САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**КАФЕДРА ВЫСШЕЙ МАТЕМАТИКИ**

**Рябова Марина Анатольевна**

**Выпускная квалификационная работа бакалавра**

**Автоморфизмы подстановок и графы**

Направление 010400

Прикладная математика, фундаментальная информатика

и основы программирования

Научный руководитель,

кандидат физ.-мат.

наук, доцент

Калинина Е. А.

Санкт-Петербург

2016

Содержание

[Введение 3](#_Toc450048141)

[Постановка задачи 4](#_Toc450048142)

[Обзор литературы 5](#_Toc450048143)

[Глава 1. Общие сведения о подстановках 6](#_Toc450048144)

[1.1. Понятие подстановки 6](#_Toc450048145)

[1.2. Произведение подстановок 6](#_Toc450048146)

[1.3. Симметрическая группа степени $n$ 7](#_Toc450048147)

[1.4. Циклы и циклическая группа 9](#_Toc450048148)

[Глава 2. Автоморфизмы подстановок 15](#_Toc450048149)

[2.1. Классы сопряженных элементов 15](#_Toc450048150)

[2.2. Автоморфизмы группы 15](#_Toc450048151)

[2.3. Разложение симметрической группы на классы сопряженности 20](#_Toc450048152)

[2.4. Нахождение группы автоморфизмов симметрической группы 22](#_Toc450048153)

[Глава 3. Применение автоморфизмов подстановок к теории графов 26](#_Toc450048154)

[3.1. Основные понятия о графах 26](#_Toc450048155)

[3.2. Автоморфизмы графов 27](#_Toc450048156)

[3.3. Связь симметрической группы и автоморфизмов графов 28](#_Toc450048157)

[Заключение 33](#_Toc450048158)

[Список литературы 34](#_Toc450048159)

# Введение

Понятие подстановки, которое является одним из центральных в данной работе, возникло еще в веке. Тогда выдающиеся математики Вандермонд и Лагранж, занимаясь изучением полиномиальных уравнений, рассмотрели композицию подстановок и установили, что они обладают свойствами групповых объектов[1, с. 349]. Поэтому можно считать, что именно с подстановок зародилась теория конечных групп.

При исследовании теории групп подстановок естественным образом может возникнуть вопрос о существовании таких отображений группы подстановок, или симметрической группы, на себя, при которых сохраняются соотношения между элементами группы. Как будет показано в настоящей работе, все такие отображения образуют группу относительно операции умножения и несут название автоморфизмов группы подстановок. Одним из примечательных свойств автоморфизмов является то, что они определяют внутреннюю структуру объектов, разбивая их на множества элементов со схожими особенностями и характеристиками.

Выделив основные принципы теории подстановок, применим их к теории графов. Если говорить точнее, то мы можем установить связь между свойствами группы автоморфизмов подстановок на множестве вершин некоторого графа и автоморфизмами этого графа.

# Постановка задачи

Наша задача заключается в исследовании различных групп подстановок и нахождении их групп автоморфизмов. Целью работы является распространение полученных результатов для теории подстановок на автоморфизмы графов.

 В первой главе мы введем основные понятия и утверждения, связанные с подстановками. Особое внимание уделим разложению подстановок в произведение циклов.

Во второй главе определим разделение группы на классы сопряженных элементов и перейдем к поиску автоморфизмов симметрической группы.

Третья глава является результатом исследований свойств автоморфизмов подстановок и их применений к теории автоморфизмов графов.

# Обзор литературы

Всю литературу, используемую при написании данной работы, можно разделить на четыре части. В первой из них содержатся литературные источники, раскрывающие такие понятия как подстановка, умножение подстановок, симметрическая группа, циклы. Это книги Постникова М. М., Головиной Л. И. и работа под редакцией Александрова А. Д., Колмогорова А. Н., Лаврентьева М. А. К ним можно добавить книги Гроссмана И. и Магнуса В. «Группы и их графы», Винберга Э. Б. «Курс алгебры», в которых рассматриваются понятия группы и циклической группы.

Вторая часть включает литературу по автоморфизмам групп. Авторами литературных источников являются Ван дер Варден , Курош А. Г., Каргаполов М. И. и Мерзляков Ю. И.

При подсчете количества всех автоморфизмов симметрической группы использовалась литература по теории вероятностей: «Введение в прикладную комбинаторику» Кофмана А., «Теория вероятностей и математическая статистика» Буре В. М. и Парилиной Е. М.

Последняя часть литературы связана с основными понятиями теории графов. К ней относятся книги «Теория графов» Харари Ф., «Перечисление графов» Харари Ф. и Палмера Э., «Лекции по теории графов» Емеличева В. А., Мельникова О. И., Сарванова В. И. и Тышкевича Р. И.

# Глава 1. Общие сведения о подстановках

## 1.1. Понятие подстановки

Подстановкой называется взаимно однозначное отображение конечного множества на себя [2, с. 87]. Далее под конечным множеством мы будем подразумевать множество с натуральными числами и записывать подстановки в следующем виде:

, (1)

где вторая строка является перестановкой множества  и состоит из различных чисел. При этом из (1) следует, что ,  и так далее[[1]](#footnote-1).

Переставляя некоторые столбцы в подстановке, мы не меняем ее смысла.

Под степенью подстановки будем понимать мощность множества, на котором она задана. В нашем случае степень подстановки будет равняться .

Если наше множество$ E $имеет  элементов, то количество различных подстановок на данном множестве, очевидно, равняется $.$ Действительно,  может перейти в  различных чисел, тогда  – в  число, 3 – в  числа и так далее. Имеем  различных перестановок второй строки.

## 1.2. Произведение подстановок

Произведением двух подстановок назовем последовательное выполнение двух подстановок одинаковой степени , результатом которого является некая подстановка тоже  степени [3, с. 281]. Стоит отметить, что умножение подстановок не всегда является коммутативным[[2]](#footnote-2).

*Пример.* Перемножим подстановки

 и .

Получаем

, . (2)

Из (2) можно заметить, что подстановки  в данном случае не коммутируют.

Произведение подстановок ассоциативно. Действительно, пусть нам даны три подстановки , каждая из них имеет степень , и пусть для чисел [[3]](#footnote-3) определено следующее:  при ,  при ,  при . Тогда нетрудно убедиться, что как при , так и при  . Следовательно, .

## 1.3. Симметрическая группа степени $n$

На протяжении всей работы мы будем не раз прибегать к понятию группы. Для того чтобы его ввести, нам необходимо знать, что собой представляет бинарная операция на множестве. Бинарная операция[[4]](#footnote-4) на множестве – это соответствие, при котором каждой упорядоченной паре элементов данного множества отвечает однозначно определенный элемент этого же множества [, с. 11]. Тогда множество  будет являться группой, если на нем определена бинарная операция и его элементы удовлетворяют следующим трем аксиомам:

1. Ассоциативности. Пусть [[5]](#footnote-5).
2. Существование единичного элемента. Существует единственный элемент такой, что .
3. Существование обратного элемента. Для  такой, что .

Если бинарная операция задается умножением[[6]](#footnote-6), то такую группу назовем мультипликативной.

Пусть нам заданы подстановки на множестве . Обозначим множество всех таких подстановок через  и назовем симметрической группой степени  [3, с. 280]. Покажем, что  – мультипликативная группа. Действительно, имеем:

1. Как было показано в параграфе 1.2, мы можем определить операцию умножения на множестве , которая является ассоциативной и ставит в соответствие двум подстановкам  их произведение ;
2. Среди всех подстановок множества  выделим единичную подстановку



и произвольную подстановку

,

тогда очевидно, что

;

1. Обратной к подстановке  назовем подстановку , которая удовлетворяет равенству

,

и очевидно, что .

## 1.4. Циклы и циклическая группа

Подстановку вида



будем называть циклом длины $m$, при этом все элементы  различны [5, с. 263]. Очевидно, что существует  различных записей одного и того же цикла длины . Например,

.

Циклы, не содержащие общих элементов, являются независимыми. Не имеет разницы, в каком порядке перемножаются независимые циклы. Действительно, пусть подстановки и  – независимые между собой циклы. Тогда



Цикл длины один переводит число само в себя.

*Пример*. В некоторой подстановке



есть два единичных цикла .

Назовем транспозицией цикл длины два. Цикл, длина которого , мы можем разложить в произведение  транспозиции:



Далее, введем понятие циклической группы. Циклическая группа – группа, порожденная степенями одного элемента [6, с. 160]:

 (3)

В таком случае будем говорить, что порождает циклическую группу. Очевидно, что на ней задана бинарная ассоциативная операция умножения, существует единственный единичный элемент , а каждому элементу  ставится в соответствие обратный ему . Элементы такой группы могут повторяться (имеются равные). Пусть , тогда

. (4)

Порядок элемента  – наименьшая натуральная степень, удовлетворяющая (4) [4, с. 60]. Пусть порядок равен . При этом все элементы

 (5)

различны. Если найдутся одинаковые, то разность их показателей меньше, чем , а это противоречит определению порядка группы. Любой элемент  из (3) совпадает с каким-либо элементом из совокупности элементов (5), в частности , остаток от деления . Получаем, что порядок группы равен порядку порождающего элемента.

Перейдем к подстановкам. Допустим, что некоторая подстановка  вида (1) из симметрической группы  порождает циклическую группу порядка , то есть элементы группы есть различные подстановки

.

Пусть подстановка  перемещает некоторое число , то есть . Обозначим через  число, которое получается из  в результате подстановки . При этом , так как, применяя подстановку  к , получаем числа , а . Следовательно, получаем перемещаемые подстановкой  числа

.

Очевидно, этих чисел не может быть больше , так как . Если  исчерпывается набором чисел , то можем определить эту подстановку как цикл длины , иначе можем выделить в данной подстановке цикл  длины .

*Пример.* Пусть произвольная подстановка  задана на множестве :

.

Порождаемая ею циклическая группа



Как видим, порядок группы равен шести. Возьмем, к примеру, число 3. Оно является перемещаемым и

.

Можем выделить цикл , длина которого равняется трем. Однако,  не исчерпывается данным набором чисел, в подстановке также имеет место цикл  длины 2.

*Утверждение 1.* Любая неединичная подстановка  раскладывается единственным способом в произведение независимых циклов [2, с. 96].

*Доказательство.* Будем проводить доказательство утверждения методом математической индукции по числу  перемещаемых подстановкой  чисел. Число  не может равняться 1, так как два числа при подстановке не могут переходить в одно. Поэтому за базу индукции возьмем , тогда, очевидно,  раскладывается в произведение транспозиции и циклов единичной длины из неперемещаемых элементов.

Пусть утверждение доказано для подстановок, перемещающих меньше  чисел. Докажем его для подстановки , перемещающей  чисел. Предположим, что  перемещает какое-то число , и применим к этому числу подстановки  таким же способом, как было показано выше. В итоге мы получим перемещаемые подстановкой  числа

 (6)

Допустим, что среди (6)  является первым числом, которое удовлетворяет уравнению , при этом все числа  различны. Тогда мы можем выделить в подстановке  цикл . Следовательно,

,

где

.

В свою очередь,  перемещает не более , а для такой подстановки выше было предположено, что она раскладывается единственным образом в произведение независимых циклов. Следовательно, подстановка  тоже имеет единственное разложение по циклам. При этом циклы в разложении  независимы, так как



Утверждение доказано.

#

# Глава 2. Автоморфизмы подстановок

## 2.1. Классы сопряженных элементов

Рассмотрим некоторую мультипликативную группу  и какой-либо ее элемент . Пусть , тогда назовем всякий элемент сопряженным с элементом  [, с. 297]. Будем обозначать сопряженность двух элементов как .

Свойства отношения сопряженности:

1. Рефлексивность.





1. Симметричность.



1. Транзитивность.



Из вышеизложенных свойств видим, что отношение сопряженности является отношением эквивалентности, поэтому определяет разбиение группы на непересекающиеся классы сопряженных между собой элементов [, с. 289].

## 2.2. Автоморфизмы группы

Для того чтобы задать определение автоморфизмов группы, нам необходимо рассмотреть понятие изоморфизма двух множеств. Установим между элементами двух произвольных множеств  и  взаимно однозначное соответствие, то есть элементу соответствует элемент и так далее. При этом заметим, что соотношения между элементами одного множества сохраняются и для другого множества. Такое соответствие двух множеств назовем изоморфизмом [7, с. 42].

Положим, что элементу  группы  взаимно однозначно соответствует элемент  группы ,  [[7]](#footnote-7), а элементу  – , . При изоморфизме двух групп произведение элементов одной группы сопоставим произведению элементов другой группы, поэтому . Аналогично, если  изоморфизм, можно записать так:



В частности, если , то такое соответствие элементов назовем автоморфизмом группы [7, с. 43]. Если рассматривать примеры на практике, то мы можем сравнить понятие автоморфизма с симметрией. Действительно, при симметрии некое тело в результате преобразований переходит само в себя, сохраняя соотношения между элементами тела.

Покажем, что множество всех автоморфизмов группы  является группой[[8]](#footnote-8) с определенной на ней бинарной операцией умножения. Будем рассматривать умножение двух автоморфизмов как их последовательное выполнение. Тогда:

1. Пусть  и  – два автоморфизма, заданных на , некоторые элементы принадлежат . Если



из чего следует, что произведение двух автоморфизмов взаимно однозначно отображает группу  на себя и является бинарной операцией на .

1. Пусть  – три автоморфизма, заданных на , некоторые элементы  принадлежат . Если

 ,

то



Доказали ассоциативность автоморфизмов.

1. Допустим, что автоморфизм  ставит в соответствие некоторому элементу из  этот же элемент, то есть является тождественной подстановкой.



Если некоторый автоморфизм  такой, что



то ,  – тождественный автоморфизм.

1. Пусть некоторый автоморфизм  может быть представлен как



Так как автоморфизмы являются взаимно однозначными отображениями, то мы можем однозначно сопоставить каждому элементу  другой элемент из этой же группы , и наоборот, элементам  можем однозначно сопоставить

.

Следовательно, для каждого автоморфизма  найдется единственный обратный ему автоморфизм .

Рассмотрим теперь такое отображение, которое ставит в соответствие некоторому элементу сопряженный ему элемент . К тому же,

.

Делаем вывод, что данное отображение является изоморфизмом группы  на себя, то есть является автоморфизмом. Назовем его внутренним автоморфизмом, а все другие автоморфизмы, если они существуют, назовем внешними [7, с. 43].

Как и было доказано выше, что множество автоморфизмов является группой, так и можно аналогично удостовериться, что множество внутренних автоморфизмов группы  тоже составляет группу[[9]](#footnote-9) относительно операции умножения (последовательного выполнения).

Так как объектом наших исследований является симметрическая группа  и все подстановки степени , которые она включает, то следует применить понятие группы автоморфизмов именно к ней. Как будет показано далее в этом параграфе, в большинстве случаев, имея дело с симметрическими группами, нам не придется сталкиваться с ее множеством внешних автоморфизмов. А внутренние автоморфизмы будут играть важную роль в установлении связи между симметрической группой и автоморфизмами графов.

Итак, установим утверждение, которое поможет нам в дальнейшем не акцентировать внимание на выделении в каждой симметрической группе ее внешних автоморфизмов. Для начала введем следующие необходимые понятия:

1. Если под инвариантными элементами группы понимать такие, которые коммутируют со всеми ее элементами, то центр группы – это множество  всех ее инвариантных элементов [8 ,с. 68].
2. Группа совершенна, если она без центра[[10]](#footnote-10) и все ее автоморфизмы внутренние [9, с. 67].

*Утверждение 1 (Теорема Гёльдера).* При  симметрическая группа  совершенна [9, с. 67].

Из теоремы Гельдера вытекает, что группы  и  не являются совершенными, потому что первая из них представляет собой группу двух коммутативных подстановок



а вторая обладает внешним автоморфизмом [9, с. 69].

Во всех остальных симметрических группах  группа автоморфизмов будет ограничиваться группой внутренних автоморфизмов. Таким образом,  включает в себя все отображения вида



откуда делаем важный вывод, что группы автоморфизмов таких симметрических групп совпадают с самими симметрическими группами.

##

## 2.3. Разложение симметрической группы на классы сопряженности

Условимся, что будем рассматривать далее симметрические группы степени . Из прошлого параграфа мы выяснили, что для нахождения группы автоморфизмов  достаточно обозначить все подстановки, которые входят в . Как будет показано далее, удобнее структурировать симметрическую группу и начать с выделения классов сопряженности в , а затем вести подсчет различных подстановок в каждом классе.

*Утверждение 1.* Чтобы получить из некоторой подстановки , разложенной в произведение циклов, сопряженную ей , нужно сделать подстановку  в каждом цикле в разложении подстановки  [10, с. 263].

*Доказательство.* Положим

 (1)

Последовательно выполним подстановки (1). Получим:



В итоге

,

что и требовалось доказать.

С помощью следующего утверждения мы, наконец, сможем выдвинуть правило, по которому будет происходить разложение симметрической группы  на классы сопряженных элементов, а впоследствии определить количество ее автоморфизмов.

*Утверждение 2.* Для того чтобы две подстановки были сопряжены в симметрической группе , необходимо и достаточно, чтобы существовало их разложение в произведение независимых циклов одинаковых порядков [10, с. 264].

*Доказательство.* Как было показано в утверждении 1, мы имеем разложение двух сопряженных подстановок  и  на соответственно одинаковые по порядку циклы. Необходимость доказана. Докажем теперь достаточность. Как мы знаем, в симметрической группе всегда найдутся такие подстановки, переводящие произвольное количество чисел в любое другое. Тогда, если две подстановки  и  из  раскладываются в произведение независимых циклов одинаковых порядков, то существует такая подстановка , которая переводит подстановку  в , при этом , то есть  и  будут сопряжены в .

Определим правило, по которому будем разбивать симметрическую группу на классы сопряженности. Пусть множество, на котором заданы подстановки, состоит из  чисел. Тогда учтем все разбиения  на слагаемые, обозначающие порядки циклов.

*Пример.* Предположим , тогда

 

Заметим, что не имеет значения, в каком порядке стоят слагаемые в разложении . Действительно, подстановка не меняет смысла при перестановке циклов в ее разложении. В итоге получилось 13 классов.

Произведем подсчет количества классов  в :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
|  | 1 | 2 | 3 | 5 | 7 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 6 | 7 | 8 | 9 | 10 |
|  | 10 | 13 | 17 | 21 | 26 |

## 2.4. Нахождение группы автоморфизмов симметрической группы

Решим задачу нахождения в симметрической группе  группы автоморфизмов. Вначале вычислим количество различных подстановок в каждом классе сопряженных элементов. Допустим, что в некотором классе  разложение подстановок порядка  по  циклам принимает следующий вид:



где  длина первого цикла,  второго цикла и так далее. Воспользуемся основами комбинаторики и посчитаем, сколько различных циклов можно получить из  чисел, а затем с помощью основного правила комбинаторики (правила умножения) вычислим количество различных подстановок в . Согласно урновой схеме, мы производим упорядоченный выбор чисел без возвращения, то есть будем находить число размещений для каждого цикла [, с. 125]. Для первого цикла разместим чисел по  элементам, для второго цикла – уже  по  элементам и так далее до  цикла, где разместим по  элементам. Перемножим размещения по правилу умножения [, с. 16]:

  (2)

Однако мы данный ответ не является верным. Как было указано выше, один и тот же цикл может быть записан несколькими способами. Например,

 

Поэтому число размещений включает в себя повторяющиеся циклы. Очевидно, что цикл длины  может быть записан способами.

Кроме того, мы не учли, что для некоторых номеров  может выполняться



Подразумевается, что если переставить циклы в разложении подстановки, то ее смысл не изменится. Поэтому разобьем циклы по группам в зависимости от их длины, и пусть у нас есть  таких групп. Количество циклов в  группе – .

Сократим формулу (2) и получим количество различных подстановок  в данном классе сопряженных элементов:

  (3)

Остается просуммировать количество подстановок для различных классов и получить конечный ответ.

*Пример.* Пусть дана симметрическая группа , ее степень . Найдем все автоморфизмы этой группы. Всего имеем пять классов сопряженности . Используя формулу (3), посчитаем количество элементов в каждом из них:



Составим итоговую таблицу с подстановками.

|  |  |  |
| --- | --- | --- |
| Класс | Разложение по циклам | Сопряженные элементы в классе |
|  |  |   |
|  |  |   |
|  |  |   |
|  |  |   |
|  |  |   |

Порядок группы, очевидно, равен



# Глава 3. Применение автоморфизмов подстановок к теории графов

## 3.1. Основные понятия о графах

Будем рассматривать простые помеченные графы без петель с неориентированными, невзвешенными, некратными ребрами и конечным множеством вершин.

Обозначим через  граф  с множеством вершин  и множеством ребер .

Если  и  – две вершины в графе , а  – ребро, которое соединяет эти две вершины, то будем говорить, что ребро  инцидентно вершинам  и  [13, с. 9]. При этом две вершины (или два ребра) инцидентными быть не могут.

Степень вершины  в графе  – количество ребер, инцидентных данной вершине [13, с. 26].

Назовем две вершины  и  смежными, если существует ребро , которое их соединяет. В противном случае вершины не являются смежными [13, с. 9].

Пусть граф  имеет  вершин, . Определим матрицу  размера  следующим образом:



тогда  – матрица смежности графа [13, с. 27].

## 3.2. Автоморфизмы графов

Два графа  и  изоморфны, если между их множествами вершин  существует взаимно однозначное соответствие, сохраняющее смежность [14, с.24].

Автоморфизмом графа  назовем изоморфизм графа  на себя. Множество всех автоморфизмов графа  образует группу[[11]](#footnote-11), называемую группой графа [15, с. 14]. Обозначим ее как . Если мы сопоставляем некоторую вершину и ее образ, в который она переходит при автоморфизме графа, то можно рассматривать такое отображение как подстановку на множестве вершин графа , а  как подгруппу симметрической группы подстановок на .

*Пример.* Найдем группу автоморфизмов графа , изображенного на рисунке 1:

1

2

5

4

3

Рис. 1

Его группа может быть представлена двумя подстановками на множестве его вершин:



Стоит заметить, что при автоморфизме степени вершин сохраняются. У первой и второй вершин степень равняется трем, у третьей и пятой – двум, у четвертой – четырем.

## 3.3. Связь симметрической группы и автоморфизмов графов

Обозначим через  единичную матрицу размера , то есть матрицу, у которой на главной диагонали стоят единицы , а все остальные элементы равны нулю. Будем говорить, что матрица  размера  ортогональна, если обратная[[12]](#footnote-12) к ней матрица совпадает с транспонированной[[13]](#footnote-13) к . Другими словами, . Пусть



 (1)

Тогда из уравнения (1) следует, что

 (2)

или, другими словами, сумма квадратов элементов каждой строки матрицы  равна одному, а сумма произведений соответствующих элементов двух строк в матрице  равна нулю. Выполнение формул (2) и являются критерием ортогональности произвольной матрицы.

Представим теперь некоторую подстановку



в матричном виде. Пусть матрица  такая, что

.

Назовем матрицу  (далее будем писать просто ) матрицей подстановки.

*Пример.* Дана следующая подстановка

.

Тогда



Так как один элемент подстановки не может переходить сразу в два других, то в каждой строке матрицы  будет ровно одна единица. Кроме того, два элемента подстановки не могут переходить в один и тот же, поэтому в каждом столбце содержится тоже по одной единице. Нетрудно заметить, что  является ортогональной матрицей, проверив выполнение для нее формул (2). Обратная матрица  к  всегда будет существовать, так как каждая подстановка имеет обратную себе.

Очевидно, что множество всех матриц подстановки  будет представлять группу с операцией умножения матриц, так как является эквивалентным симметрической группе .

Непосредственно умножая слева матрицу подстановки  на матрицу смежности  графа , имеющего  вершин, можно удостовериться, что в результате произведения строки матрицы  переставляются. Если умножать матрицу  на матрицу  справа, то переставляются столбцы. Причем правило перестановки строк и столбцов зависит от подстановки, по которой строилась матрица .

*Пример.* Посмотрим, как влияет подстановка

,

на матрицу смежности графа 

.

Представим  в матричном виде:

.

Умножим  слева и справа на :



Сравнивая результаты, мы убедились, что умножая  слева, на место первой строки перешла третья, на место третьей – вторая, на место второй – четвертая, на место четвертой – первая. Умножая  справа, аналогично поменялись строки в установленном подстановкой  порядке.

Вернемся к автоморфизмам графов. Пусть граф  построен на  вершинах , и ему удовлетворяет некая матрица смежности . Установим, как связаны автоморфизмы подстановок и графы. Так же, как мы поступали с подстановками в параграфе 4.2, зададим отображение  матрицы  в сопряженную ей матрицу , где  - матрица некоторой подстановки :

.

Как и в случае подстановок, данное отображение является внутренним автоморфизмом. Кроме того, из ортогональности  следует, что . Для того, чтобы отображение  было автоморфизмом графа, необходимо равенство матриц , поэтому получаем

.

Как мы знаем из параграфа 4.2, группа автоморфизмов симметрической группы степени  совпадает с ее группой внутренних автоморфизмов, а группа различных матриц  является матричным представлением . Логично предположить из этого, что все матрицы , при которых , будут составлять группу графа .

# Заключение

В ходе работы подробно рассмотрены симметрические группы и их свойства, установлена взаимосвязь между автоморфизмами подстановок и автоморфизмами графов через матрицы подстановок и смежности. Были получены следующие результаты:

1. Симметрическая группа  может быть разложена на классы сопряженных между собой элементов, при этом подстановки из одного класса имеют разложение на циклы одинаковых порядков.
2. Если степень симметрической группы   и отлична от шести, то группа автоморфизмов  совпадает с самой группой .
3. Установлено, что используя матрицу смежности графа , подстановки на множестве вершин графа и представляя эти подстановки в виде матрицы , можно вывести уравнение для нахождения автоморфизмов графа

.

# Список литературы

1. Стиллвелл Д. Математика и ее история. М.-Иж.: Институт компьютерных исследований, 2004. 580 с.
2. Постников М. М. Теория Галуа. М.: Изд. Физ-мат. литературы, 1963. 220 с.
3. Головина Л. И. Линейная алгебра и некоторые ее приложения: Учебное пособие для вузов. Изд. 4-е., испр. М.: Наука, 1985. 392 с.
4. Гроссман И., Магнус В. Группы и их графы / Под ред. В. Е. Тараканова. М.: Мир, 1971. 231 с.
5. Математика, ее содержание, методы и значение. Том 3 / Под ред. А. Д. Александрова, А. Н. Колмогорова, М. А. Лаврентьева. М.: Изд. Академии наук СССР, 1956. 336 с.
6. Винберг Э. Б. Курс алгебры. Изд. 2-е, испр. и доп. М.: Факториал Пресс, 2001. 544 с.
7. Ван дер Варден Б.Л. Алгебра / Под ред. Ю. И. Мерзлякова. М.: Наука, 1979. 623 с.
8. Курош А. Г. Теория групп. Изд. 3-е, доп. М.: Наука, 1967. 648 с.
9. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. Изд. 3-е, перераб. и доп. М.: Наука, 1982. 288 с.
10. Фаддеев с: Учебное пособие для вузов. М.: Наука, 1984. 416 с.
11. Кофман А. Введение в прикладную комбинаторику / Под ред. Б.А. Севастьянова. М.: Наука, 1975. 480 с.
12. Буре В. М., Парилина Е. М. Теория вероятностей и математическая статистика: Учебник. СПб.: Лань, 2013. 416 с.
13. Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. М.: Наука, 1990. 384 с.
14. Харари Ф. Теория графов. Изд. 2-е / Под ред. Г. П. Гаврилова. М.: Едиториал УРСС, 2003. 296 с.
15. Харари Ф., Палмер Э. Перечисление графов. М.: Мир, 1977. 324 с.
1. Здесь и далее **** значит, что число переходит в число . [↑](#footnote-ref-1)
2. Для двух подстановок  и  не всегда выполняется . [↑](#footnote-ref-2)
3. Здесь и далее  – символ принадлежности. [↑](#footnote-ref-3)
4. Обозначим ее как . [↑](#footnote-ref-4)
5. Здесь и далее  – следовательно,  – любой,  – существует. [↑](#footnote-ref-5)
6. Будем обозначать как  или опускать данный символ. [↑](#footnote-ref-6)
7. Здесь и далее  – элементу  взаимно однозначно соответствует элемент . [↑](#footnote-ref-7)
8. Обозначим ее как . [↑](#footnote-ref-8)
9. Обозначим ее как . [↑](#footnote-ref-9)
10. Другими словами, центр состоит из одного элемента. [↑](#footnote-ref-10)
11. Относительно операции композиции автоморфизмов. [↑](#footnote-ref-11)
12. Такая матрица , что . [↑](#footnote-ref-12)
13. Транспонированная матрица  получается из , если поменять местами соответствующие столбцы и строки [↑](#footnote-ref-13)