МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА «ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Введение в алгебраические системы. Группы.

Методические указания к изучению курса
«*Дискретная математика*»

для студентов специальностей:
1-53 01 02 «Автоматизированные системы обработки информации»,
1-40 03 01 «Искусственный интеллект»
и 1-40 01 01 «Программное обеспечение информационных технологий»

Брест 2019

УДК 512.5/.8(07)

В методических указаниях рассмотрены основные понятия теории групп, изучаемой в курсе «Дискретная математика». Теория изложена доступным языком, с многочисленными примерами и пояснениями.

Методические указания предназначены для использования студентами специальностей 1-53 01 02 «Автоматизированные системы обработки информации», 1-40 03 01 «Искусственный интеллект» и 1-40 01 01 «Программное обеспечение информационных технологий » в ходе изучения курса «Дискретная математика».

Составители: Глущенко Т.А., старший преподаватель кафедры ИИТ
Хацкевич М.В., старший преподаватель кафедры ИИТ
Кот А.А., инженер-электроник кафедры АТПиП

Рецензент: Козинский А.А., доцент кафедры прикладной математики и информатики Учреждения образования «Брестский государственный университет им. А.С. Пушкина», к. пед. н., доцент

Учреждение образования

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Дискретная математика является важной составляющей в системе подготовки инженеров специальностей «Автоматизированные системы обработки информации», «Искусственный интеллект» и «Программное обеспечение информационных технологий », поскольку понятия, методы и алгоритмы дискретной математики широко применяются как в информатике в целом, так и в практическом программировании.

В данном пособии рассмотрены основные положения теории групп. Теория групп лежит в основе криптографических методов защиты информации, построения корректирующих кодов. Как раздел абстрактной алгебры, теория групп занимает важное место в системе подготовки специалистов, работающих в *IT* сфере.

В пособии в доступной форме изложены основные понятия теории групп, каждое вновь вводимое понятие пояснено на примерах. Подробно разобрана группа подстановок, дано понятие фактор-группы.

Данное методическое пособие разработано в соответствии с учебными программами по дисциплине « Дискретная математика» для специальностей 1-53 01 02 «Автоматизированные системы обработки информации», 1-40 03 01 «Искусственный интеллект» и 1-40 01 01 «Программное обеспечение информационных технологий ».

ТЕМА № 1. ***ОСНОВНЫЕ ПОНЯТИЯ ГРУППЫ***

Будем рассматривать *алгебраические структуры*, на которых задано только множество алгебраических операций (множество отношений пусто) и определим *алгебраическую структуру* как *непустое* множество вместе с операциями, определенными на этом множестве. Будем рассматривать *бинарные операции*. Как мы знаем, бинарные операции обладают *свойством замыкания*, т. е. результат операции над двумя элементами *a* и *b* множества *S* также является элементом *S*. Условно будем обозначать бинарную операцию символом *. Обычно операции имеют некоторые характерные свойства, которые могут быть обоснованы в виде теорем и правил, используемых в вычислениях. Структуру вместе со всеми теоремами, правилами вычислений и вывода иногда называют *алгебраической системой*.

Например, $(Z,+)$ – алгебраическая система целых чисел с операцией сложения, являющаяся абелевой группой; система $(Z,+,*)$ с двумя бинарными операциями: сложением и умножением – коммутативное кольцо целых чисел. В то же время множество Z с операцией деления не является алгебраической системой, поскольку результат выполнения данной операции не обязательно принадлежит множеству Z (не выполняется свойство замкнутости алгебраической системы).

Алгебраические системы различают по операциям и свойствам этих операций.

Алгебраическая система (*S*,*) с одной алгебраической операцией * на множестве *S* называется *группоидом*. И, как мы уже отмечали, если $a,b \in S$, то и результат операции $a*b \in S$ (говорят также, что множество *S* обладает свойством замкнутости относительно операции *).

Если у группоида (*S*,*) операция * *ассоциативна*, т. е. для всех *a, b* и *c* из *S* имеет место

*(a*b) * c = a* (b* c),*

то такую алгебраическую систему называют *полугруппой*. Если, в дополнение к этому, для всех *a* и *b* из *S* выполняется

*a*b = b**a*,

то полугруппа называется *абелевой*, или *коммутативной полугруппой*.

Если в полугруппе (*S*,*) существует элемент *e* такой, что

*e*a = a*e =a*

для всех *a* из *S*, то такой *e* называется *нейтральным элементом*, или *единичным элементом*, или *единицей полугруппы* (*S*,*), а сама (*S*,*) называется *полугруппой с единицей*, или *моноидом*.

Рассмотрим примеры алгебраических систем.

- Множество натуральных чисел *N* с операцией сложения, $(N,+)$ – коммутативная (абелева) полугруппа. Напомним, что $0 \notin N$ и в полугруппе нет нейтрального элемента относительно сложения.
- Множество натуральных чисел *N* с операцией умножения, $(N,*)$ – абелев моноид, нейтральный элемент – *1*.

В то же время множество натуральных чисел *N* с операциями вычитания или деления не является группоидом (и алгебраической системой), поскольку результат выполнения этих операций не обязательно принадлежит множеству *N* (не выполняется свойство замкнутости алгебраической системы).

- Множество целых чисел Z относительно умножения, $(Z,*)$ – абелев моноид, $(Z,-)$ – группоид (операция *«-»* – не ассоциативна).
- Множество целых чисел, делящихся на n $(n \in N \wedge n > 1)$ без остатка относительно операции умножения, $(nZ,*)$ – абелева полугруппа.
- Множество квадратных матриц порядка $n>1$ с вещественными коэффициентами относительно сложения, $(M_n(R),+)$ – коммутативный моноид (точнее группа), единичным элементом является нулевая матрица; относительно операции умножения $(M_n(R),*)$ – некоммутативный моноид, единичный элемент – единичная матрица.

Если множество S бесконечно, алгебраическая система является *бесконечной*, все рассматриваемые нами ранее алгебраические системы являлись бесконечными. Если множество S *конечно*, то система *конечна* и мощностью системы (*порядком*) называется мощность множества S. Конечные алгебраические системы удобно задавать таблицами *Кэли*, если операций несколько, строится своя таблица для каждой операции.

Группы

Группой $(G,*)$ называется *непустое* множество G с определённой на нем *бинарной алгебраической операцией* *, обладающей следующими свойствами:

1. Операция * *ассоциативна*, т. е. $a*(b*c)=(a*b)*c$ *для* $\forall a,b,c \in G$
2. В G существует *нейтральный элемент* e, такой, что для любого $a \in G$ выполняется $a*e=e*a=a$.
3. Для *каждого* $a \in G$ существует *обратный* элемент $a^{-1} \in G$, такой что $a*a^{-1}=a^{-1}*a=e$.

Эти условия иногда называют *аксиомами группы*.

Если групповая операция * удовлетворяет также следующему условию:

4. Для любых $a,b \in G$ выполняется $a*b=b*a$ (операция * коммутативна), то группа G называется *абелевой* (или *коммутативной*).

В любой группе G нейтральный элемент e и обратный элемент a^{-1} к каждому элементу определены *однозначно*.

Для элементов группы справедливы следующие соотношения:

$(a*b)^{-1}=b^{-1}*a^{-1} \quad \forall a,b \in G$

$(a^{-1})^{-1}=a \quad \forall a \in G$

Заметим, что здесь * – это *условное обозначение бинарной операции*.

Группа называется *аддитивной*, или *группой по сложению*, если групповая операция является *сложением*. В этом случае символ операции * заменяют на +: $c = a + b$, нейтральный элемент называется *нулем* и обозначается символом *«0»*, а обратный элемент к a называется *противоположенным* и обозначается как $-a$.

Группа называется *мультипликативной*, или *группой по умножению*, если групповая операция является *умножением*. Нейтральный элемент мультипли-

кативной группы называется *единицей* и обозначается символом *«1»*, обратный элемент к элементу *a* обозначается как a^{-1}.

В каждой мультипликативной группе *однозначно* разрешимы уравнения $a \cdot x = b$ и $y \cdot a = b$. Соответствующие решения уравнений: $x = a^{-1} \cdot b$ и $y = b \cdot a^{-1}$. Если группа абелева, эти уравнения имеют одинаковое решение: $x = y = a^{-1} \cdot b$.

Пусть $a \in G$ и $n \in N$.

Для аддитивной группы полагаем, что *na = a + a +…+ a* (*n* слагаемых *a*).

Для мультипликативной группы полагаем, что $a^n = a \cdot a \cdot ... \cdot a$ (*n* сомножителей *a*).

Для *n = 0* полагаем *0a = 0* в аддитивной записи и $a^0 = 1$ в мультипликативной записи. В обоих соотношениях справа стоят нейтральные элементы соответствующих групп.

Если *a* – элемент группы *G*, то обозначим $(a^{-1})^n = a^{-n}$ для мультипликативной записи и *n(-a) = (-n)a* для аддитивной записи.

С учетом введенных обозначений справедливы следующие соотношения (в мультипликативной записи):

1. $a^n \cdot a^{-n} = 1$ для всех $n \in N$.
2. $a^{(m+n)} = a^m \cdot a^n$ для всех $n, m \in Z$.
3. $(a^m)^n = a^{m \cdot n}$ для всех $n, m \in Z$.
4. $(a^{-n})^{-1} = a^n$ для всех $n \in Z$

По количеству элементов группы делятся на *конечные* и *бесконечные* группы.

Порядком конечной группы называется количество элементов этой группы. Если *G = (G,∗)* − конечная группа, то |*G*| − ее порядок.

Рассмотрим примеры групп.

Аддитивными абелевыми группами являются:

1. $(Z,+), (Q,+), (R,+), (C,+)$;

2. Множество прямоугольных $(n \times m)$ матриц с вещественными коэффициентами и бинарной операцией сложения матриц.

3. Множество *A = {0,1,2,3,4,5}* с операцией сложения по модулю *6*: $G = (A, \oplus_{\mathrm{mod}6})$.

Группы из *1*, *2* примера являются бесконечными, *3* пример – конечная группа порядка *6*.

Построим для группы из примера *3* таблицу *Кэли*.

$\oplus_6$	*0*	*1*	*2*	*3*	*4*	*5*
0	*0*	*1*	*2*	*3*	*4*	*5*
1	*1*	*2*	*3*	*4*	*5*	*0*
2	*2*	*3*	*4*	*5*	*0*	*1*
3	*3*	*4*	*5*	*0*	*1*	*2*
4	*4*	*5*	*0*	*1*	*2*	*3*
5	*5*	*0*	*1*	*2*	*2*	*4*

Нейтральный элемент – *0*. Найдем обратные элементы, например, для *5* обратным элементом является *1*, для *2* обратный элемент – *4*.

Мультипликативными группами являются:

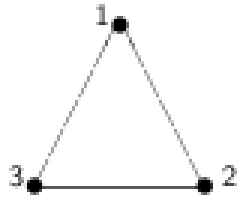
4. Множество *{-1,1}* с операцией умножения образует абелевую группу по умножению. Нейтральным элементом является *1*, в этой группе обратный элемент к каждому элементу совпадает с самим элементом, $a^{-1} = a$ для всех $a \in G$. Как мы уже отмечали, множества *Z* не образует группу по умножению.

5. $(Q,^**)$, $(R,^**)$, $(C,^**)$, где $Q^* = Q \setminus \{0\}$, $R^* = R \setminus \{0\}$, $C^* = C \setminus \{0\}$. Эти группы являются абелевыми.

6. Множество квадратных матриц порядка *n>1* с вещественными коэффициентами и определителем, не равным нулю, относительно операции матричного умножения образует некоммутативную группу $(GL_n(R),*)$.

7. Множество *A = {1,2,3,4}* с операцией умножения по модулю *5*: $G = (A, \otimes_{\mathrm{mod}5})$. Это конечная абелева группа.

8. Группа вращений правильного треугольника в плоскости, при которых он совмещается сам с собой. Имеем три элемента, три поворота на углы в градусах: $e = 0$ $\varphi_1 = 2\pi/3$, $\varphi_2 = 4\pi/3$.



Здесь групповая операция * представляет собой последовательное применение поворотов. Группа является абелевой. Таблица Кэли имеет вид:

*	e	φ_1	φ_2
e	e	φ_1	φ_2
φ_1	φ_1	φ_2	e
φ_2	φ_2	e	φ_1

Непустое подмножество *H* группы *G* называется *подгруппой* этой группы, если *H* само образует группу относительно операции группы *G*. Подгруппа *H = {e}* называется *тривиальной*. Если $H \neq \{e\}$ и $H \neq G$, то такая подгруппа *H* группы *G* называется *собственной* подгруппой и обозначается *H < G*. *Нейтральный элемент группы G обязательно принадлежит H.*

Очевидно, аддитивные группы целых, рациональных, вещественных и комплексных чисел образуют систему подгрупп:

(*Z*,+) < (*Q*,+) < (*R*,+) < (*C*,+).

Подмножество всех целых чисел, кратных натуральному числу *n >1*, образует подгруппу в группе целых чисел с операцией сложения. Эту подгруппу обозначают через (*nZ*,+).

Следовательно, имеют место бесконечные цепочки аддитивных подгрупп типа *(Z,+)>(2Z,+)>(4Z,+)>…* .

Для нашего примера *3* множество *H = {0, 2 ,4}* является подгруппой группы $G = (A, \oplus_{\mathrm{mod}6})$. Составим для *H* таблицу *Кэли*.

$\oplus_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Справедлива следующая теорема, дающая *критерий* подгруппы.

Теорема 1. Непустое подмножество *H* группы (*G*, *) будет подгруппой тогда и только тогда, когда для всех $a,b \in H$ имеем $a*b^{-1} \in H$.

Проверим выполнение критерия для нашей конечной подгруппы: $2,4 \in H$, обратный элемент к *4* это *2*, $2+2=4 \in H$. Как видим, критерий выполняется, и так для всех пар элементов подгруппы *H*.

Пусть *G = (G,∗)* – группа с нейтральным элементом *e*. Для элемента $a \in G$ *наименьшее натуральное число n* (если оно существует) такое, что $a^n = e$ для мультипликативной группы или $na = e$ для аддитивной группы, называется его *порядком*. Если же для элемента $a \in G$ такого n не существует, то говорят, что элемент $a \in G$ имеет *бесконечный* порядок. Например, для аддитивной группы, $G = (A, \oplus_{\mathrm{mod}6})$, где *A={0,1,2,3,4,5}*, порядок элемента *4* равен *3*: *4 + 4 + 4 = 12* по модулю *6* равно *0* (нейтральный элемент). Для мультипликативной группы $G = (A, \otimes_{\mathrm{mod}5})$ из примера *7*, где множество *A = {1, 2, 3 ,4}*, порядок элемента *4* равен *2*: $4^2 = 16$ и по модулю *5* равно *1* (нейтральный элемент).

Для группы $(Z,+)$ все ненулевые элементы имеют бесконечный порядок.

Пусть *G = (G,∗)* – конечная группа и $e \in G$ – ее нейтральный элемент. Тогда для любого элемента $a \in G$ справедливо: $a^{|G|} = e$ в мультипликативной записи или $|G|\,a = e$ в аддитивной записи.

Группа *G = (G,∗)* называется *циклической*, если в ней имеется такой элемент *a*, что каждый элемент $b \in G$ является степенью элемента *a*, т. е. существует *целое число k*, такое, что $b = a^k$. Этот элемент *a* называется *образующим элементом* группы *G*, и он может быть *не единственным*. Для циклической группы *G*, *порожденной элементом a*, применяют обозначение *G = <a>*.

Подгруппа группы *G*, состоящая из всех степеней элемента *g* этой группы, называется подгруппой, порожденной элементом *g*, и обозначается символом <g>. Эта подгруппа является, очевидно, циклической. Если *<g>* – конечная подгруппа, то ее порядок называется порядком элемента *g*.

Рассмотрим пример.

Пусть задано множество *A = {0 ,1, 2, 3, 4, 5, 6, 7}*. Рассмотрим группу $G = (A, \oplus_{\mathrm{mod}8})$ с групповой операцией сложения по модулю *8*. Тогда $<2>=\{2,\ 2^2 = 2+2 = 4,\ 2^3 = 2+2+2 = 6,\ 2^4 = 2+2+2+2 = e\} = \{2,4.6.0\}$ – циклическая подгруппа группы *G*, порядка *4*, порожденная элементом *2*, а $<4>=\{4,4^2 = 4+4 = e\} = \{4.,0\}$ – циклическая подгруппа порядка *2*, порожденная элементом *4*. Сама наша группа *G* также является циклической и *G = <1> = = <3> = <5>*.

Справедливы следующие теоремы.

Теорема 2. Всякая подгруппа циклической группы является циклической.

Теорема 3. Всякая циклическая группа абелева.

ТЕМА № 2. *ГРУППА ПОДСТАНОВОК*

Пусть A – конечное множество из n элементов. Поскольку природа его элементов для нас несущественна, будем предполагать, что $A = \{1, 2, \ldots, n\}$.

Всякая *биекция*, то есть взаимно однозначное отображение множества A *на себя* называется *подстановкой* на A (иногда употребляют термин перестановка). Будем обозначать подстановку строчными латинскими буквами, имеем $f : i \to f(i),\ i = 1,\ldots,n$.

Подстановку f можно задавать различными способами.

- В виде двустрочной таблицы:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix},$$

где в каждом столбце элемент первой строки подстановкой переводится в элемент второй строки. Например, в подстановке $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ элемент *1* переходит в *2*, *2* – в *4* и т. д. Подстановки, отличающие порядком следования столбцов, не считаются различными. Например, нашу подстановку мы могли бы записать в виде: $f = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

- Второй строкой: $f = [3412]$, в этом случае имеется в виду, что первая строка в подстановке записана в порядке возрастания элементов
- Произведением циклов: $f = (13)(24)$. Мы рассмотрим этот вопрос позднее.
- В виде орграфа, если элемент i переходит в элемент j, то дуга имеет направление от вершины i к вершине j.

Тождественной подстановкой называется подстановка, переводящая каждый элемент в самого себя: $e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$.

На множестве подстановок определена бинарная операция *композиции (умножение)* подстановок. Композицией подстановок называется их последовательное применение, сначала правого сомножителя, затем левого:

$(fg)(i) = f(g(i))$.

Введем подстановку $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$. Найдем композицию fg и gf.

Имеем:

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \text{ и } gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

Еще раз напомним, что композиция выполняется *справа налево*: в композиции подстановок fg сначала выполняется подстановка, записанная справа (g), затем слева (f).

Поясним полученный результат. Как мы уже говорили, при композиции fg сначала выполняем подстановку g: *1* переводится в *4*, затем для *4* выполняем подстановку f: переводим *4* в *2*, и так для всех остальных элементов. Получаем: $2 \to 2 \to 4;\ 3 \to 1 \to 3;\ 4 \to 3 \to 1$.

Очевидно, $fe = ef = f$.

Как видим, операция композиции подстановок, в общем случае, *не обладает свойством коммутативности*: $fg \neq gf$.

Композиция подстановок *ассоциативна*, т. е. справедливо равенство:

$(fg)h = f(gh)$.

Каждая подстановка f из n элементов имеет обратную подстановку f^{-1}. Чтобы получить обратную подстановку, необходимо поменять строки местами, а затем столбцы упорядочить по возрастанию элементов первой строки. Для наших подстановок, соответственно, имеем обратные подстановки: $f^{-1} = f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ и $g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$.

Очевидно, что $f^{-1}f = ff^{-1} = e$ и $g^{-1}g = gg^{-1} = e$.

Как видим, для множества подстановок из n элементов и операции композиции выполняются все аксиомы группы.

Множество подстановок из n элементов относительно введенной операции композиции образует группу. Эта группа называется *симметрической группой n-й степени*, и её обозначают S_n. Так как число перестановок из n элементов равно $n!$, то порядок группы S_n равен $n!$

При $n=3$, имеем 6 элементов в группе S_3.

Рассмотрим подгруппу группы S_3:

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Таблица Кэли имеет вид:

*	e	f_1	f_2
e	e	f_1	f_2
f_1	f_1	f_2	e
f_2	f_2	e	f_1

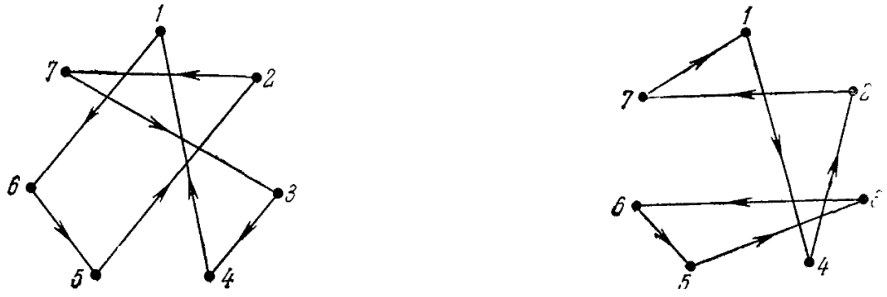
Сравним данную таблицу *Кэли* с таблицей для группы вращений правильного треугольника. Как видим, таблицы *Кэли* для обеих групп идентичны, если провести взаимно однозначное соответствие между элементами групп: $e \leftrightarrow e$. $\varphi_1 \leftrightarrow f_1$, $\varphi_2 \leftrightarrow f_2$. Такие группы, как мы рассмотрим позднее, являются *изоморфными*.

Пусть f – некоторая подстановка на множестве A и пусть B – некоторое подмножество A: $B \subseteq A$. Если мы проходим, следуя подстановке f, все элементы множества B, начиная с некоторого элемента $a_i \in B$, и опять возвращаемся в него, то получаем подстановку, называемую *циклом*.

Цикл записывается в круглых скобках, в виде последовательности элементов, согласно их обходу. В записи считается, что первый элемент переходит во второй, второй в третий и т. д., и последний переходит в первый. *Длиной цикла* называется количество элементов в нем.

Например, на *рисунке 1* изображены подстановки f и g из *7* элементов, записанные в виде циклов *f = (1652734), g = (1427)(365)*. Подстановка f записана

в виде цикла длины *7*, подстановка g – в виде двух циклов длины *4* и *3*, соответственно. Обычно цикл записывают, начиная с наименьшего элемента в нем (или элемента с наименьшим индексом). Так как это цикл, то, очевидно, *(365) = (536) = (653)*.



а) f *б) g*

Рисунок 1

Если биекция подмножества $B \subseteq A$ на себя представляет собой цикл, а остальные элементы множества *A* отображаются сами на себя без перестановок, то такую подстановку мы тоже будем записывать циклами, предполагая, что каждый из таких элементов образует цикл длины *1*. Например, подстановка $t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 5 & 6 & 4 & 1 \end{pmatrix}$ запишется в виде: $t = (456)(17)(2)(3)$. Элементы *2, 3* переходят сами в себя. Имеем один *3*-цикл, *(456)* , один *2*-цикл, *(17)* и два *1*-цикла, *(2), (3)*. Орграф подстановки представлен на *рисунке 2*:

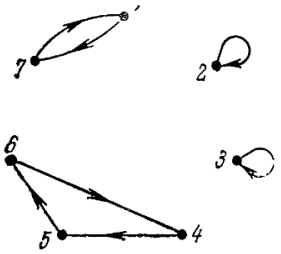


Рисунок 2

Иногда циклы длины *1* не указывают в записи подстановок, в этом случае мы обязательно должны указывать число элементов в подстановке. Если подстановка содержит в себе несколько циклов, то ее можно представить как композицию подстановок, *содержащих по одному из этих циклов.* Например, пусть дана подстановка $t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix} = (134)(56)(2)$.

Ее можно представить как композицию двух подстановок $r = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{pmatrix} = (134)$ и $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix} = (56)$, содержащих ровно по одному циклу, длиной $n \geq 2$: $t = rs$. Циклы в данных подстановках *r* и *s*, как мы видим, содержат *непересекающиеся* подмножества (такие циклы называются *независимыми*) и, следовательно, $t = rs = sr$.

Справедлива следующая теорема.

Теорема 4. Каждая подстановка $f \neq e$ является композицией *независимых циклов* длиной больше или равных *2*. Это разложение в произведение определено *однозначно* с точностью до порядка следования циклов.

Транспозицией называется подстановка, переставляющая между собой два элемента, не меняя остальных, т. е. транспозиция – цикл длиною *2*. Например, подстановка, приведенная ниже, является транспозицией.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = (25)(1)(3)(4) = (25).$$

Имеет место следующая теорема.

Теорема 5. Каждая подстановка, $f \neq e$, раскладывается в произведение транспозиций.

Разложение подстановки в произведение транспозиций *неоднозначно*.

Произведение транспозиций в общем случае *некоммутативно*.

Согласно *теореме 4* любая подстановка раскладывается в произведение независимых циклов. Любой цикл раскладывается в произведение транспозиций по следующему правилу:

$$(i_1 i_2 ... i_k) = (i_1 i_k)(i_1 i_{k-1})...(i_1 i_3)(i_1 i_2).$$

Рассмотрим пример. Пусть дана подстановка $s = \begin{pmatrix} a & b & c & d & e \\ b & c & d & e & a \end{pmatrix} = (abcde)$. Согласно приведенному выше правилу разложим ее в произведение транспозиций.

Имеем: $s = (abcde) = (ae)(ad)(ac)(ab) = t_4 t_3 t_2 t_1$.

Проиллюстрируем полученный результат графически – *рисунок 3*.

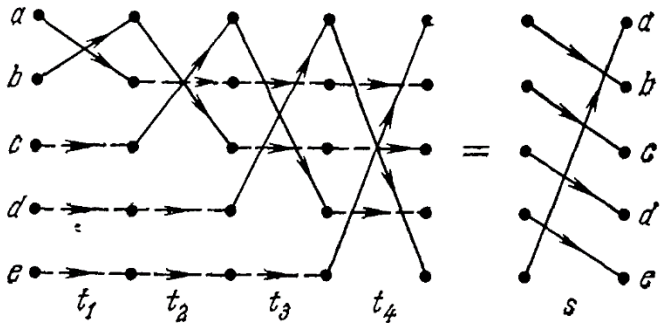


Рисунок 3

Поясним полученный результат. Первой применяем транспозицию t_1: *a* переходит в *b*, элемент *b* переходит в *a*, остальные элементы остаются на своих местах. Затем к полученной подстановке применяем композицию с транспозицией t_2, в результате выполнения композиции двух транспозиций элемент *a* перейдет в элемент *b*, элемент *b* перейдет в элемент *c*, элемент *c* перейдет в элемент *a*, элементы *d* и *e* останутся на своих местах. И так далее. В результате последовательного выполнения операций композиции с ттранспозициями , указанными справа, мы получим исходную подстановку *s*.

Рассмотрим еще пример. Разложим подстановку *f* в произведение транспозиций.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324) = (14)(12)(13).$$

Степенью подстановки называется композиция подстановки на саму себя соответствующее количество раз. Например: $f^2 = f \cdot f$; $f^3 = f^2 \cdot f$;...; $f^p = f^{p-1} \cdot f$.

Очевидно, что $f^p \cdot f^q = f^q \cdot f^p$.

Пусть дана подстановка $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324)$. Найдем ее квадрат: $f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$.

Порядком подстановки $f \in S_n$ называется наименьшее натуральное число p такое, что $f^p = e$. Очевидно, что порядок подстановки равен порядку циклической группы $\{f,\ f^2,..., f^p = e\}$, являющейся подгруппой S_n. *Порядок подстановки равен наименьшему общему кратному длин независимых циклов, входящих в разложение f.*

Рассмотрим пример. Пусть дана подстановка $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (132)(4)$, найдем ее порядок. Имеем: $f^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$ и *НОК* длин независимых циклов также равен *3*, порядок подстановки *f* равен *3*.

Подстановка *f* называется *четной (нечетной)*, если ее разложение в произведение транспозиций содержит *четное (нечетное)* количество сомножителей.

Например, подстановка $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324) = (14)(12)(13)$ является нечетной, а $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (132)(4) = (12)(13)$ – четной.

Всякая транспозиция является *нечетной* подстановкой.

Четность подстановки можно определить и по количеству *инверсий*.

Рассмотрим подстановку $f = [a_1 a_2 ... a_n]$. Пару $(a_i a_j)$, $i < j$ будем называть *инверсией* подстановки f, если $a_i > a_j$. Например, в подстановке $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324)$ пары (3,1), (3,2), (4,2), (4,1), (2,1) – инверсии (мы рассматриваем вторую строку подстановки).

Подстановка называется *четной*, если число инверсий *четно*, и *нечетной*, если число инверсий *нечетно*.

Для подсчета числа инверсий в подстановке необходимо подсчитать для каждого элемента подстановки, сколько элементов больше него стоит перед ним (или сколько элементов меньше него стоит за ним) и суммировать по всем элементам полученные резудьтаты.

Подсчитаем число инверсий для наших подстановок f и g, будем считать для каждого элемента сколько элементов меньше него стоит за ним .

Для подстановки $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324)$ имеем: для *3 – 2* элемента, для *4 – 2* элемента, для *2 -1* элемент, общее число инверсий *– 5*, подстановка нечетная.

Для подстановки $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (132)(4)$ имеем: для *3 – 2* элемента, для *1, 2, 4* – ноль элементов, общее число инверсий – *2*, подстановка четная.

Типом подстановки $f \in S_n$ называется вектор $\lambda(f) = (\lambda_1(f),...,\lambda_i(f),...,\lambda_n(f))$, где $\lambda_i(f)$ – число циклов длины i в подстановке f. Для любой подстановки $f \in S_n$ выполняется соотношение:

$$\sum_{i=1}^{n} i \cdot \lambda_i(f) = n \ .$$

Таким образом, каждый элемент принадлежит ровно одному циклу. Для подстановки $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (132)(4)$, тип перестановки равен: $\lambda(g) = (1,0,1,0)$.

Для подстановки $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$, соответственно, $\lambda(f) = (0,2,0,0)$.

ТЕМА №3. ***СМЕЖНЫЕ КЛАССЫ ПО ПОДГРУППЕ***

Рассмотрим понятие смежных классов по подгруппе.

Пусть H – *собственная* подгруппа группы $(G,*)$.

Пусть $a \in G$. Через aH обозначим множество элементов $aH = \{a*h \mid h \in H\}$ и назовем его *левым смежным классом* группы G по подгруппе H, порожденным элементом a. Здесь h – любой элемент подгруппы H, a – фиксированный элемент группы G.

Очевидно, элемент a принадлежит смежному классу aH, поскольку подгруппа H содержит нейтральный элемент e и $a*e = a$. Всякий левый смежный класс порождается любым из своих элементов, т. е. если $b \in aH$, то $bH = aH$.

Если существует $b \in G$, $b \notin H \cup aH$, можно построить новый левый смежный класс bH и так далее. Аналогично строят *правый смежный класс*: это множество Ha, т. е. множество всех элементов вида $h*a$, где h – любой элемент из H, a – фиксированный элемент G.

$Ha = \{h*a \mid h \in H\}$.

Очевидно, что сама подгруппа H является одним из левых (правых) смежных классов, этот класс порождается элементом e (или любым элементом $h \in H$, поскольку $h*H = H$).

Если каждый левый смежный класс и правый, порожденные соответствующим элементом a, совпадают: $aH = Ha$, то тогда смежные классы называют *двусторонними*. Такими являются смежные классы в любой *абелевой* группе G. В этом случае говорят просто о разложении группы по подгруппе.

Смежные классы обладают рядом важных свойств.

Пусть H – собственная подгруппа группы G. Тогда:

1) каждый элемент $a \in G$ принадлежит какому-нибудь левому смежному классу по подгруппе H;

2) два элемента $a,b \in G$ принадлежат одному левому смежному классу тогда и только тогда, когда $a^{-1}*b \in H$;

3) любые два левых смежных класса либо не пересекаются, либо совпадают;

4) для всякого $a \in G$ мощности множеств aH и H совпадают;

5) G есть объединение попарно непересекающихся левых смежных классов по подгруппе H.

Приведенные утверждения справедливы и для правых смежных классов.

Рассмотрим пример.

Пример 1.

Пусть $G = (Z,+)$ – аддитивная абелева группа целых чисел, а $H = (3Z,+)$ – ее подгруппа, состоящая из всех чисел, кратных 3. Разложим G на смежные классы по подгруппе H. Имеем:

$H = \{\ldots,-6, -3, 0, 3, 6,\ldots\};$

$1H = 1 + H = \{\ldots,-5, -2, 1, 4, 7,\ldots\};$

$2H = 2 + H = \{\ldots,-4, -1, 2, 5, 8,\ldots\}.$

Итак, получили 3 различных смежных класса, *считая одним из классов и подгруппу H*. Взяв любое другое число в качестве элемента a, например 4, мы

попадаем в один из указанных классов. Получаем, наши смежные классы порождены соответственно числами *0, 1, 2*. В один класс попадают числа, дающие при делении на *3* одинаковый остаток.

Для фиксированной подгруппы H группы G левые (правые) смежные классы образуют разбиение G.

Рассмотрим еще пример.

Пример 2.

Пусть задано множество *A = {0, 1, 2, 3 ,4, 5 ,6, 7}*. Рассмотрим группу $G = (A, \oplus_{\mathrm{mod}8})$ и ее подгруппу $H = (B, \oplus_{\mathrm{mod}8})$, где *B = {0, 4}*. Здесь групповая операция – *сложение по модулю 8*. Разложим *G* по подгруппе *H*. Имеем:

$H = \{0,4\}$;

$1H = 1 \oplus_8 H = \{1,5\}$;

$2H = 2 \oplus_8 H = \{2,6\}$;

$3H = 3 \oplus_8 H = \{3,7\}$;

$1H = 5H$, $2H = 6H$, $3H = 7H$.

Как видим, группа *G* представляет собой объединение *4* смежных классов.

Для нашего примера порядок подгруппы *H* равен *2*, порядок группы *G* равен *8*. Как видим, порядок подгруппы *H* является делителем порядка группы *G*. Приходим к важной теореме.

Теорема Лагранжа.

Порядок конечной группы делится на порядок любой ее подгруппы.

Пусть *G* – конечная группа порядка *n*, *H* – ее подгруппа порядка *m*. Разложим группу *G* на левые смежные классы по подгруппе *H*. Пусть *k* – число полученных классов. Каждый левый смежный класс *aH* состоит ровно из *m* элементов. Действительно, если $a*h_1 = a*h_2$, то $h_1 = h_2$. Следовательно, общее число элементов группы *n = km*. Это означает, что *n* делится на *m*. Число *k*, равное мощности множества всех левых смежных классов группы *G* по данной подгруппе *H*, называется *индексом подгруппы H в группе G*. Для нашего примера *k = 4*.

Из теоремы *Лагранжа* следует, что:

1. Порядок любого элемента конечной группы будет делителем порядка группы.

2. Всякая конечная группа, порядок которой есть простое число, является циклической и не содержит собственных подгрупп.

Дадим определение *нормальной* подгруппы.

Собственная подгруппа *H* группы *G* называется *нормальной*, если для всякого $a \in G$, $aH = Ha$, то есть каждые левый смежный класс и правый смежный класс по подгруппе *H* , порожденные одним и тем же элементом *a*, совпадают.

Очевидно, являются верными следующие *2* утверждения:

1. У абелевых групп все подгруппы нормальные.

2. Всякая подгруппа индекса *2* является нормальной.

Справедлива также следующая *теорема*:

Подгруппа H группы G является нормальной тогда и только тогда, когда для каждого $a \in G$ *выполняется* $aHa^{-1} = H$.

Пусть *(G,∗)* − группа и *H* − ее *нормальная* подгруппа. *Фактор-множеством* группы *G* по подгруппе *H* называется множество всех левых, или что то же самое, правых смежных классов по подгруппе *H* и обозначается через *G/H* = *= {H, aH, bH,…}*.

Пусть *H* − нормальная подгруппа. Тогда фактор-множество *G/H* является группой относительно *индуцированной операции*, определяемой по следующему правилу:

$aH \bullet bH = (a*b)H$, $a,b \in G$.

Для множества *G/H* и определенной таким образом индуцированной операции $\bullet$ выполняются все аксиомы группы.

1. Операция $\bullet$ замкнута на *G/H*, поскольку $(a*b) \in G$ и, следовательно, $(a*b)H \in G/H$.

2. Операция $\bullet$ ассоциативна по причине ассоциативности операции * в самой группе *G*.

3. Единицей относительно индуцированной операции является, очевидно, группа *H*:

$aH \bullet H = aH \bullet eH = (a*e)H = aH$;

$H \bullet aH = eH \bullet aH = (e*a)H = aH$.

4. Обратным к данному классу *aH* является класс смежности $a^{-1}H$:

$aH \bullet a^{-1}H = (a*a^{-1})H = eH = H$;

$a^{-1}H \bullet aH = (a^{-1}*a)H = eH = H$.

Эта группа называется *фактор-группой* группы *G* по нормальной подгруппе *H*.

Отметим, что фактор-группа абелевой групы является абелевой.

Фактор-группа циклической группы является циклической.

Рассмотрим предыдущий *пример 2*.

Отметим, что наша группа *G* является циклической и абелевой.

Фактор-множество *G/H* состоит из *4* смежных классов: *G/H = {H, 1H, 2H, 3H}*. Построим таблицу *Кэли* для фактор-группы *G/H*.

$\bullet$	*H*	*1H*	*2H*	*3H*
H	*H*	*1H*	*2H*	*3H*
1H	*1H*	*2H*	*3H*	*H*
2H	*2H*	*3H*	*H*	*1H*
3H	*3H*	*H*	*1H*	*2H*

Поясним полученный результат.

$3H \bullet 2H = (2 \oplus_8 3)H = 5H = 1H$.

$3H \bullet 3H = (3 \oplus_8 3)H = 6H = 2H$.

Наша фактор-группа является циклической, порожденной смежными классами: *<1H> = G/H* и *<3H> = G/H*.

Она также является абелевой, что видно из таблицы *Кэли*.

ЛИТЕРАТУРА

1. Андерсон, Д. Дискретная математика и комбинаторика. – СПб: Вильямс, 2003. – 960 с.

2. Биркгоф, Г. Современная прикладная алгебра / Г.Биркгоф, Т. Барти. –2-е изд., стер. – СПб. Лань, 2005. – 400 с.

3. Кофман, А. Введение в прикладную комбинаторику – М.: Наука, 1975. – 480 с.

4. Каргополов, М.И. Основы теории групп / М.И. Каргополов, Ю.И. Мерзляков. – М.: Наука, 1972. – 240 с.

5. Кострикин, А.И. Введение в алгебру: Часть 1. Основы алгебры: учебник для вузов. – 3-е изд. – М.: ФИЗМАТЛИТ, 2004. – 272 с.

6. Лиддл, Р. Конечные поля / Р. Лиддл, Г. Ниддеррайтер. – М: Мир, 1988. – 882 с.

7. Ленг, С. Алгебра. – М: Мир, 1968. – 564 с.

8. Липницкий, В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учеб.-метод. пособие – 2-е изд., испр. – Мн.: БГУИР, 2006. – 88 с.

УЧЕБНОЕ ИЗДАНИЕ

Составители:
Глущенко Татьяна Александровна
Хацкевич Мария Викторовна
Кот Александр Александрович

Введение в алгебраические системы. Группы.

Методические указания к изучению курса
«***Дискретная математика***»

для студентов специальностей:
1-53 01 02 «Автоматизированные системы обработки информации»,
1-40 03 01 «Искусственный интеллект»
и 1-40 01 01 «Программное обеспечение информационных технологий»

Ответственный за выпуск: Глущенко Т.А.
Редактор: Боровикова Е.А.
Компьютерная вёрстка: Соколюк А.П.
Корректор: Никитчик Е.В.

Подписано в печать 22.01.2020 г. Формат 60x84 $^{1}/_{16}$. Бумага «Performer».
Гарнитура «Times New Roman». Усл. печ. л. 1,16. Уч. изд. л. 1,25. Заказ № 1740. Тираж 22 экз.
Отпечатано на ризографе учреждения образования «Брестский государственный технический университет». 224017, г. Брест, ул. Московская, 267.