ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ЦИФРОВЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Кафедра «Прикладная математика»

Краткое введение в теорию групп

Часть 2

«Высшая алгебра»

Авторы
И.В. Баранов,
И.А. Гусева

Ростов-на-Дону, 2022

Аннотация

Методические указания предназначены для студентов всех форм обучения.

Авторы

доцент, к.ф.–м.н.,
доцент каф. «Прикладная математика»
Баранов И.В.

доцент, к.ф.–м.н.,
доцент каф. «Теоретическая и прикладная механика»
И.А. Гусева

Оглавление

§1. ГРУППА

Определение:
Непустое множество M с бинарной операцией «$\circ$ » – группа, если выполнены следующие аксиомы:
$G1)\ \forall a, b, c \in M \Rightarrow (a \circ b) \circ c = a \circ (b \circ c);$ (операция ассоциативна)
$G2)\ \exists e \in M: \forall a \in M \Rightarrow a \circ e = e \circ a = a;$ (относительно операции имеется нейтральный элемент)
$G3)\ \forall a \in M\ \exists b \in M: \Rightarrow a \circ b = b \circ a = e;$ (каждый элемент обратим)
Если в добавок к этим трём аксиомам выполняется
$G4)\ \forall a, b \in M \Rightarrow a \circ b = b \circ a$ (т.е. соблюдается закон коммутативности), то и группу называют *коммутативной* или «*абелевой*».

Определение:
Если число элементов группы $<M,\circ>$ – конечно, т.е. $|M| = n < \infty$, то группу называют конечной, а число n называют порядком этой конечной группы. Если группа содержит бесконечное число элементов, то её называют группой бесконечного порядка.

Пример.
Рассмотрим множество целых чисел Z с операцией сложения.
$<Z, +>$ - *аддитивная* (add- складывать) группа целых чисел (абелева, бесконечного порядка).

Пример.
Пусть X – множество.
Обозначим через $S(X)$ *всевозможные* биективные отображения $X \to X$.
$S(X) = \{g: X \to X \mid \forall g(x)$ - биекция$\}$
На множестве S(X) рассмотрим операцию «$\circ$ » – композиции отображений.
Утверждается, что $<S(X), \circ>$ - группа.
Действительно, замечаем, что композиция на $S(X)$ бинарная операция, т.к. композиция биекций – биекция. Кроме того, выполнены аксиомы группы:
$G1:$ композиция отображений ассоциативна.
$G2:\ e(x) = x$ (тождественное отображение) очевидно $\in S(x)$, $e(x)$ – нейтральный элемент относительно операции «$\circ$ ».
$G3:$ Для $\forall$ биекции существует обратное отображение, которое тоже является биекцией.
Следовательно, $S(X)$ с операцией композиции «$\circ$ » – группа.

Пример.
Рассмотрим частный случай $S(X)$, когда множество X представляет собой отрезок множества натуральных чисел: $X = \{1, 2, 3, \ldots, n\}$. Тогда в качестве $S(X)$ получаем группу подстановок $S(\{1, 2, 3, \ldots, n\})$, которую обозначают Sn;
$<S_n, \circ>$ - группа подстановок.
Так как $|S_n| = n!$, то эта группа является конечной и имеет порядок $n!$

Пример.
$GL(n, R)$ – (General linear group) полная линейная группа невырожденных квадратных матриц порядка n с вещественными коэффициентами из R с операцией матричного умножения.
$GL(n, R) = \{A \in M_{n \times n} \mid det(A) \neq 0, a_{ij} \in R\}$
Нейтральный элемент в этой группе – единичная матрица $E \in GL(n, R)$.

Пример.
$GL(n, Q)$ – полная линейная группа невырожденных квадратных матриц порядка n с рациональными коэффициентами из Q с операцией матричного умножения.
$GL(n, Q) = \{A \in M_{n \times n} \mid det(A) \neq 0, a_{ij} \in Q\}$

Пример.
$SL(n, R)$ – (Special linear group) специальная линейная группа квадратных матриц порядка n с определителем равным 1 и с вещественными коэффициентами (операция - матричное умножение).
$SL(n, R) = \{A \in M_{n \times n} \mid det(A) = 1, a_{ij} \in R\}.$

Пример.
SL(n, Q) – специальная линейная группа квадратных матриц порядка *n* с рациональными коэффициентами и с определителем равным 1.
$SL(n, Q) = \{A \in M_{nxn} \mid det(A)=1, a_{ij} \in Q\}$.

Пример.
SL(n, Z) – специальная линейная группа квадратных матриц порядка *n* с целыми коэффициентами.
$SL(n,Z) = \{A \in M_{nxn} \mid det(A)=1, a_{ij} \in Z\}$.

Пример.
$<R, +>$ - аддитивная группа вещественных чисел.

Пример.
$<Q, +>$ - аддитивная группа рациональных чисел.

Пример.
$<R \setminus \{0\}, *>$ – мультипликативная (multiply - умножать) группа вещественных чисел.
Операция «$\circ$ » в этой группе – умножение. («*» – обычное умножение чисел).

Если имеется конечное множество *X*, снабженное бинарным законом $\circ$: *(X, $\circ$)*, то можно описать этот закон при помощи квадратной таблицы, строки и столбцы которой занумерованы элементами множества *X*, а на пересечении строки с индексом *x* и столбца с индексом *y* находится элемент $x \circ y$. В случае, когда *(X, $\circ$)* – группа, эту таблицу называют *таблицей Кэли*.

Пример.
Рассмотрев матрицы размера 1*x*1 с целыми коэффициентами получаем группу $SL(1, Z) = \{1, -1\}$ - конечную группу второго порядка.
Составим таблицу операции в этой группе (таблицу Кэли):

“o”	1	-1
1	1	-1
-1	-1	1

Теорема (Следствия из аксиом группы):
Пусть $<G, \circ >$ - группа, тогда:
1. Нейтральный элемент $e \in G$ – единственнен.
2. Элемент $a^{-1} \in G$ (являющийся обратным к элементу $a \in G$) единственнен.
3. $(a^{-1})^{-1} = a$.
4. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Доказательство.
1 и 2 пункты доказываются аналогично, как для моноида.
Докажем пункт 3. Согласно аксиоме G3 $a \circ a^{-1} = e$, то есть обратным к a^{-1} является a. Докажем пункт 4.
$(a \circ b) \circ (b^{-1} \circ a^{-1}) = (\text{согласно G1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = (G3;G1) =$
$= (a \circ e) \circ a^{-1} = (G2) = a \circ a^{-1} = (G3) = e$
Т.е. обратным для $(b^{-1} \circ a^{-1})$ является элемент $(a \circ b)$.

Определение.
Пусть $<G, \circ >$ - группа, множество $H \subset G$ называется *подгруппой*, если $<H, \circ >$ – группа.

Совершенно очевидно, что всякая группа $<G, \circ >$ всегда содержит 2 тривиальные подгруппы: подгруппу $<\{e\}, \circ >$ и подгруппу $<G, \circ >$.

Пример. Рассмотрим группу <Z,+>.
Множество четных чисел $2Z=\{2k \mid k \in Z\} \subset Z$. Несложно проверить, что $<2Z,+>$ -- группа.
Вообще, множество $mZ=\{mk \mid k \in Z\}$ чисел, кратных *m*, образует подруппу в аддитивной группе <Z,+>.

Теорема (Т1. о подгруппе):
Следующие три утверждения равносильны:
1. H – подгруппа группы G.
2. Если $a, b \in H$, то $(a \circ b) \in H$; если $b \in H$, то и $b^{-1} \in H$.
3. Если $a, b \in H$, то элемент $(a \circ b^{-1}) \in H$.

Доказательство.
Докажем импликацию (1) => (2):
Поскольку H – подгруппа группы G, то H – сама является группой относительно операции «$\circ$ », а, значит, эта операция бинарна на H, т.е. Если $a, b \in H$, то $(a \circ b) \in H$. Поскольку H – группа, то в ней выполнена аксиома G2, т.е. если $a \in H$, то и $a^{-1} \in H$.
Покажем, что (2)=>(1). Первая часть пункта 2 означает наличие бинарной операции на H, которая очевидно ассоциативна, поскольку в G ассоциативность выполнена. Вторая часть пункта 2 означает обратимость каждого элемента из H. Полагая $a = b^{-1}$ в $(a \circ b) \in H$ получаем, что $e \in H$. Все три аксиомы группы выполнены.
Докажем (2) => (3): Пусть $a, b \in H$; тогда $a^{-1} \in H$; $b^{-1} \in H$,
имеем $a, b^{-1} \in H => (a \circ b^{-1}) \in H$
Докажем (3) => (2):
Имеем $a, b \in H$, $(a \circ b^{-1}) \in H$.
Положим $a = b => (b \circ b^{-1}) \in H$, т.е. $e \in H$,
Положим теперь $a = e$, получим $(e \circ b^{-1}) \in H$, т.е. $b^{-1} \in H$,
Далее $a, b^{-1} \in H$, $=> a \circ (b^{-1})^{-1} \in H => a \circ b \in H$.

Теорема (Т2. о пересечении подгрупп):
Пусть H_α – семейство подгрупп в группе G (α- индекс, нумерующий подгруппы, не обязательно дискретный), тогда $\cap H_\alpha$ (пересечение подгрупп) является подгруппой.

Доказательство.
В силу Т1. (о подгруппе), достаточно доказать импликацию:
$a, b \in \cap H_\alpha => (a \circ b^{-1}) \in \cap H_\alpha$.
Имеем $a, b \in \cap H_\alpha => a, b \in$ каждому H_α (т.е. для $\forall \alpha$).
Тогда, т.к. H_α – подгруппа, то $(a \circ b^{-1}) \in H_\alpha$ (для каждого α), т.е. $(a \circ b^{-1}) \in \cap H_\alpha$.

Пусть G – группа.
Выберем в группе G какое нибудь подмножество $M \subset G$. Рассмотрим всевозможные подгруппы, каждая из которых содержит множество M. По Т2 (о пересечении подгрупп) пересечение всех этих подгрупп снова будет подгруппой. Её обозначают $<M>$. Эта подгруппа, в некотором смысле, будет минимальной подгруппой, содержащей M. Говорят, что множество M порождает подгруппу $<M>$.
Пусть M состоит из одного элемента $\{a\}$, тогда этот элемент порождает подгруппу $<a>$. Опишем более подробно структуру $<a>$.

Введем следующее соглашение:
$\underbrace{a \circ a \circ \ldots \circ a}_{\textbf{m раз}} = a^m, \quad m \in N$

тогда $(a^{-1})^m = \underbrace{a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}}_{\textbf{m раз}}$,

Лемма:
$(a^{-1})^m = (a^m)^{-1}$.

Доказательство.
$a^m \circ (a^{-1})^m = \underbrace{(a \circ a \circ \ldots \circ a)}_{\textbf{m раз}} \circ \underbrace{(a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1})}_{\textbf{m раз}} = e.$

Введем обозначение $a^{-m} = (a^{-1})^m$.

Напомним, также, что ранее введено соглашение $a^0=e$.

Теорема (Т3. о свойствах степеней):

1. $a^m \circ a^n = a^{m+n}$, $m, n \in Z$.
2. $(a^m)^n = a^{mn}$.

Доказательство пункта 1.

Случай $m \geqslant 0, n \geqslant 0$ рассмотрен и доказан ранее. Осталось рассмотреть следующие случаи:

1) $m < 0, n > 0$.

Обозначим $m' = -m$, тогда $m' > 0$.

Пусть для определенности $n > m'$.

$a^m \circ a^n = a^{-m'} \circ a^n = \underbrace{(a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1})}_{m' \text{ раз}} \circ \underbrace{(a \circ a \circ \ldots \circ a)}_{n \text{ раз}} = \underbrace{a \circ a \circ \ldots \circ a}_{n - m' \text{ раз}} = a^{n-m'} = a^{m+n}$.

Случаи $n < m'$ и $n = m'$ рассматриваются аналогично.

2) Случай $m < 0, n < 0$.

Обозначим $m' = -m$, $n' = -n$, тогда $m' > 0$, $n' > 0$.

$a^m \circ a^n = a^{-m'} \circ a^{-n'} = (a^{-1})^{m'} \circ (a^{-1})^{n'} = (a^{-1})^{m'+n'} = a^{-(m'+n')} = a^{-(-m-n)} = a^{(m+n)}$.

Пункт 2 доказывается аналогично.

Рассмотрим элемент $a \in$ группе G. Рассмотрим его всевозможные степени a^k, $(k \in Z)$.

Имеются 2 логические возможности:

1. Все степени a^k – различны, в этом случае говорят, что элемент a имеет *бесконечный порядок*.
2. Имеется совпадение, например $a^s = a^k$, $(s, k \in Z)$. Пусть для определенности $s > k$, тогда умножим обе части на a^{-k}.
   $a^s \circ a^{-k} = a^k \circ a^{-k}$, получим $a^{s-k} = e$. Обозначим $s - k = n \in N$. Т.е. в этом случае существует такое $n \in N$, что $a^n = e$. Пусть n – наименьшее из таких натуральных чисел n. Тогда говорят, что элемент a имеет *конечный порядок n*.

Определение:

Группа, содержащая конечное число элементов называется *конечной*. Число элементов группы называют *порядком группы*. Если же группа содержит бесконечное число элементов, то ее называют бесконечной.

Определение:

Группа, порожденная одним элементом a называется *циклической* и обозначается $<a>$.

Очевидно, что порядок циклической группы совпадает с порядком элемента, который эту группу порождает:

$<a> = \{a^k \mid k \in Z\}$. Она состоит из всевозможных степеней этого элемента.

Теорема (Т4. о циклической группе).

Всякая циклическая группа коммутативна.

Доказательство.

Для $\forall x, y \in <a>$:

$x = a^k$

$y = a^m$

$x \circ y = a^k \circ a^m = a^{k+m} = a^{m+k} = a^m \circ a^k = y \circ x$.

Итак, структура группы $<a>$ изучена полностью. Она циклическая -- т.е. состоит из *всевозможных* степеней элемента a, и обязательно коммутативна.

Группа $<a>$ устроена достаточно просто:

$<a> = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\}$ *если она бесконечного порядка, и*

$<a> = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ *если она имеет порядок n.*

Пример.

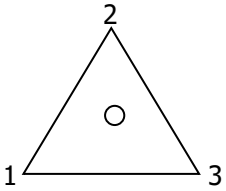
Аддитивная группа целых чисел - бесконечная, циклическая, порождена числом 1.
<Z, +> = <1>;
a = 1 – порождающий элемент этой группы.
Действительно, рассмотрим его степени:
$a^0 = e = 0$
$a^1 = a = 1$
$a^2 = a \circ a = 1 + 1 = 2$
$a^3 = a \circ a \circ a = 1 + 1 + 1 = 3$
и так далее.
Отрицательные степени:
$a^{-1} = -1$
$a^{-2} = (a^{-1})^2 = a^{-1} \circ a^{-1} = (-1)+(-1) = -2$
$a^{-3} = -3$ и т.д.

Пример.

Рассмотрим множество корней уравнения $z^m - 1 = 0$. Все его решения имеют вид $z_k = e^{i2\pi k/m} = \cos\left(\frac{2\pi k}{m}\right) + i\sin\left(\frac{2\pi k}{m}\right)$, $k = 0,1,2,\ldots,m-1$. Множество $K_m = \{z_k\}_{k=0}^{m-1}$ относительно операции умножения образует мультипликативную циклическую группу K_m порядка m, корней степени m из единицы.

Теорема (Т5. о порядке подгруппы, порожденной двумя образующими).
Если *a* и *b* – перестановочные элементы в группе *G*, имеющие взаимно простые порядки *m* и *k*, то тогда эти элементы порождают циклическую подгруппу *<a, b> = <ab>*, порядка *mk*.

Пример: (Группа D_3 самосовмещений правильного треугольника)
Рассмотрим равносторонний треугольник. Занумеруем его вершины.



Выпишем все движения, при которых он переходит в себя. Это вращения на 0°, 120°, -120° :

$$e = a_0 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \quad a_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \quad a_4 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

и отражения относительно высот:

$$a_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} \quad a_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} \quad a_5 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

Введем на множестве $\{a_0, \ldots, a_5\}$ операцию композиции " ∘ " (последовательного применения преобразований).
Например, вращение по часовой стрелке (на –120°) a_4, а затем отражение a_1 относительно высоты, проходящей через вершину 1 переводит вершину 1 → 3, вершину 2 → 2, вершину 3 → 1:

$$a_1 \circ a_4 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = a_3$$

Множество $\{a_0, \ldots, a_5\}$ относительно операции " ∘ " (последовательного применения преобразований) образует группу D_3 симметрий треугольника. Эта группа (порядка 6) может быть порождена, например, элементами a_2 (имеет порядок 3) и a_1 (порядка 2): $D_3 = \langle a_1, a_2 \rangle$.

В случае правильного n-угольника группу обозначают D_n. Ее называют группой диэдра. Вполне очевидно, что она порождается поворотами на углы $\frac{2\pi k}{n}$, $k = 0,1,\ldots,n-1$, и n осевыми симметриями. Легко проверить, что её порядок равен $|D_n| = 2n$.

§2. СРАВНЕНИЯ. ГРУППА КЛАССОВ ВЫЧЕТОВ

Определение:
Назовём два целых числа *a* и *b*, *сравнимыми по модулю* натурального числа *m,* если при делении на *m* они дают один и тот же остаток.

Пример.
Пусть, например, *m* = 3, тогда сравнимы числа 1, 4, 7, -2, -5, …
1 : 3 = 0 * 3 + 1
4 : 3 = 1 * 3 + 1
7 : 3 = 2 * 3 + 1
…

Если *a* и *b* сравнимы по модулю *m*, то пишут: $a \equiv b \pmod m$, например:
$4 \equiv 1 \pmod 3$
$7 \equiv -2 \pmod 3$
Объединим все числа сравнимые между собой по данному фиксированному модулю в множество, называемое классом сравнимых между собой чисел (по данному модулю). Например, если модуль *m*=3, то имеем следующие классы:
{0, 3, -3, 6, -6, …}
{1, 4, -2, 7, -5, …}
{2, 5, -1, 8, -4, …}
Для сокращения записи будем обозначать класс квадратными скобками, внутри которых укажем какое-нибудь число входящее в этот класс (его называют представителем класса), например
{0, 3, -3, 6, -6, …} = [0]
{1, 4, -2, 7, -5, …} = [7]
{2, 5, -1, 8, -4, …} = [-1]

Получившиеся классы называются классами вычетов по модулю *m*.

Договоримся, для удобства в качестве представителя класса писать остаток от деления на *m*, тогда классы по модулю *m* будут иметь вид:
[0], [1], [2], …, [*m*-1] – такую систему обозначений называют приведенной системой классов вычетов (по модулю *m*).
На множестве классов вычетов по модулю *m* введём операцию $\oplus$ сложения классов по правилу: $[x]\oplus[y] = [x+y]$. Можно показать, что операция сложения классов введена корректно, в том смысле, что результат операции не зависит от того, какой именно представитель класса указан в квадратных скобках. На множестве классов имеем бинарную операцию $\oplus$. Непосредственной проверкой убеждаемся, что для нее выполнены аксиомы *G1-G4*. Таким образом, на множестве классов имеем структуру абелевой группы, которую называют группой классов вычетов по модулю *m* и обозначают Z_m.

Пример.
Построим таблицу Кэли для классов вычетов по модулю 3 (группа Z_3):

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

В общем случае $<Z_m,\oplus>$ - аддитивная группа классов вычетов по модулю *m*.

Пример.
Введем операцию умножения классов по правилу: $[x]\otimes[y] = [xy]$. На множестве классов [1], [2], …, [*m*-1] имеем структуру группы. Ее называют мультипликативной группой классов вычетов $<Z_m\setminus[0],\otimes>$ по модулю *m*.

§3. СМЕЖНЫЕ КЛАССЫ ГРУППЫ ПО ПОДГРУППЕ, ФАКТОРГРУППА

Пусть $<G, \circ>$ группа, H – подгруппа группы G.

Определение.
Левым *смежным классом* элемента $x \in G$ называется множество
$x \circ H = xH = \{x \circ h / \forall h \in H\}$.

Определение.
Правым смежным классом элемента $x \in G$ называется множество
$H \circ x = Hx = \{h \circ x / \forall h \in H\}$.

Теорема (Т6. О левых смежных классах).
Два левых смежных класса (ЛСК) либо не пересекаются, либо совпадают.

Доказательство.
Пусть xH и yH – два каких либо левых смежных класса. Предположим, что они имеют общий элемент a, тогда существуют такие h_1 и $h_2 \in H$, что
$a = x \circ h_1$;
$a = y \circ h_2$; далее значок групповой операции "$\circ$" опускаем
$=> xh_1 = yh_2 => x = yh_2h_1^{-1}$; но, поскольку $h_2 h_1^{-1} \in H$, то $x \in yH$. Но тогда каждый элемент xh, $\forall h \in H$ представим в виде $xh = yh_2h_1^{-1}h$, то есть принадлежит классу yH. Имеем $xh \in yH => xH \subset yH$.
Аналогично доказывается $yH \subset xH$.
Из этих двух вложений следует, что классы совпадают.

Множество всех левых смежных классов (л.с.к.) принято обозначать G / H, а множество всех правых смежных классов (п.с.к.) – $G \mid H$.

Теорема (Т7. Об отображении H → xH):
Отображение $H \rightarrow xH$ является биекцией.

Доказательство.
Сюръективность $h \rightarrow xh$ следует из определения левых смежных классов. Осталось доказать инъективность. Нужно показать, что из условия
$h_1 \neq h_2 => xh_1 \neq xh_2$
Предположим, что это не так:
$xh_1 = xh_2 => x^{-1}xh_1 = x^{-1}xh_2 => h_1 = h_2$ – противоречие с условием.

Следствие.
Если группа конечная, то доказанная выше теорема означает, что каждый левый смежный класс содержит одинаковое число элементов равное числу элементов в подгруппе H .

Теорема 8. (Лагранжа):
Пусть G – конечная группа порядка $|G|$, H – её подгруппа. Тогда порядок подгруппы H является делителем порядка группы G.

Доказательство.
На основании Т7 делаем заключение, что каждый левый смежный класс содержит столько же элементов, сколько подгруппа H, кроме того, левые смежные классы не пересекаются, поэтому имеем разбиение группы G на $|G / H|$ непересекающихся подмножеств, каждое из которых содержит $|H|$ элементов, тогда:
$|G| = |G / H| * |H|$

Следствие из теоремы Лагранжа.
Порядок любого элемента конечной группы является делителем порядка группы.

Доказательство.
Всякий элемент a конечной группы G порождает в этой группе конечную циклическую подгруппу, но, согласно, теореме Лагранжа порядок этой подгруппы, есть делитель порядка группы. Осталось заметить, что порядок элемента и порядок порожденой им циклической подгруппы совпадают.

Определение.
Подгруппа H группы G называется *нормальной подгруппой* (нормальным делителем), если для любого элемента x группы G выполняется $xH = Hx$ (если левый смежный класс любого элемента x совпадает с его правым смежным классом).

Заметим, что на множестве левых смежных классов можно естественным образом ввести операцию по правилу $(xH)\circ(yH) = (x\circ y)H$. Легко убедиться, что эта операция является бинарной и удовлетворяет аксиомам группы.

Определение.
Множество левых смежных классов группы G по её нормальной подгруппе H относительно операции над левыми смежными классами $(xH)\circ(yH) = (x\circ y)H$, называется *фактор группой* группы G по ее нормальной подгруппе H и обозначается G / H.

Пример.
В аддитивной группе $G=<Z,+>$ имеется нормальная подгруппа $H=<2Z,+>$. Действительно,

Л.с.к. G/H:	П.с.к. $G\|H$:
$0+H=\{0,2,-2,4,-4,\ldots\}$	$H+0=\{0,2,-2,4,-4,\ldots\}$
$1+H=\{1,3,-1,5,-3,\ldots\}$	$H+1=\{1,3,-1,5,-3,\ldots\}$

Таблица Кэли факторгруппы $Z/2Z$

+	0+H	1+H
0+H	0+H	1+H
1+H	1+H	0+H

Несложно видеть, что л.с.к. группы Z по подгруппе $2Z$ представляют собой классы вычетов по модулю 2, и эта факторгруппа совпадает с аддитивной группой Z_2 классов вычетов по модулю 2. И, вообще $Z/mZ = Z_m$.

§4. ГРУППА ПОДСТАНОВОК S_N

Пусть S_n – множество всех подстановок элементов множества $M = \{1, 2, 3, \ldots, n\}$ (S_n – множество всех биекций из M в M).
Операция «$\circ$ » на S_n – композиция (последовательное выполнение) подстановок. Несложно видеть, что множество S_n с операцией «$\circ$ » образует группу. Напомним, что $|S_n| = n!$

Пример: (Группа S_3)
Рассмотрим подстановки трехэлементного множества (Подстановок 3! = 6)

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \quad a_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \quad a_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$
$$a_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \quad a_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \quad a_5=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

Построим таблицу умножения элементов группы (таблицу Кэли). Для этого вычислим всевозможные произведения, например

$$a_4\circ a_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=a_5$$

Далее найдем, что (значок " $\circ$ " не пишем)

$$a_1a_1=e \quad a_1a_2=a_5 \quad a_1a_3=a_4 \quad a_1a_5=a$$
$$a_2a_1=a_3 \quad a_2a_2=a_4 \quad a_2a_3=a_5 \quad a_2a_4=e \quad a_2a_5=a_1$$
$$a_3a_1=a_2 \quad a_3a_2=a_1 \quad a_3a_3=e \quad a_3a_4=a_5 \quad a_3a_5=a_4$$

$a_4a_1=a_5 \quad a_4a_2=e \quad a_4a_3=a_1 \quad a_4a_4=a_2 \quad a_4a_5=a_3$

$a_5a_1=a_4 \quad a_5a_2=a_3 \quad a_5a_3=a_2 \quad a_5a_4=a_1 \quad a_5a_5=e$

таблица Кэли:

"∘"	e	a_1	a_2	a_3	a_4	a_5
e	e	a_1	a_2	a_3	a_4	a_5
a_1	a_1	e	a_5	a_4	a_3	a_2
a_2	a_2	a_3	a_4	a_5	e	a_1
a_3	a_3	a_2	a_1	e	a_5	a_4
a_4	a_4	a_5	e	a_1	a_2	a_3
a_5	a_5	a_4	a_3	a_2	a_1	e

Группа S_3 вообще говоря не является комутативной, например $a_1a_4 \neq a_4a_1$.

Задача: Найти элемент, обратный к $a=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

Решение: $a^{-1}=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

Найдем нетривиальные подгруппы данной группы S_3:
$H_1=\{ e, a_2, a_4\}$, $H_2=\{ e, a_1 \}$, $H_3=\{ e, a_3 \}$, $H_4=\{ e, a_5 \}$,

Вычислим всевозможные степени элемента a_2:

$$a_2^2=a_2a_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=a_4$$

$$a_2^3=a_2a_2a_2=a_2a_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$$

Значит, $H_1=\{ e, a_2, a_4\}=\langle a_2\rangle$ – циклическая подгруппа порядка 3, порождаемая элементом a_2. Замечаем, что $a_2a_4=a_2a_2a_2=a_4a_2$ (H_1 – коммутативна, т.к. циклическая). Порядок элемента a_2 равен 3.
Заметим, что $S_3=\langle a_1, a_2\rangle$, т.е. ее можно породить элементами a_1 и a_2 .

Выпишем S_3/H_2 (л.с.к. S_3 по H_2)
$eH_2=\{ e, a_1 \}$, $a_2H_2=\{ a_2, a_3 \}$, $a_4H_2=\{ a_4, a_5 \}$
Выпишем $S_3|H_2$ (п.с.к. S_3 по H_2)
$H_2e=\{ e, a_1 \}$, $H_2a_2=\{ a_2, a_5 \}$, $H_2a_4=\{ a_4, a_3 \}$

Левый класс элемента a_2 не совпадает с его правым классом.
Выпишем теперь S_3/H_1 (л.с.к. S_3 по H_1) и $S_3|H_1$ (п.с.к. S_3 по H_1):

Л.с.к:
$eH_1=\{ e, a_2, a_4\}$ и $a_1H_1=\{ a_1, a_5, a_3\}$.
П.с.к:
$H_1e=\{ e, a_2, a_4\}$ и $H_1a_1=\{ a_1, a_5, a_3\}$.
Левый смежный класс каждого элемента группы совпадает с его правым смежным классом. Следовательно подгруппа H_1 нормальная, поэтому по ней можно построить факторгруппу..

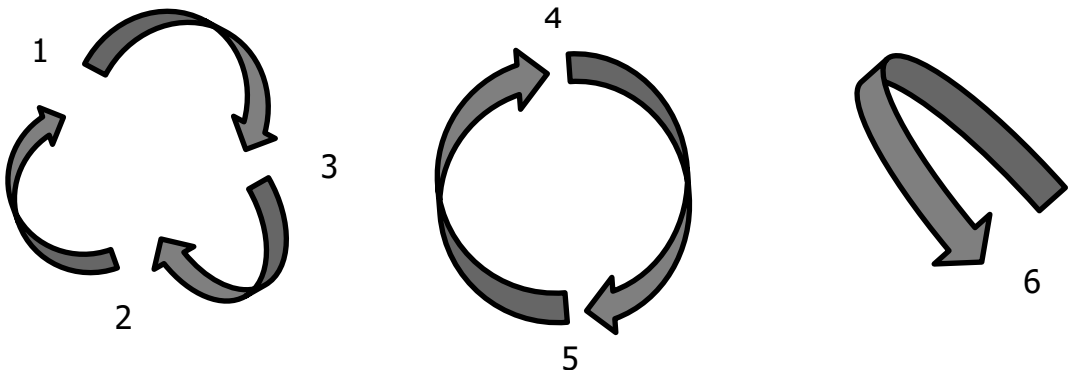
Таблица Кэли факторгруппы S_3/H_1

" ∘ "	eH_1	a_1H_1
eH_1	eH_1	a_1H_1
a_1H_1	a_1H_1	eH_1

Изучим более детально действие подстановок S_n на множестве $M = \{1, 2, 3, \ldots, n\}$. Например, рассмотрим множество подстановок шестой степени $<S_6, \circ >$, и возьмем из этого множества, подстановку

$\delta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{bmatrix}$

$\delta \in S_6$, которую можно изобразить на рисунке



{1, 2, 3} {4, 5} {6}

Ω_1 Ω_2 Ω_3

Видим, что эта подстановка действует на трех независимых множествах Ω_1,Ω_2 и Ω_3. Поэтому ее можно записать в виде композиции подстановок, каждая из которых действует на своем множестве Ω_i. Подстановку, действующую на Ω_i называют независимым циклом.

$\delta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 5 & 4 \end{bmatrix} \begin{bmatrix} 6 \\ 6 \end{bmatrix}$

$\delta = (1 \to 3 \to 2) \circ (4 \to 5) \circ (6) = (1\ 3\ 2) \circ (4\ 5) \circ (6)$ – запись подстановки в виде трех независимых циклов . Независимые циклы коммутируют, поскольку действуют на непересекающихся множествах. Удобно ввести понятие длины (порядка) цикла, которая равна $|\Omega_i|$. Например, цикл (132) имеет длину (порядок) 3, которая равна $|\Omega_1|$. Цикл (45) имеет длину 2. Цикл (6) имеет длину 1.

Теорема (Т9. О порядке подстановки):

Порядок подстановки равен наименьшему общему кратному (НОК) порядков (длин) независимых циклов.

Доказательство.

Рассмотрим подстановку δ и разложим её в независимые циклы:

$\delta = \beta_1\beta_2 \ldots \beta_k$;

Обозначим q_k – порядок цикла β_k (он совпадает с длиной цикла), тогда

$\beta_k^{q_k} = e$

Если $\delta^q = e \Rightarrow \beta_1^q\beta_2^q \ldots \beta_k^q = e \Rightarrow \forall k,\ \beta_k^q = e \Rightarrow q$ – НОК чисел $q_1, q_2, \ldots q_k$.

Рассмотрим независимый цикл (1 2 3), его можно представить как композицию циклов длины 2:

(1 2 3) = (1 3)$\circ$ (1 2)

Однако, заметим, что (1 3)$\circ$ (1 2) $\neq$ (1 2)$\circ$ (1 3)

не коммутируют

Совершенно ясно, что если циклы действуют на непересекающихся множествах, то они коммутируют. И, напротив, если они действуют на множествах, имеющих общие элементы, то, вообще говоря, переставлять их нельзя.

Договоримся далее, при записи не коммутирующие циклы заключать в квадратные скобки [].

Определение.

Цикл длины 2 называется *транспозицией*.

Совершено очевидно, что всякий независимый цикл длины 2 или больше можно разложить в транспозиции:

(1 2 3 … k) = (1 k) … (1 3)(1 2).

Таким образом *всякую* подстановку можно разложить в транспозиции.

Определение.
Число $(-1)^m$, где m – число транспозиций подстановки называют её *сигнатурой*.

Пример:
$\delta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{bmatrix}$;

δ = (1 3 2)(4 5)(6) = [(1 2)(1 3)][(4 5)][(6)];
Три транспозиции, сигнатура подстановки = -1.

Определение.
Подстановка называется *чётной*, если её сигнатура равна (+1) и *нечётной*, если её сигнатура равна (-1).

Обозначим через A_n множество всех четных подстановок в группе S_n . Операция «$\circ$ » (композиция) является бинарной на A_n. Несложно проверить, что A_n - подгруппа в группе S_n.
Группа A_n имеет специальное название – знакопеременная группа степени n.

Теорема.
$|A_n| = n!/2$.

§5. ПРЯМОЕ ПРОИЗВЕДЕНИЕ ГРУПП

Пусть имеется две группы: $<G_1, \circ >$ и $<G_2, *>$.
Из этих двух групп можно построить новую группу следующим образом: образуем множество всевозможных пар (g_1,g_2), где $\forall g_1 \in G_1$, $\forall g_2 \in G_2$.
Далее, введем над полученными парами операцию по правилу:
$(g_1,g_2)\ (s_1,s_2) = (g_1 \circ s_1,\ g_2 * s_2)$
Несложно проверить, что множество таких пар относительно введенной операции над парами образует группу. Его называют *прямым произведением* групп G_1 и G_2 и обозначают G_1 x G_2.

Пример: Группа $Z_3 x Z_2$.

$Z_3=\{0,1,2\}$ *(квадратные скобки при обозначении классов опущены)*
$Z_2=\{0,1\}$
Имеем шесть пар
$Z_3 x Z_2=\{(0,0);\ (0,1);\ (1,0);\ (1,1);\ (2,0);\ (2,1)\}$.

Таблица Кэли операции над парами

	(0,0)	**(0,1)**	**(1,0)**	**(1,1)**	**(2,0)**	**(2,1)**
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(2,1)	(2,0)	(0,1)	(0,0)
(2,0)	(2,0)	(2,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(0,1)	(0,0)	(1,1)	(1,0)

Нейтральный элемент этой группы (0,0).
Группа циклическая с образующим элементом (1,1).

§6. ИЗОМОРФИЗМ ГРУПП

При внимательном рассмотрении многочисленных примеров групп, обнаруживается, что многие из них устроены одинаковым образом, например группы D_3 и S_3, факторгруппа S_3/H_1 и группа Z_2 классов вычетов по модулю 2, группа классов вычетов Z_m и факторгруппа Z/mZ, и так далее. Это обстоятельство приводит к понятию изоморфных групп.

Пусть $<G, \circ>$ и $<G', *>$ - группы. Отображение $f: G \to G'$ называют *изоморфизмом*, если:
1) f – биекция;
2) $f(a \circ b) = f(a)*f(b), \quad \forall a,b \in G$. (т.е. f сохраняет операцию)

Если группы G_1 и G_2 изоморфны, то пишут $G_1 \sim G_2$.

Свойства изоморфизма:
1) $e \to e'$ *(нейтральный элемент переходит в нейтральный)*
2) $f(a^{-1}) = f(a)^{-1}$
3) Отображение обратное к изоморфизму также является изоморфизмом.

Доказательство.
1) $e \circ a = a \circ e = a$
$f(e \circ a) = f(a \circ e) = f(a)$
$f(e) * f(a) = f(a) * f(e) = f(a)$. Обозначим $f(e)=x$.
$x*a' = a'*x = a' \Rightarrow x=e' \Rightarrow f(e) = e'$

2) $a \circ a^{-1} = a^{-1} \circ a = e$
$f(a \circ a^{-1}) = f(a^{-1} \circ a) = f(e)$
$f(a) * f(a^{-1}) = f(a^{-1})*f(a) = e'$, т.е. $f(a)^{-1} = f(a^{-1})$.

3) Т.к. f – биекция, то f^{-1} тоже биекция.
$f^{-1}(a'* b') = f^{-1}(a') \circ f^{-1}(b')$, для $\forall a' и\ b' \in G'$
Возьмем $\forall a' и\ b' \in G'$, тогда
$a'* b' = f(a) * f(b)$ = (найдутся такие $a, b \in G$) $= f(a \circ b)$
$f^{-1}(a'* b') = a \circ b$
$f^{-1}(a'* b') = f^{-1}(a') \circ f^{-1}(b')$

Пример. $Z_3 \times Z_2 \sim Z_6$. Изоморфизм устанавливается правилом (1,1) <—> [1].

Пример. Вполне очевидно, что $D_3 \sim S_3$.

Пример. $SL(1, Z) \sim Z/2Z \sim S_3/H_1$

Теорема (об изоморфизме циклических групп).
Все циклические группы одинакового порядка изоморфны.

Доказательство.
Пусть $<G, *>$ - циклическая группа, порожденная элементом g.
$<G, *> = \{e, g, g^2, \ldots\}$
Возможны 2 случая:
1) G – циклическая группа бесконечного порядка, тогда она состоит из элементов:
$\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots$
Рассмотрим группу $<Z, +>$
$f: g^k \to 1^k = 1 + 1 + 1 + \ldots + 1 = k$
Док-во того факта, что f – изоморфизм, предоставляем читателю для самостоятельного рассуждения.
2) G – конечная циклическая группа порядка n.
Рассмотрим отображение из G в группу классов вычетов по модулю n.
$f: G \to Z_n$.
Док-во того, что f – изоморфизм также предоставляем читателю.

Следующая теорема позволяет полностью описать структуру *всех* конечных групп.

Теорема (Кэли).

Всякая *конечная* группа G изоморфна либо S_n, либо какой либо её подгруппе.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1) Декартово произведение.
2) Отношения.
3) Отображение, инъекция, сюръекция, биекция, композиция. Теорема об ассоциативности композиций.
4) Тождественное отображение. Левое и правое обратное, двустороннее. Теорема об обратимости биекции. Следствие.
5) Теорема о композиции инъективных отображений. Теорема о композиции сюръективных отображений. Теорема о композиции биективных отображений.
6) Подстановки.
7) Бинарная операция. Ассоциативные и комутативные операции. Нейтральный элемент. Полугруппа. Моноид. Примеры.
8) Степени. Теорема о комутирующих элементах. Обратимые элементы моноида. Лемма о единственности обратного.
9) Группа. Порядок группы. Следствие из аксиом группы.
10) Подгруппа. Теоремы о подгруппах.
11) Порождающие элементы. Теорема о свойствах степеней.
12) Циклические группы. Порядок элемента. Теорема о комутативности циклической группы.
13) Сравнения. Группа классов вычетов.
14) Смежные классы.
15) Теорема о левых смежных классах.
16) Теорема об отображении из H в xH.
17) Теорема Лагранжа. Следствие.
18) Нормальная подгруппа. Фактор группа.
19) Прямое произведение групп. Изоморфизм.
20) Теорема об изоморфизме циклических групп.
21) Теорема (Кэли).