, такое что $\forall a \in A : \omega(a) = f \circ g(a) = g(f(a)) \in C$.

1.2 Операция на множествах

Определение	На “математическом языке”
Множества M и N равномощны, если существует биекция из M в N .	$\exists \phi : M \rightarrow N$, где ϕ - биекция $\Rightarrow M = N \Rightarrow M = N $, где $\Rightarrow M = N $ - биекция $\Rightarrow M = N $
Множество M имеет большую или равную мощность, чем N , если существует сюръекция из M в N . (“Меньше или равно” задается также)	$\exists \phi : M \rightarrow N$, где ϕ - сюръекция $\Rightarrow M \leq N \Rightarrow M \leq N $, где $\Rightarrow M \leq N $ - сюръекция $\Rightarrow M \leq N $
Множество M имеет большую мощность, чем N , если существует сюръекция из M в N и не существует биекции из M в N .	$\exists \phi : M \rightarrow N$, где ϕ - сюръекция и $\nexists \Psi : M \rightarrow N$, где Ψ - биекция $\Rightarrow M < N \Rightarrow M < N $, где $\Rightarrow M < N $ - сюръекция и $\Rightarrow M < N $, где $\Rightarrow M < N $ - биекция $\Rightarrow M < N $

Также мы будем пользоваться декартовым произведением множеств.

Определение. *Декартовым произведением* множеств называется множество из пар элементов двух множеств.

$$A \times B \Leftrightarrow \forall a \in A \forall b \in B : (a, b) \in A \times B$$

1.3 Мощность множества

Определение. *Мощность* множества - это количество элементов в множестве.

Определения.

Множество A называется *конечным*, если существует биективное отображение из A в $\{1, \dots, n\}$. В этом случае n - мощность множества A .

Если такого отображения не существует, множество называется *бесконечным*. Если можно построить биекцию элементов множества на множество натуральных чисел, такое множество называется *счетным*. (При этом множество все равно бесконечное)

Определение	На "математическом языке"
Множества M и N равномощны, если существует биекция из M в N .	$\exists \phi : M \rightarrow N$, где ϕ - биекция $\Rightarrow M = N \Rightarrow M = N $, где $\Rightarrow M = N $ - биекция $\Rightarrow M = N $
Множество M имеет большую или равную мощность, чем N , если существует сюръекция из M в N . ("Меньше или равно" задается также)	$\exists \phi : M \rightarrow N$, где ϕ - сюръекция $\Rightarrow M \leq N \Rightarrow M \leq N $, где $\Rightarrow M \leq N $ - сюръекция $\Rightarrow M \leq N $
Множество M имеет большую мощность, чем N , если существует сюръекция из M в N и не существует биекции из M в N .	$\exists \phi : M \rightarrow N$, где ϕ - сюръекция и $\nexists \Psi : M \rightarrow N$, где Ψ - биекция $\Rightarrow M < N \Rightarrow M < N $, где $\Rightarrow M < N $ - сюръекция и $\Rightarrow M < N $, где $\Rightarrow M < N $ - биекция $\Rightarrow M < N $

1.4 Сравнение мощности множеств

Определение. Множества A и B *равномощны*, если они имеют одинаковую мощность (одинаковое количество элементов).

Теорема Кантора.

Любое множество менее мощно, чем множество всех его подмножеств.

Примечание: Множество всех подмножеств множества M обозначается как 2^M .

Утверждение о биективности композиции биективных отображений.

Пусть A, B – непустые множества. Также пусть заданы биекции f и g , такие что $f : A \rightarrow B$, $g : B \rightarrow C$. Тогда их композиция также будет биекцией.

Утверждение о транзитивности отношения «иметь большую мощность» на множествах.

Пусть заданы непустые множества A, B, C . Тогда если $|A| < |B|$ и $|B| < |C|$, то $|A| < |C|$.

2 Группы и подгруппы

2.1 Операции на множестве

Определение. *Операция* - это отображение пар из чисел принадлежащих этому множеству на само это множество.

Определение. Операция *коммутативна*, если $\forall a, b \in M, a * b = b * a$.

Определение. Операция *ассоциативна*, если $\forall a, b, c \in M (a * b) * c = a * (b * c)$.

Суть этого свойства заключается в том, что от порядка выполнения вычислений результат не зависит. При этом элементы остаются на месте (к коммутативности ассоциативность не имеет никакого отношения).

Определение.

Нейтральный элемент - это такой элемент, что при применении операции (будем называть это умножением) справа и слева, элемент, на который умножается нейтральный не меняется.

Математически это определяется так:

Пусть e - нейтральный элемент. Тогда $\forall a \in A : e * a = a * e = a$.

Утверждение о единственности нейтрального элемента

Если в множестве M есть *нейтральный элемент*, то такой элемент будет *единственным*.

Определение. *Обратный элемент* - это такой элемент, при умножении на который слева и справа получается нейтральный.

Утверждение о единственности обратного элемента к обратимому элементу.

Если у элемента есть *обратный элемент*, то он *единственный*.

2.2 Обратимость и сопряженность

Определение. Пусть a^{-1} - обратный элемент для a из множества M .

Тогда $a * a^{-1} = a^{-1} * a = e$. Элемент будет обратим, если у него есть обратный элемент.

Определение. Элемент $g_1 \in M$ сопряжен к $g_2 \in M$, если существует $h \in M$ такой, что $g_1 = h g_2 h^{-1}$.

Примечание: Если g_1 сопряжен к g_2 , то и g_2 будет сопряжен к g_1 , потому что из первого равенства можно вывести второе:

$$g_1 = h g_2 h^{-1} \Leftrightarrow g_2 = (h^{-1}) g_1 (h^{-1})^{-1} = h_1 g_1 h_1^{-1}$$

2.3 Про группоиды, моноиды, полугруппы и группы

- Множество с операцией называется **группоидом**, если операция замкнута на этом множестве.
- Если элементы в группоиде ассоциативны, то группоид называется **полугруппой**.
- Если в полугруппе есть нейтральный элемент, то такая полугруппа называется **моноидом**.
- Если в моноиде все элементы обратимы, то такой моноид называется **группой**.

Утверждение о совпадении нейтральных элементов в подгруппе и группе.

Нейтральные элементы в группе и подгруппе совпадают.

Утверждение о виде обратного элемента к произведению обратимых элементов.

Пусть на группоиде M с операцией $*$ есть элементы g, h , у которых есть обратные элементы g^{-1}, h^{-1} (-1 — это не степень!). Тогда обратным к произведению gh будет элемент $h^{-1} * g^{-1}$.

Другими словами $(g * h)^{-1} = h^{-1} * g^{-1}$.

Утверждение о множестве обратимых элементов моноида.

Множество всех обратимых элементов моноида образует группу.

2.4 Про виды групп

Определение. Если элементы в группе коммутативны, такая группа называется абелевой (или еще её называют коммутативной).

Примечание: Любая группа, в которой меньше 5 элементов, будет абелевой.

Определение. *Конечная группа* — это группа, для которой можно построить биекцию вида: $\phi : G \rightarrow \{1, \dots, n\}$ (на множество чисел от 1 до n).

2.5 Порядок элемента в группе

Определение. *Порядок элемента* — это минимальная положительная степень (то, сколько раз нужно умножить элемент сам на себя), в которую нужно

	g_1	\cdots	g_n
g_1	g_k	\cdots	g_i
\vdots	\vdots	\ddots	\vdots
g_n	g_j	\cdots	g_m

возвести элемент, чтобы он стал равен нейтральному. Если такой степени не существует, то мы говорим, что порядок элемента бесконечен.

Определение. *Порядок группы* – это количество элементов, которые содержатся в этой группе.

Определение. (Из Глухова-Елизарова-Нечаева)

Экспонента группы — это минимальная натуральная степень, при возведении в которую любой элемент группы становится равен нейтральному.

Определение. (Из лекций)

Экспонента группы — наибольшее общее кратное степеней всех элементов в группе.

2.6 Таблица Кэли

Таблица Кэли – это такая таблица (математическая структура), с помощью которой можно задавать операции на множестве и определить порядки элементов.

Пусть заданы G – группа ($G = \{g_1, \dots, g_n\}$) и операция $*$ на этом множестве. У неё есть несколько свойств:

1. В таблице есть единственный нейтральный элемент (следует из единственности нейтрального элемента в группе)
2. В каждой строке и столбце таблицы стоят все элементы из G . (Каждая следующая строка получается перестановкой элементов группы G)
3. Если G – коммутативная группа, то таблица будет симметрична относительно диагонали: $TK(G) = TK(G)^T$

2.7 Подгруппы

Определение. *Подгруппа* – это такое подмножество H в группе G , что оно само является группой. если оно образует группу относительно операции G .

Критерий для подмножества быть подгруппой.

Непустое подмножество H является *подгруппой* группы $(G, *)$, если для произвольных элементов $a, b \in H$ выполняется $a * b^{-1} \in H$.

Теорема Лагранжа.

Пусть G - конечная группа. Тогда порядок подгруппы H ($H < G$) делит порядок группы G .

Теорема о взаимоотношении порядка элемента и порядка группы.

Порядок элемента должен делить порядок группы.

Определение. *Порождающее множество* – это минимальная подгруппа группы G , содержащая элемент a называется порожденной элементом/множеством или системой образующих a и обозначается $\langle a \rangle$.

Определение. *Циклическая группа* – группа, порожденная одним элементом.

Утверждение о числе (различных) образующих конечной циклической группы

У конечной циклической группы количество конечных образующих будет равно функции эйлера от порядка (количество взаимно простых чисел меньших данного)

Определение. Произведением подгрупп A и B группы $(G, *)$ называется называют подмножество группы G вида $A * B = \{a * b : a \in A, b \in B\}$.

Примечание: Подмножество $A * B$ может и не быть подгруппой. Произведение двух подгрупп группы является группой тогда и только тогда, когда эти подгруппы перестановочны (коммутируют)

Критерий для произведения подгрупп быть подгруппой

Для того, чтобы произведению подгрупп быть подгруппой, они должны коммутировать.

Утверждение о пересечении подгрупп

Пересечение 2-ух подгрупп – это подгруппа

Определение. Смежные классы по подгруппе H группы G :

- **Левый смежный класс** группы G по подгруппе H – это множество вида $\{g * h | h \in H\}$.
- **Правый смежный класс** группы G по подгруппе H – это множество вида $\{h * g | h \in H\}$, где g – элемент G .

Примечание: g называется представителем группы G .

2.8 Нормальные подгруппы

Определение. *Нормальная подгруппа* – это (далее пойдут эквивалентные определения) ...

1. Подгруппу называют нормальной если множество левых смежных классов совпадает с множеством правых смежных классов, т.е. $\forall g \in G : g * H = H * g$. В таком случае пишут $H \triangleleft G$.
2. подгруппа, которая сопряжена со всеми элементами группы: $\forall g \in G : g^{-1}Hg \subset H$
3. подгруппа, элементы которой сопряжены со всеми элементами группы:

$$\forall g \in G, \forall h \in H : g^{-1}hg \in H$$

Примечание: Под записью вида ab подразумевается выражение вида $a * b$. (Для множеств тоже)

Определение. *Простая группа* – не единичная группа, не имеющая нормальных подгрупп.

Определение. *Функция Эйлера* – отображение $\phi : N \rightarrow N$, сопоставляющее каждому натуральному числу количество меньших взаимно простых с ним натуральных чисел

Определение. *Центр группы* – множество элементов коммутирующих с любым элементом группы.

Определение. *Индекс подгруппы в группе* – число правых/левых смежных классов группы по подгруппе (бесконечность в противном случае).

Определение. Если $H \triangleleft G$, то *фактор-группой* G по H называют группу смежных классов G по H . Произведением двух классов смежности считается класс, в который входит произведение представителей этих классов.

Определение. *Четвертная группа Клейна* – В группе S_4 подмножество вида:

$$K_4 = \{\epsilon, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

Примечания:

1. Является самой маленькой не циклической группой.
2. Таблица Кэли для четвертной группы Клейна будет выглядеть так:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

2.9 Про виды различных групп

Определение. *Симметрическая группа* – множество всех обратимых преобразований на множестве из n элементов. Обозначается S_n

Определение. *Знакопеременная группа* – подгруппа всех четных подстановок группы S_n . Обозначается A_n

Определение. *Диэдральная группа* – группа симметрий правильного n -угольника. Обозначается D_n

Определение. *Группа кватернионов* – это неабелева группа восьмого порядка. Является подгруппой группы S_8 , образованная из 5-ти элементов:

$$Q_8 = \langle \{-1, i, j, k | (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\} \rangle$$

Утверждение о нормальности центра группы

Центр группы – нормальная подгруппа.

Теорема о структуре подгрупп группы целых чисел по сложению

Все подгруппы группы целых чисел имеют вид nZ (умножение целого n на все целые числа)

Теорема о структуре подгрупп в группе остатков по модулю n

Все подгруппы в группе остатков по модулю n имеют вид (кроме несобственных) Z/pZ , где p – простой множитель.

3 Перестановки

3.1 Перестановки

Пусть есть непустое множество M , а также порожденное им множество $E(M) = \{\phi : M \rightarrow M\}$ - отображения из M в M .

Мы знаем, что $(E(M), *)$ - моноид. $E^*(M)$ - группа обратимых преобразований (т.е. биекцией, докажете сами).

m_1	m_2	m_3	m_4	m_5
m_2	m_1	m_5	m_3	m_4

1	2	3	4	5
2	1	5	3	4

$$E^*(M) = \{\phi : M \rightarrow M \mid \phi - \text{биекция}\}$$

Пусть задано конечное множество $M = \{m_1, m_2, \dots, m_n\}$. Тогда подстановкой (перестановкой) на M называется взаимно однозначное отображение множества M на себя.

Используя нумерацию элементов конечного множества, всякая подстановка на множестве M сводится к подстановке на множестве натуральных чисел $\{1, 2, \dots, n\}$. При этом соответствующие подстановки называются подстановками степени n .

Группа S_n всех подстановок на множестве $\{1, 2, \dots, n\}$ называется *симметрической группой степени n* .

Обычно подстановка представляется в виде таблицы из двух строк: первая строка содержит числа $1, 2, \dots, n$ в естественном порядке, а вторая строка содержит образы соответствующих элементов первой строки.

Порядок группы S_n равен $n!$ ($|S_n| = n!$)

Перестановку можно задать и единственной строкой, если мы уверены, что верхняя - $1, 2, 3, \dots, n$.

Определение. Каноническая запись: запись, в которой в верхней строке идут элементы от $1, 2, \dots, n$, а под ними элементы. ϕ имеет вид:

Определение. Обратный элемент для подстановки $\phi : \phi^{-1}$ (не степень, а обратный):

Видно, что это не каноническая запись.

Определение. Число биекций $M \rightarrow M$ множества $|M| = n$.

2	1	5	3	4
---	---	---	---	---

1	2	3	4	5
i_1	i_2	i_3	i_4	i_5

i_1	i_2	i_3	i_4	i_5
1	2	3	4	5

3.2 Описание элементов S_n и перестановок

- $a \in M$, a - **мобильный элемент в подстановке**, если $\pi(a) \neq a$. (У нас это элементы 1, 2, 4, 5) - $a \in M$, a - **неподвижный элемент в подстановке**, если $\pi(a) = a$. (У нас это элемент 3)

Примечание: π - подстановка

Определение. Представление перестановки в виде цикла - это перестановка вида:

1. $\pi(k) = k + 1, 1 \leq k < n$
2. $\pi(n) = 1$

Примечание 1: При этом каждый элемент цикла мобильный

Примечание 2: Подстановка $\pi \in S_n$ называется циклом, если существуют числа $a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\}$, такие что $\pi(a_1) = a_2, \pi(a_2) = a_3, \dots, \pi(a_k) = a_1, \pi(i) = i$ при $i \notin \{a_1, \dots, a_k\}$.

Определение. Транспозицией называется перестановка соседних элементов.

3.3 Четность/Нечетность подстановки

Определение. Беспорядком называется такая расстановка элементов в подстановке, что $\pi(i) > \pi(j)$ при $i < j$.

Определение. Подстановка называется четной, если в ней четное количество беспорядков. Иначе она называется нечетной.

Определение. Знакопеременная группа – подгруппа всех четных подстановок группы S_n . Обозначается A_n

Утверждение о том, что множество четных подстановок образуют подгруппу.

1	2	3	4	5
5	4	3	2	1

Утверждение: $A_n < S_n$ Множество четных перестановок A_n является подгруппой группы подстановок

Доказательство: В начале проверяем, что A_n является группой (кроме последнего пункта): 1. $e \in A_n$, т.к. e - четная перестановка; 2. $\pi = t_{i,i+1} * t_{i+1,i+2} * \dots * t_{i_n,i_{n+1}}$ - состоит из четного числа транспозиций.

Обратный элемент $\pi^{-1} = (t_{i,i+1} * t_{i+1,i+2} * \dots * t_{i_n,i_{n+1}})^{-1} = t_{i_n,i_{n+1}}^{-1} * \dots * t_{i+1,i+2}^{-1} * t_{i,i+1}^{-1} = t_{i_n,i_{n+1}} * \dots * t_{i+1,i+2} * t_{i,i+1}$ - также состоит из четного числа транспозиций, а следовательно $\pi^{-1} \in A_n$;

Группа $H \subset G$ является подгруппой группы G , если $\forall a, b \in H: a * b^{-1} \in H$

Остается проверить это утверждение. Число перестановок остается все так же четным

Утверждение о нормальности знакопеременной подгруппы.

Утверждение: $A_n \triangleleft S_n$

Доказательство: Группа $H < G$ является **нормальной** подгруппой группы G , если $\forall g \in G \forall h \in H: g^{-1} * h * g \in H$ Поэтому, один из вариантов доказательства, необходимо доказать, что $\forall \pi \in S_n \forall g \in A_n: \pi^{-1} * g * \pi \in A_n$

1. Построим такое отображение $\phi: S_n \rightarrow S_n: \phi(\pi) = t_{1,2} * \pi$ Очевидно, что:

1. $\phi(A_n) \subset S_n \setminus A_n$
2. $\phi(S_n \setminus A_n) \subset A_n$
3. $|A_n| = |\phi(A_n)|$
4. $|S_n \setminus A_n| = |\phi(S_n \setminus A_n)|$
5. $|S_n \setminus A_n| = |S_n| - |A_n|$

Собирая все вместе: $|A_n| = |\phi(A_n)| \leq |S_n \setminus A_n| = |\phi(S_n \setminus A_n)| \leq |A_n| \Rightarrow |A_n| = |S_n \setminus A_n|$

Тогда: $|S_n \setminus A_n| = |S_n| - |A_n| = |A_n|; |A_n| = \frac{|S_n|}{2} \Rightarrow |S_n : A_n| = 2 \Rightarrow A_n \triangleleft S_n$

Определение Цикловой тип подстановки - это разложение представление подстановки в виде длин независимых циклов, в которые она раскладывается.

Пример:

$\pi = (1)(2)(3, 4, 5)$ - разложение подстановки π . s - цикловой тип подстановки π . $s = \{1^{[2]}, 3^{[1]}\}$

Критерий сопряженности подстановок

Элементы $a, b \in S_n$ сопряжены тогда и только тогда, когда существуют элементы $u, v \in S_n : a = u * v, b = v * u$

Другая формулировка: Подстановки a и b сопряжены тогда и только тогда, когда их цикловой тип совпадает

Утверждение о четности подстановки через четность числа транспозиций

Четность подстановки совпадает с четностью числа транспозиций (транспозиция – нечетная перестановка)

Утверждение о четности подстановки через четность числа транспозиций соседних элементов

Если есть k инверсий в подстановке, то она может быть разложена в k транспозиций соседних элементов. Тогда четность подстановки соответствует четности числа транспозиций соседних элементов.

Утверждение о четности подстановки через четность количества циклов четной длины

В цикле четной длины нечетное количество инверсий. Тогда четность подстановки соответствует четности количества циклов четной длины.

Другая формулировка: Если подстановка при разложении в независимые циклы содержит четное число циклов четной длины, то она четная, в противном случае - нечетная.

Определение

Диэдральная группа - группа симметрий правильного n -угольника. Обозначается D_n

Утверждение о неабелевости группы подстановок

Для любого n большего или равного трем группа S_n - неабелева. ($n!$ элементов)

$$\forall n \geq 3 \Rightarrow S_n - \text{неабелева.}$$

Доказательство: Возьмем две перестановки: $\pi_1 = (1, 2)$ и $\pi_2 = (2, 3)$.

$$\pi_1 * \pi_2 = (1, 2) * (2, 3) = (1, 3, 2)$$

$$\pi_2 * \pi_1 = (2, 3) * (1, 2) = (1, 2, 3)$$

Таким образом, перестановки не коммутируют, а значит для всех $n \geq 3$ S_n - неабелева

Утверждение о неабелевости знакопеременной группы

Начиная с $n \geq 4$, A_n – неабелева. Для любого n большего или равного 4 группа A_n – неабелева. ($\frac{n!}{2}$ элементов)

$$\forall n \geq 4 \Rightarrow A_n - \text{неабелева.}$$

Утверждение о неабелевости группы диэдра . Для любого n большего или равного трем группа D_n – неабелева. ($2n$ элементов)

$$\forall n \geq 3 \Rightarrow D_n - \text{неабелева}$$

Утверждение о тривиальности центра группы подстановок

Для любого n большего или равного 3 группа S_n имеет тривиальный центр.

$$\forall n \geq 3 \Rightarrow Z(S_n) = \{e\}$$

Утверждение о тривиальности центра знакопеременной группы

Для любого n большего или равного 4 группа A_n имеет тривиальный центр.

$$\forall n \geq 4 \Rightarrow Z(A_n) = \{e\}$$

Утверждение о центре групп Диэдра Если n – четное, то тогда центром группы будет являться множество $\{e, r^{\frac{n}{2}}\}$, в противном случае он тривиален.

$$Z(D_n) = \begin{cases} \{e, r^{\frac{n}{2}}\} & n = 0 \pmod{2} \\ \{e\} & n = 1 \pmod{2} \end{cases}$$

Утверждение о нормальных подгруппах группы Диэдра.

Группа D_4 (группа Диэдра) – это самый маленький пример группы, у которой нормальность их подгрупп не транзитивная.

Для нечетных n нормальные подгруппы – D_n и подгруппы вида $\langle R^d, d|n \rangle$

Если n – четное, то существует еще 2 нормальные подгруппы: $\langle R^2, S \rangle, \langle R^2, RS \rangle$

Читать тут: <https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral2.pdf>.