**1. Алгебраические системы**

**1.1. Множества и отображения**

Среди понятий дискретной математики, пожалуй, базовыми являются понятия множества и отображения. Эти объекты обычно рассматриваются в начале первого семестра в курсе математического анализа. Однако имеет смысл рассмотреть их здесь более подробно.

«Наивное» определение множества заключается в том, что множество – это совокупность объектов произвольной природы. Сами объекты при этом называются элементами данного множества. Такое определение долгое время не встречало никаких возражений. Примерами множеств являются множество всех людей на планете, множество натуральных чисел, множество студентов данной конкретной группы, множество групп на потоке и т.д. Последние два примера показывают, что само множество может служить элементом какого-то другого множества. Если никаких ограничений нет, то можно даже рассматривать множества, которые являются элементами самих себя. Таким, например, должно являться множество всех множеств. Однако в начале этого века в математической печати стали появляться различные парадоксы, связанные с множествами и действиями над ними. Одним из наиболее известных является «парадокс Рассела». Он состоит в следующем.

Если допустимо рассматривать множества произвольной природы и, в частности, такие, которые содержат сами себя в качестве элемента, разобьём все множества на два класса. К первому классу отнесём те множества, которые не содержат сами себя в качестве элемента. Такие множества назовём собственными. К другому классу отнесём множества, которые содержат в качестве элемента сами себя. Их мы назовём несобственными. Далее, рассмотрим множество  всех собственных множеств. К какому классу относится само множество ? Если оно собственное, то должно содержать само себя в качестве элемента, так как по своему определению оно содержит все собственные множества. Но тогда оно будет являться элементом самого себя, что противоречит определению первого класса собственных множеств. Допустим теперь, что множество  несобственное. Но оно содержит только собственные множества, поэтому множество  не является элементом самого себя и, значит, его следует отнести к собственными множествам по определению первого класса. Опять противоречие.

Всё вышесказанное свидетельствует о том, что понятие множества является далеко не таким простым, как это может показаться на первый взгляд. В частности, нельзя произвольно образовывать множества, здесь нужны определённые правила. В дальнейшем такие правила были созданы и соответствующая теория получила название «теории классов». Тем не менее для наших целей «наивного» определения множества будет достаточно. «Несобственных множеств» мы рассматривать не будем.

Сразу отметим, что мы будем использовать следующие общепринятые обозначения для числовых множеств:

 – множество всех натуральных чисел;

 – множество всех целых чисел;

 – множество всех рациональных чисел;

 – множество всех действительных чисел;

 – множество всех комплексных чисел.

Договоримся обозначать множества большими латинскими буквами . Элементы этих множеств будем, как правило, обозначать маленькими латинскими буквами . Тот факт, что  есть элемент множества  будем записывать с помощью следующего обозначения

.

Задать множество означает описать, из каких элементов оно состоит. Если множество состоит из конечного, причём, небольшого числа элементов, то его часто задают «списком». Например, запись  означает, что множество  состоит из трёх элементов 1, 3 и 5. Иногда для задания множества используется запись типа

.

Она означает следующее: запись в фигурной скобке до вертикальной черты указывает, откуда берутся элементы данного множества, а запись после вертикальной черты – какому свойству эти элементы удовлетворяют, т.е., берутся только те элементы, для которых высказывание после вертикальной черты оказывается верным. В данном примере множество  образуют все точки плоскости ( обозначает множество всех точек плоскости), которые удовлетворяют уравнению . Другими словами,  – это окружность единичного радиуса с центром в начале координат. Иногда пишут просто

.

если из контекста ясно, откуда берутся элементы .

**Определение 1.** *Если каждый элемент множества  принадлежит множеству , то будем говорить, что множество  вложено в множество  и обозначать*

*.*

*Если , но , будем говорить, что  – строгое подмножество множества .*

**Определение 2.** *Пусть имеются два множества  и . Их объединением будем называть множество, элементами которого являются все элементы множества  и множества . Объединение множеств  и  обозначается символом .*

**Определение 3.** *Пересечением множеств  и  будем называть множество, элементами которого являются все элементы, принадлежащие  и  одновременно. Пересечение множеств обозначается символом .*

**Определение 4.** *Разностью множеств  и  будем называть множество, состоящее из всех тех элементов множества , которые не принадлежат . разность множеств обозначается символом .*

**Определение 5.** *Множество, в котором нет элементов, будем называть пустым и обозначать символом . Считается, что пустое множество является подмножеством любого множества*.

**Определение 6.** *В случае если множество  конечно, число его элементов будем обозначать символом . В случае, когда множество  бесконечно, будем писать .*

**Определение 7.** *Пусть все рассматриваемые множества содержатся в некотором одном множестве , которое мы будем называть универсальным, и  – одно из них. Тогда множество  будем называть дополнением множества  и обозначать символом .*

Например, если мы рассматриваем множества на плоскости, то роль  будет играть вся плоскость, а множество  будет состоять из всех точек плоскости, не принадлежащих .

**Определение 8.** *Пусть имеются два множества  и . Их декартовыми произведением будем называть множество , элементами которого являются пары , где . Если имеется  множеств , то аналогично можно образовать их декартово произведение*

*.*

*Если множества  и  конечны, то . Аналогично, если множества  конечны, то .*

Например, если множество , а множество , то множество  состоит из 6 элементов: , , , , , .

**Определение 9.** *Пусть имеются два множества  и . Если каждому элементы  поставлен в соответствие какой-то элемент , то говорят, что задано отображение  из множества  в множество . Этот факт обозначается следующим образом*

*.*

*Если элементу  поставлен в соответствие элемент , то  называют образом элемента  и обозначают символом . Элемент  при этом называют прообразом элемента .*

Каждый элемент при отображении  имеет ровно один образ, в то время как элемент множества  может иметь несколько прообразов. Множество прообразов может быть также и пустым.

Задать отображение означает, во-первых, указать множества  и , и, во-вторых, каким-то образом определить элемент  для каждого элемента .

Приведём некоторые примеры отображений.

**Пример 1.** .

Здесь для каждого элемента  элемент  определён формулой. Например, .

**Пример 2.** .

Рис_1_1.wmf

Здесь образ каждого элемента из множества  определён стрелочкой. Например, .

**Пример 3.** .

Рис_1_2.wmf

**Определение 10.** *Отображение  называется взаимно однозначным, если*

*1) образу различных элементов из множества  различны, то есть, если , то и ;*

*2) для любого элемента  найдётся элемент  такой, что .*

Отображение  из примера 2 удовлетворяет условию 1), однако, не удовлетворяет условию 2). Отображение  из примера 3, напротив, удовлетворяет условию 2), но не удовлетворяет условию 1).

Если множества  и  конечны, и существует взаимно однозначное отображение  то отсюда, очевидно, следует, что количество элементов в множествах  и  одно и то же. Для бесконечных множеств, однако, взаимно однозначное отображение  может существовать даже если  – строгое подмножество в . Например,  – множество действительных чисел из отрезка , ,  определено формулой .

**Определение 11.** *Пусть . Отображение , для которого , можно представить следующей таблицей*

*.*

*Взаимно однозначное отображение  будем называть подстановкой.*

**Определение 12.** *Если имеются отображения  и , то можно образовать отображение . При этом полагаем  для всех . Отображение  будем называть суперпозицией отображений  и .*

Как следует из определения, суперпозиция двух отображений всегда действует справа налево, т.е., чтобы найти , нужно сначала к элементу  применить отображение , а потом .

Аналогично, можно рассматривать суперпозицию трёх отображений, и т.д. Нетрудно проверить, что операция суперпозиции отображений удовлетворяет закону ассоциативности, т.е. .

**Определение 13.** *Отображение , для которого  для всех , называется тождественным и обозначается  или .*

**Определение 14.** *Обратным для отображения  называется такое отображение , что  и . Обратное отображение часто обозначают .*

**Пример 4.** Пусть  и

, .

Тогда

, , .

**Определение 15.** *Пусть  – множество точек плоскости. Взаимно однозначное отображение , сохраняющее расстояния между точками называется движением.*

Примерами движений на плоскости являются параллельный перенос, поворот, симметрия относительно некоторой прямой. Можно показать, что любое движение на плоскости можно представить в виде суперпозиции этих преобразований.

**Определение 16.** *Точка  называется неподвижной для движения , если . Движение, для которого все точки являются неподвижными, называется тождественным. В дальнейшем тождественное движение будет обозначаться буквой .*

Можно показать, что движение, имеющее три неподвижных точки не лежащие на одной прямой, является тождественным.

**Задачи.**

Для данных множеств  и  и универсального множества  найдите множества .

1. .

2. , , .

Для подстановок  и  найдите .

3**. .**

4**. .**

5.Докажите, что отображение  является взаимно однозначным тогда и только тогда, когда оно имеет обратное отображение .

6. Найдите, сколько всего существует отображений  в следующих случаях: а) ; б) ; в) 

7. Сколько существует взаимно однозначных отображений  в случаях а), б), в) задачи 6?

8. Пусть . Найдите, сколько всего существует отображений .

9. Пусть . Найдите, сколько существует отображений , удовлетворяющих условию 1) определения 10?

10. Сколько существует взаимно-однозначных отображений , если ?

11. Сколько существует отображений , удовлетворяющих условию 2) определения 10, если ?

12. Сколько существует отображений , удовлетворяющих условию 2) определения 10, если ?

13. Докажите, что если , то число отображений, удовлетворяющих условию 2) определения 10 равно

.

Пусть  и  – указанные ниже подмножества в . Определите, существует ли взаимно однозначное отображение ?

14. .

15. .

16. .

17. .

18. .

19. .

20. .

21. Докажите, что суперпозиция двух движений является движением.

22.Докажите, что параллельный перенос, поворот относительно некоторой точки на некоторый угол и симметрия относительно некоторой прямой являются движениями.

23. Докажите, что если  – это симметрия относительно некоторой прямой, то .

24. Пусть движение  имеет две неподвижные точки  и . Докажите, что тогда вся прямая  является неподвижной для преобразования .

25. Пусть движение  имеет неподвижную прямую  и точку . Докажите, что либо точка  симметрична точке  относительно прямой , либо .

26. Докажите, что если  – движение, имеющее три неподвижные точки, не лежащие на одной прямой, то .

27. Докажите, что если  – движение, имеющее неподвижную прямую  и не являющееся тождественным отображением, то  – симметрия относительно прямой .

28. Докажите, что суперпозиция двух параллельных переносов также является параллельным переносом.

29. Пусть  – симметрия на плоскости относительно прямой , а  – симметрия относительно прямой . Пусть прямые  и  пересекаются и угол между ними равен . Что собой представляют преобразования  в ?

30. Пусть  – симметрия на плоскости относительно прямой , а  – симметрия относительно прямой . Пусть прямые  и  параллельны и расстояние между ними равно . Что собой представляют преобразования  в  в этом случае?

31. Пусть  – это поворот относительно точки  на угол , а   
 – это поворот относительно точки  на угол . Докажите, что суперпозиция  также будет с поворотом на угол . Где будет находиться центр этого поворота?

32. Докажите, что любое движение плоскости можно представить в виду суперпозиции параллельного переноса, поворота и симметрии относительно некоторой прямой.

33. Докажите, что любое движение плоскости можно представить в виде суперпозиции некоторого количества симметрий.

**1.2. Бинарные отношения, их свойства. Отношения   
эквивалентности и порядка**

**Определение 1.** *Бинарным отношением на множестве  называется любое подмножество . Условимся писать , если .*

**Пример 1.** На множестве  рассмотрим отношение порядка

.

**Пример 2.** На множестве натуральных чисел  рассмотрим отношение делимости . Будем считать, что  , если  делится на . Например, .

**Пример 3.** Пусть имеется функция , заданная на . Для  будем считать, что , если . Множество всех  является графиком функции .

**Пример 4.** На множестве  матриц размера  с действительными коэффициентами рассмотрим бинарное отношение :

, если .

**Определение 2.** *Бинарное отношение  на множестве  называется рефлексивным, если каждый элемент множества  состоит сам с собой в бинарном отношении .*

**Определение 3.** *Бинарное отношение  на множестве  называется симметричным, если  тогда и только тогда, когда .*

**Определение 4.** *Бинарное отношение  на множестве  называется антисимметричным, если  и  может быть только в том случае, когда .*

**Определение 5.** *Бинарное отношение  на множестве  называется транзитивным, если всегда, когда  и , пара  также принадлежит .*

**Определение 6.** *Бинарное отношение , обладающее свойствами рефлексивности, симметричности и транзитивности, называется отношением эквивалентности. Для элемента  множество  называется смежным классом отношения , содержащим .*

**Определение 7.** *Бинарное отношение , обладающее свойствами рефлексивности, антисимметричности и транзитивности, называется отношением порядка. Множество с заданным на нём отношением порядка называется частично упорядоченным. Два элемента, состоящие в отношении , называются сравнимыми.*

Отметим, что отношения  являются рефлексивными. Отношение  является рефлексивным только в случае . Отношение  – симметрично, а  – нет. Отношение  симметрично только в том случае, когда . Этому условию удовлетворяет, например, функция



Отношения  – антисимметричны, а  – нет. Отношения  транзитивны. Отношение  является отношением эквивалентности, а  – отношениями порядка.

**Пример 5.** Рассмотрим множество  всех непрерывных функций на отрезке . Будем считать, что . Тогда множество  будет частично упорядоченным.

**Определение 8.** *Частично упорядоченное множество , в котором любые два элемента сравнимы, называется линейно упорядоченным.*

Множество действительных чисел с обычным отношением порядка  является линейно упорядоченным, а множество  из примера 5 – нет.

**Определение 9.** *Разбиением множества  называется любое семейство подмножеств , обладающее двумя свойствами*

1) ;

2) .

**Предложение.** *Пусть  – отношение эквивалентности на множестве . Тогда семейство всех его смежных классов является разбиением множества .*

*Обратно. Для любого разбиения множества  существует единственное отношение эквивалентности  на множестве , для которого каждое из подмножеств разбиения является смежным классом отношения .*

***Доказательство.*** Пусть  – отношение эквивалентности на множестве . Поскольку , то объединение всех смежных классов отношения  даст . Осталось только показать, что любые два смежных класса либо не пересекаются, либо совпадают.

Рассмотрим  и . Допустим, что . Покажем, что . Действительно, пусть  и . Тогда . Таким образом, . Аналогично, , откуда .

Обратно. Пусть имеется разбиение  множества . Определим  следующим образом:  и  принадлежат одному и тому же подмножеству  данного разбиения. Очевидно, отношение  обладает свойствами рефлексивности, симметричности и транзитивности и, значит, является отношением эквивалентности. Единственность отношения  также очевидна.

Предложение доказано.

**Определение 10.** *Пусть имеется множество , на котором задано отношение эквивалентности . Тогда можно образовать новое множество, элементами которого будут являться классы эквивалентности отношения . Это множество будет называться фактор-множеством множества  по отношению  и обозначаться .*

**Пример 6.** Пусть  – множество целых чисел. Зададим отношение  следующим образом. Для  будем считать, что   
, если  делится на 5. Несложно проверить, что  будет отношением эквивалентности. Фактор-множество  будет состоять из пяти элементов. Одним из элементов будет являться множество всех целых чисел, делящихся на 5. Другой элемент будет образовывать множество целых чисел, которые при делении на 5 дают в остатке 1 и т.д.

**Задачи.**

1. Сколько существует бинарных отношений на множестве из трёх элементов?

2. Сколько существует рефлексивных бинарных отношений на множестве из трёх элементов?

3. Сколько существует симметричных бинарных отношений на множестве из трёх элементов?

4. Сколько существует антисимметричных бинарных отношений на множестве из трёх элементов?

5. Приведите пример рефлексивного, симметричного, но не транзитивного бинарного отношения на множестве из трёх элементов.

6. Приведите пример рефлексивного, транзитивного, но не симметричного бинарного отношения на множестве из трёх элементов.

7. Приведите пример симметричного, транзитивного, но не рефлексивного бинарного отношения на множестве из трёх элементов.

Выясните, является ли следующее бинарное отношение  на множестве  натуральных чисел: 1) рефлексивным; 2) симметричным; 3) антисимметричным; 4) транзитивным? Будет ли  отношением эквивалентности или порядка?

8.  – чётно.

9.  – нечётно.

10.  – чётно.

11.  – нечётно.

12. .

13.  – целое чётное.

14.  – целое.

15.  – целое положительное.

16.  делит .

17. , где  – наибольший общий делитель чисел  и .

18. .

19. Сколько существует отношений эквивалентности на множестве из двух элементов?

20. Сколько существует отношений эквивалентности на множестве из трёх элементов?

21. Сколько существует отношений эквивалентности на множестве из четырёх элементов?

22. Сколько существует отношений порядка на множестве из двух элементов?

23. Сколько существует отношений порядка на множестве из трёх элементов?

Какие из следующих бинарных отношений  на множестве  всех непрерывных функций на отрезке  являются отношениями порядка?

24. .

25. .

26. .

27. .

28. Пусть  – множество всех упорядоченных наборов длины  из 0 и 1. Если , , то будем считать, что . Проверьте, что отношение  является отношением порядка.

29. Пусть  – множество всех упорядоченных наборов длины  из 0 и 1. Если , , то будем считать, что  тогда и только тогда, когда  и  или . Проверьте, что отношение  является отношением порядка. Этот порядок называется лексикографическим, потому что в этом порядке располагаются слова в словарях и энциклопедиях.

**1.3. Понятие группы. Примеры групп**

**Определение 1.** *Пусть  – некоторое множество. Бинарной операцией на  называется произвольное отображение . Если , то результат бинарной операции чаще всего будем обозначать , где  – знак бинарной операции.*

**Определение 2.** *Множество  с бинарной операцией  называется группой, если*

*1) ;*

*2) , этот элемент  будем называть единицей группы ;*

*3) , элемент  для элемента  будем называть обратным к .*

*Если к условиям 1) – 3) добавить условие*

*4) , то группа  называется абелевой или коммутативной. В этом случае знак бинарной операции чаще обозначают , что мы и будем делать.*

Результат бинарной операции  в дальнейшем будем называть произведением. Прежде всего, заметим, что, благодаря условию 1), произведение нескольких элементов группы можно записывать без скобок.

**Предложение 1.** *Единица в группе может быть только одна.*

***Доказательство.*** Действительно, если два элемента  обладают свойством 2), то .

Предложение доказано.

**Предложение 2.** *В группе элемент, обратный к данному элементу , может быть только один.*

***Доказательство.*** Если два элемента  и  обладают свойством 3) для элемента , то

.

Предложение доказано.

Приведём примеры групп.

**Пример 1.** Множества целых чисел , рациональных чисел , действительных чисел  с обычной операцией сложения  являются абелевыми группами.

**Пример 2.** Множества положительных рациональных чисел , положительных действительных чисел  с обычной операцией умножения  являются абелевыми группами.

**Пример 3.** Множество  всех -матриц с действительными элементами и с отличным от нуля определителем образует группу относительно операции произведения матриц (но уже не абелеву).

**Пример 4.** Пусть  – фиксированное натуральное число, большее единицы. Рассмотрим множество символов . На этом множестве определим операцию . Положим , где  – остаток от деления числа  на . Нетрудно проверить, что получится абелева группа. Она называется группой вычетов по модулю  и обозначается символом . Например, в группе 

.

**Пример 5.** Пусть  – множество из  первых натуральных чисел. Взаимно однозначные отображения множества  в себя называются подстановками и записываются в виде



(§ 1, определение 11 и пример 4). Роль операции играет суперпозиция отображений. Отметим, что суперпозиция действует справа налево. Например, если  и  – подстановки, а , то , т.е. сначала на элемент  действует , а потом . Единицей является тождественное отображение . Легко убедиться, что каждая подстановка имеет обратную. Кроме того суперпозиция отображений всегда обладает свойством ассоциативности. Поэтому подстановки образуют группу, которую мы будем называть группой подстановок  или симметрической группой. Эта группа некоммутативна. Число подстановок на  символах равно . Поэтому . В частности, .

**Пример 6.** Рассмотрим группу, состоящую из элементов . Перемножаются они следующим образом: , , . Умножение на (–1) соответствует смене знака. Если под  понимать орты координатных осей , декартовой системы координат в пространстве, то умножение элементов  соответствует векторному произведению ортов. Эта группа называется группой кватернионов и обозначается .

В § 1 мы дали определение движения на плоскости (определение 15). Далее сформулируем понятие группы движений геометрической фигуры.

**Определение 3.** *Пусть  – некоторая фигура на плоскости, которую мы понимаем как множество точек. Будем говорить, что движение плоскости  оставляет фигуру  на месте, если для любой точки  точка  также принадлежит . Или, более формально, если*

*.*

*Множество всех движений, оставляющих фигуру  на месте, образует группу, которая называется группой движений фигуры .*

**Пример 7.** Группа движений правильного -угольника обозначается .

Рассмотрим группу  движений правильного треугольника. Пусть  – правильный треугольник на плоскости (рис.1.1).

Существует 6 движений, оставляющих треугольник  на месте:

 – поворот на 120° вокруг центра треугольника точки  против часовой стрелки;

 – поворот на 240°;

 – симметрия относительно прямой, проходящей через точки  и ;

 – симметрия относительно прямой ;

 – симметрия относительно прямой ;

 – тождественное преобразование.

Каждая конечная группа может быть задана таблицей умножения, которая иначе называется «таблицей Кэли».

Для составления таблицы элементы группы выписываются по горизонтали и вертикали в определённом порядке. В клетке на пересечении строки  и  пишется элемент .

Выпишем таблицу Кэли для группы .

*Таблица 1.1*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Таблица Кэли обладает важным свойством: в каждой строке и каждом столбце каждый элемент группы встречается ровно один раз. Таким образом, каждый столбец и каждая строка являются некоторой перестановкой элементов группы.

**Задачи.**

Какие из указанных множеств с заданной на них операцией являются группами?

1., где  – одно из множеств , а операция  – обычное сложение.

2. , где  – одно из множеств , а операция  – обычное умножение.

3. , где  – одно из множеств , .

4. , где  – некоторое фиксированное натуральное число.

5. .

6. , где  – множество положительных действительных чисел.

7. , где  – множество положительных рациональных чисел.

8. Множество степеней данного натурального числа большего единицы с целыми показателями относительно умножения.

9. Множество всех комплексных корней из 1 фиксированной степени  относительно умножения.

10. Множество всех комплексных корней из единицы всех степеней относительно операции умножения.

11. Множество всех комплексных чисел с модулем 1 относительно умножения.

12. Функции  с операцией суперпозиция функций.

13. Функции   с операцией суперпозиция функций.

14. Сколько элементов содержит группа движений правильного -угольника?

15. Составьте таблицу умножений для группы  движений квадрата.

16. Составьте таблицу умножений для группы движений прямоугольника, не являющегося квадратом.

17. Составьте таблицу умножений для группы движений ромба, не являющегося квадратом.

18. Составьте таблицу умножений для группы движений правильного пятиугольника.

19. Составьте таблицу умножений для группы кватернионов .

**1.4. Гомоморфизмы и изоморфизмы групп**

**Определение 1.** *Пусть  и  – группы. Отображение*

**

*называется гомоморфизмом, если для любых *

.

**Определение 2.** *Изоморфизмом групп  называется гомоморфизм, который является взаимно однозначным отображением. Если группы  и  изоморфны, то принято обозначать* .

**Предложение 1.** *Пусть  – гомоморфизм групп,  – единицы групп ,  соответственно. Тогда .*

***Доказательство.*** Умножая левую и правую части равенства  на , получим требуемое.

Предложение доказано.

**Предложение 2.** *Пусть  – гомоморфизм групп и . Тогда *.

***Доказательство.*** Действительно,  . Аналогично . Это и означает, что .

Предложение доказано.

**Определение 3.** *Пусть  – группа с единицей . Наименьшее натуральное , для которого  называется порядком элемента  и обозначается . Если такого  не существует, то считается, что .*

**Предложение 3.** *Пусть  – гомоморфизм групп и  – элемент конечного порядка. Тогда элемент  также имеет конечный порядок, причём, если , то  делится на .*

***Доказательство.*** . Поэтому элемент  имеет конечный порядок. Допустим, что  не делится на . Тогда , где . В этом случае  , что противоречит тому, что  – наименьшая степень такая, что .

Предложение доказано.

**Пример 1.** Покажем, что . Каждому преобразованию группы  можно сопоставить перестановку – перестановку вершин треугольника . Действительно, занумеруем вершины:  – 1,   
 – 2,  – 3. Тогда отображение , при котором

,

.

является изоморфизмом.

**Пример 2.** Отображение , при котором каждому целому  ставится в соответствие его остаток  при делении на , является гомоморфизмом групп, но не изоморфизмом. Например, если , то , , , т.к. .

**Пример 3.** Пусть  – группа всех действительных чисел отличных от нуля с обычной операцией умножения.



сопоставляет каждой матрице её определитель. Тогда  – гомоморфизм групп, т.к. определитель произведения матриц равен произведению определителей. Гомоморфизм  не является изоморфизмом, т.к. разные матрицу могут иметь одинаковые определители.

**Пример 4.** Пусть  – группа всех действительных чисел с операцией сложения, а  – группа всех положительных действительных чисел с операцией умножения. Гомоморфизм



определён формулой . Это действительно гомоморфизм, т.к.

.

Более того, этот гомоморфизм является изоморфизмом.

**Определение 3.** *Пусть  – группа. Нетрудно убедиться, что множество всех изоморфизмов  также образует группу, которая называется группой автоморфизмов группы  и обозначается .*

**Пример 5.** Найдём группу . Заметим, что в группе  каждый элемент  является суммой  нескольких единиц. Поэтому, чтобы задать гомоморфизм , достаточно задать . Действительно, если , то  и т.д. Чтобы гомоморфизм был взаимно однозначным отображением,  может равняться либо , либо . Обозначим первый гомоморфизм , а второй – . Тогда . Поэтому .

**Задачи.**

1. Пусть  – группа окружности.  состоит из всех комплексных чисел с модулем, равным 1 и с операцией умножения. Рассмотрим отображение , определённое формулой . Определите, является ли : а) гомоморфизмом; б) изоморфизмом.

2.Пусть на множестве всех действительных чисел из интервала  задана операция , где  – дробная часть числа . Докажите, что множество  с операцией  является группой, изоморфной группе окружности .

3. Докажите, что следующие группы попарно изоморфны:

а) ;

б) ;

в) множество матриц ,  с операцией умножения матриц, причём сложение осуществляется по модулю ;

г) функции ,  с операцией суперпозиция функций.

4. Найдите группу автоморфизмов  для следующих групп:

а) ; б) ; в) ; г) ; д) .

5. Пусть , . Эти множество образуют группы относительно операции обычного умножения. Определите, какие из следующих отображений  являются гомоморфизмами:

а) ; б) ; в) ; г) ;

д) ; е) ; ж) .

6. Известно, что группы  и  изоморфны. Изоморфизм  может быть задан, например, формулой . Изоморфны ли группы  и ?

**1.5. Подгруппы. Теорема Кэли. Смежные классы.   
Теорема Лагранжа.**

**Определение 1.** *Подмножество  группы  называется подгруппой, если выполнены следующие условия*

1) ;

2) ;

3) .

**Пример 1.** Целые числа, делящиеся на фиксированное натуральное число  образуют подгруппу  в группе .

**Пример 2.** Следующие множества чисел с обычной операцией сложения образуют цепочку подгрупп

.

**Пример 3.** В группе  имеется подгруппа , состоящая из -матриц с определителем, равным .

**Пример 4.** Если число  не является простым, и  – нетривиальный делитель числа , то  – нетривиальная подгруппа в . (Тривиальными подгруппами в любой группе называются единичная подгруппа и вся группа).

**Пример 5.** В группе  всех движений треугольника нетривиальными подгруппами являются

.

**Пример 6.** В группе  движений правильного -угольника имеется подгруппа вращений . При любом .

**Определение 2.** *Если  – подгруппа группы  и , то множество*

**

*называется левым смежным классом группы  по подгруппе . Соответственно, множество  называется правым смежным классом.*

**Пример 7.** Найдём левые и правые смежные классы группы  по подгруппе . Левые смежные классы:

.

Правые смежные классы:

.

Левые и правые смежные классы группы  по подгруппе  совпадают:

 и .

Каждое разбиение группы  на левые (правые) смежные классы по любой подгруппе  задаёт некоторое отношение эквивалентности.

**Определение 3.** *Число элементов конечной группы  будем называть её порядком и обозначать символом  .*

**Определение 4.** *Пусть . Через  будем обозначать наименьшую подгруппу в , содержащую элементы . Если , то элементы  будем называть системой образующих группы . Систему  будем называть минимальной системой образующих группы , если после удаления любого элемента оставшееся множество уже не будет являться системой образующих для . Группу  будем называть циклической, если найдётся элемент  такой, что .*

Например, в группе  множество  будет минимальной системой образующих. Так как группа  не коммутативна, она не может быть циклической. Циклической будет, например, группа вычетов по любому модулю , поскольку она порождается элементом .

**Теорема (Лагранжа).** *Порядок подгруппы делит порядок конечной группы.*

***Доказательство.*** Пусть  – конечная группа,  – подгруппа. Рассмотрим разбиение группы  на левые смежные классы по подгруппе . Во-первых, всегда . Значит, объединение всех левых смежных классов даёт .

Далее, покажем, что левые смежные классы либо не пересекаются, либо совпадают. Действительно, если , то  для некоторых . Но тогда , а . Отсюда следует, что .

Теперь покажем, что все левые смежные классы состоят из одного и того же числа элементов. Действительно, рассмотрим отображение , задаваемое правилом . Разные элементы при этом отображении переходят в разные. Действительно, если , то умножая равенство слева на , получим . Следовательно, . Таким образом, конечное множество  разбилось на некоторое множество (пусть ) подмножеств, состоящих из  элементов. Тогда .

Теорема доказана.

**Следствие.** *Если  – конечная группа, то порядки её элементов являются делителями числа .*

***Доказательство.*** Если , то множество  образует подгруппу в .

Следствие доказано.

**Пример 8.** Найдём все гомоморфизмы из группы  в группу . Каждый такой гомоморфизм определяется образом элемента , поскольку , то порядок элемента  должен быть делителем числа 6. С другой стороны, , поэтому порядок элемента  должен быть делителем числа 15. Значит, порядок элемента  должен быть делителем числа 3. Таких элементов в группе  три. Это  и . Поэтому существуют три гомоморфизма из группы  в группу , для которых ,  и .

**Задачи.**

1. Найдите все подгруппы группы  движений квадрата. Найдите порядки всех элементов этой группы.

2. Найдите все подгруппы группы движений прямоугольника, не являющегося квадратом. Найдите порядки всех элементов этой группы.

3. Найдите все подгруппы группы движений ромба, не являющегося квадратом. Найдите порядки всех элементов этой группы.

4. Найдите все подгруппы группы движений правильного пятиугольника. Найдите порядки всех элементов этой группы.

5. Найдите все подгруппы группы кватернионов . Найдите порядки всех элементов этой группы.

**1.6. Нормальные подгруппы. Фактор-группы**

**Определение 1.** *Подгруппа  группы  называется нормальной, если левые и правые смежные классы по этой подгруппе совпадают, т.е., если*

*.*

*Тот факт, что  – нормальная подгруппа в  обозначается так: .*

**Пример 1.** В группе  подгруппа  является нормальной. Подгруппы  нормальными не являются.

**Определение 2.** *Пусть  – нормальная подгруппа в . Смежный класс  будем обозначать . Рассмотрим множество  всех смежных классов с бинарной операцией.*

*.*

*Это множество образует группу, которую мы будем называть фактор-группой и обозначать .*

*Гомоморфизм , определённый формулой , будем называть каноническим.*

**Предложение 1.** *Результат бинарной операции, определённый в определении 2, не зависит от выбора представителя.*

***Доказательство.*** Пусть  и  – другие представители смежных классов  и . Тогда , , . Поскольку , то найдётся элемент  такой, что . Тогда  и поэтому .

Предложение доказано.

**Пример 2.**  (группа окружности). Отображение явно может быть задано формулой .

**Пример 3.** .

**Пример 4.** .

**Задачи.**

1. Пусть ,  – подгруппа матриц с определителем, равным единице. Докажите, что .

2. Подгруппа Клейна  группы  состоит из четырёх элементов:



и единицы. Верно ли, что ?

3. Пусть  – подгруппа конечной группы . Число  называется индексом подгруппы . Докажите, что всякая подгруппа индекса 2 нормальна.

4. Докажите, что в группе кватернионов  любая подгруппа является нормальной.

Выясните, что из себя представляет фактор-группа , если

5. .

6. .

7. .

8.  – группа всех ненулевых действительных чисел с операцией умножения,  – группа всех положительных действительных чисел с операцией умножения.

**1.7. Циклические группы. Теорема о строении   
конечных абелевых групп**

**Теорема 1.** *Всякая бесконечная циклическая группа изоморфна . Всякая конечная циклическая группа изоморфна  для подходящего натурального .*

***Доказательство.*** Пусть  – образующий циклической группы . Если все степени элемента  различны, то отображение  осуществляет изоморфизм  и . Допустим теперь, что не все степени различны. Тогда  для некоторых целых . В этом случае . Пусть  – наименьшее натуральное число, при котором . Тогда все степени  различны, и отображение  осуществляет изоморфизм  и .

Теорема доказана.

Примером конечной циклической группы может служить группа  вращений правильного -угольника.

**Определение 1.** *Пусть имеются две группы  и . На декартовом произведении  введём структуру группы, задав умножение формулой*

*.*

*Легко проверить, что множество  с введённой таким образом операций образует группу. Эту группу будем называть прямым произведением групп  и . В случае, когда группы  и  – абелевы, будем использовать аддитивную запись: . В этом случае полученную группу будем называть прямой суммой групп  и .*

**Определение 2.** *Пусть  – абелева группа, и  – простое число. Множество элементов группы , порядки которых равны степени числа , образуют подгруппу группы , которую мы будем называть -примарной компонентой или просто примарной компонентой и обозначать символом . Группу , совпадающую со своей -примарной компонентой будем называть -группой.*

**Определение 2.** *Циклическую группу будем называть примарной циклической группой, если ее порядок является степенью простого числа***.**

Например, группы  яваляются примарными циклическими, так как их порядки являются степенями простых чисел: . Однако, группа  не является примарной циклической.

Следующие две теоремы приведём без доказательства.

**Теорема 2.** *Всякая конечная абелева группа  порядка  изоморфна прямой сумме своих примарных компонент:*



**Теорема 3.** *Каждая конечная абелева группа изоморфна прямой сумме примарных циклических групп. Это разложение однозначно с точностью до перестановки слагаемых.*

**Пример 1.** Рассмотрим группу вычетов . Тогда , . Изоморфизм  можно задать следующим образом

.

Если , то группа вычетов по модулю  раскладывается в прямую сумму примарных -компонент следующим образом

.

**Пример 2.** Разложим группу вычетов  в прямую сумму своих примарных компонент. Поскольку , то

.

Для того, чтобы разложить абелеву группу



в прямую сумму примарных циклических групп, нужно разложить каждое слагаемое этой группы.

**Пример 3.** Разложим группу



в прямую сумму примарных циклических групп. Поскольку , , , то

,

,

.

Поэтому

.

**Пример 4.** Определим, изоморфны ли группы  и .

Поскольку , , то

.

Далее, , . Поэтому

.

Поскольку разложения совпадают с точностью до перестановки слагаемых, группы изоморфны.

**Пример 5.** Определим, изоморфны ли группы  и . Находим разложение каждой группы в прямую сумму примарных циклических групп.

,

.

Примарные циклические группы не совпадают. группы не изоморфны.

Число неизоморфных абелевых групп порядка  равно числу  разбиений числа  в сумму нескольких (возможно, одного) натуральных чисел

, где .

Например, существуют две неизоморфные абелевы группы порядка :  и .

, т.к. .

, т.к. .

, т.к.  .

**Пример 6.** Найдём число неизоморфных абелевых групп порядка 64. Поскольку  и  , то . Поэтому существует 11 неизоморфных абелевых группы порядка 64.

**Пример 7.** Найдём число неизоморфных абелевых групп порядка 864. . Так как , , то абелевых групп порядка 864 существует .

**Задачи.**

Разложите в прямую сумму примарных циклических групп следующие группы

1. .

2. .

3. .

4. Сколько существует неизоморфных абелевых групп порядка: а) 36; б) 100; в) 64?

Выясните, изоморфны ли следующие группы.

5.  и ?

6.  и ?

7.  и ?

**1.8. Конечные группы до 10-го порядка**

В этом параграфе мы перечислим все конечные группы до 10-го порядка включительно с точностью до изоморфизма.

. Существует одна группа порядка 1, состоящая из одной единицы . Естественно, она абелева.

. Существует одна абелева группа порядка 2 – это .

. Существует одно абелева группа порядка 3 – это .

. Здесь существует две группы – это  и . Обе они абелевы.

. Существует одна абелева группа порядка 5 – это .

. Здесь существуют две группы, одна из них абелева – это , другая – неабелева. Это  – группа движений треугольника.

. Существует одна абелева группа порядка 7 – это .

. Существует 5 групп порядка 8. Три из них абелевы. Это  и . Кроме них существуют две неабелевы группы. Это  – группа движений квадрата и  – группа кватернионов.

. Существует две абелевы группы порядка 9. Это  и .

. Существуют две группы порядка 10. Одна из них абелева. Это . Другая – неабелева. Это  – группа движений правильного пятиугольника.

**Задачи.**

1. Докажите, что всякая циклическая группа является абелевой.

2. Докажите, что любая конечная группа простого порядка  изоморфна  – группе вычетов по модулю .

3. Докажите, что если в конечной группе каждый элемент кроме единицы имеет порядок 2, то эта группа абелева.

4. Докажите, что любая группа порядка 4 изоморфна либо , либо группе движений ромба.

5. Докажите, что в неабелевой группе порядка 6 должен существовать элемент порядка 3.

6. Пусть  – неабелева группа порядка 6,  – элемент порядка 3 и . Докажите, что тогда все элементы   – разные и  имеет порядок 2.

7. Докажите, что в обозначениях предыдущей задачи .

8. Докажите, что всякая неабелева группа порядка 6 изоморфна .

**1.9. Кольцо, модуль над кольцом, тело, поле.**

**Определение 1.** *Множество  с двумя бинарными операциями  и  называется ассоциативным кольцом, если*

*1) относительно операции  множество  является абелевой группой;*

*2) ;*

*3) ;*

*В случае, если*

*4) , кольцо  называется коммутативным.*

*В случае, когда*

*5) , говорят, что кольцо  имеет единицу.*

Неассоциативных колец мы рассматривать не будем, поэтому в дальнейшем слово кольцо будет обозначать ассоциативное кольцо.

**Пример 1.** Множество  с обычными операциями  и  является коммутативным кольцом с 1.

**Пример 2.** Множества  с обычными операциями  и  являются коммутативными кольцами с 1.

**Пример 3.** Множество  операции  и , в котором определяются как остатки от деления на  результатов обычных операций сложения и умножения, является кольцом. Например, в кольце .

 – всегда коммутативное кольцо с 1.

**Пример 4.** Кольцо матриц  размера  с коэффициентами из  и с операциями сложения и умножения матриц,  является уже некоммутативным кольцом с 1.

**Пример 5.** Множество  всех непрерывных функций на отрезке  с операциями «поточечного» сложения и умножения функций. Это коммутативное кольцо с 1.

**Пример 6.** Кольцо многочленов  от одной переменной с действительными коэффициентами и с обычными операциями сложения и умножения многочленов. Это также коммутативное кольцо с 1.

**Определение 2.** *Кольцо с 1 называется телом, если каждый ненулевой элемент имеет обратный*.

**Определение 3.** *Коммутативное кольцо с единицей, в котором каждый ненулевой элемент имеет обратный, называется полем.*

Оказывается, всякое конечное тело является полем. Эта теорема была доказана Веддербарном в 1905 году.

**Определение 4.** *Пусть  – подмножество в кольце . Если относительно существующих в кольце  операций «сложения» и «умножения»  также является кольцом, то  называется подкольцом кольца .*

**Определение 5.** *Подкольцо  кольца  называется идеалом, если  и  элементы  и  принадлежат .*

**Пример 7.** Множество  для фиксированного натурального  является идеалом кольца .

**Определение 6.** *Пусть  – идеал кольца . Рассмотрим множество смежных классов кольца  по идеалу , рассматриваемое пока как абелева группа. Смежными классами будут являться подмножества кольца  вида , которые мы будем обозначать . В фактор-группе  имеется операция сложения, определённая формулой . Определим операцию умножения равенством*

*.*

*В силу того, что  – идеал, это определение корректно.*

Рассмотренное множество смежных классов с определёнными на нём операциями  и  образуют кольцо, которое называется фактор-кольцом кольца  по идеалу  и обозначается .

**Пример 8.** .

**Определение 7.** *Пусть  и  – кольца. Отображение  называется гомоморфизмом колец, если *

*.*

*Если к тому же  – взаимно однозначное отображение, то  называется изоморфизмом.*

Среди рассмотренных примеров 1 – 6 примерами полей являются . Если же  – простое число, то кольцо  вычетов по модулю  также является полем.

**Пример 9.** Пусть  – кольцо -матриц вида

.

Проверка показывает, что отображение



является изоморфизмом, т.е. кольцо  изоморфно полю комплексных чисел.

**Пример 10.** Рассмотрим кольцо многочленов  и идеал , состоящий из всех многочленов, делящихся на . В этом случае говорят, что  порождён многочленом . Можно записать . В каждом смежном классе можно выбрать представитель в виде многочлена степени не выше первой. Поэтому элементы этого фактор-кольца можно записывать в виде . Отображение  является изоморфизмом, т.е. опять .

**Пример 11.** Примером тела, не являющегося полем, может служить «тело кватернионов».

Пусть  – символы, перемножающиеся по правилу

. (\*)

Множество выражений , где , с операцией покомпонентного сложения и умножения, определённого с помощью формул (\*) и закона дистрибутивности, образует тело, называемое телом кватернионов.

**Задачи.**

1. В кольце вычетов  найдите все обратимые элементы.

2. Найдите все нетривиальные идеалы в кольце вычетов .

3. Пусть  – множество всех векторов в пространстве. В качестве операции  рассмотрим обычное сложение векторов, а в качестве операции  рассмотрим векторное произведение. Будет ли  с двумя этими операциями ассоциативным кольцом?

**1.10. Строение конечных полей**

**Определение 1.** *Пусть  – поле. Наименьшее натуральное , при котором , называется характеристикой поля  и обозначается . Если такого  не существует, то считается, что .*

**Теорема 1.** *Характеристика конечного поля – простое число.*

***Доказательство.*** Если бы , где , то в поле  произведение двух ненулевых элементов  и  равнялось бы 0. Это невозможно. Действительно, равенство  можно было бы умножить на , и тогда . Противоречие.

Теорема доказана.

Если характеристика поля  равна , то  содержит подполе из  элементов, изоморфное . Элементами этого подполя являются суммы .

**Теорема 2.** *Число элементов конечного поля характеристики  равно  для некоторого натурального .*

***Доказательство.*** Поле  можно рассматривать как векторное пространство над подполем . Как во всяком векторное пространстве, в  можно выбрать базис  над . Этот базис конечен в силу конечности поля . Каждый элемент поля  можно единственным образом представить в виде . Число таких выражений равно .

Теорема доказана.

**Теорема 3.** *Для каждого простого  и натурального  существует единственное с точностью до изоморфизма конечное поле из  элементов.*

Без доказательства.

**Определение 2.** *Конечное поле из  элементов обозначается  и называется полем Галуа.*

**Определение 3.** *Если рассматривать все ненулевые элементы конечного поля, то относительно операции умножения они образуют коммутативную группу. Эта группа называется мультипликативной группой поля.*

Имеет место следующий факт.

**Теорема 4.** *Мультипликативная группа конечного поля циклическая.*

Без доказательства.

**Определение 4.** *Образующие мультипликативной циклической группы поля называются примитивными элементами этого поля.*

Если , то примитивными элементами  будут те, для которых .

Если  – конечное поле, то можно рассматривать кольцо многочленов  над . Элементами этого кольца являются многочлены от переменной  с коэффициентами из . Как обычно, степенью многочлена  называется число .

**Определение 5.** *Многочлен  над полем  называется неприводимым, если его нельзя представить в виде произведения двух многочленов меньших степеней.*

**Пример 1.** Найдём неприводимые многочлены над полем  степени 2. Всего существует 4 многочлена степени 2:

.

Неприводимым среди них является только , т.к.

.

Многочлен  неприводим, т.к. 0 и 1 не являются его корнями, и поэтому он не может быть разложен в произведение двух линейных многочленов.

Существуют 2 неприводимых многочлена 3-й степени: , .

**Теорема 5.** *Для каждого простого  и натурального  в кольце  существуют неприводимые многочлены степени .*

Без доказательства.

**Теорема 6.** *Пусть  – неприводимый многочлен степени  над полем . Пусть  – идеал в кольце многочленов , порождённый многочленом . Тогда  – конечное поле из  элементов.*

***Доказательство.*** Фактор-кольцо  коммутативно и имеет единицу. Если , то в кольце  найдутся многочлены  и  такие, что  (Это следует из алгоритма Евклида). Тогда  в кольце , т.е. каждый ненулевой элемент кольца  обратим. Значит  – поле.

**Пример 2.** Рассмотрим поле . Его можно представлять как фактор-кольцо , где  (нам будет удобнее здесь писать  вместо ). В каждом смежном классе можно выбрать в качестве представителя многочлен степени не выше первой: . Таблица умножений элементов этого поля выглядит так:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 0 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 |  |  |
|  | 0 |  |  | 1 |
|  | 0 |  | 1 |  |

Пусть . Каждый ненулевой элемент поля является корнем уравнения . Многочлен  в кольце  можно разложить в произведение неприводимых многочленов:

.

Тогда каждый ненулевой элемент поля является корнем одного из них.

**Определение 6.** *Пусть элемент  конечного поля  из  элементов является корнем многочлена  – одного из неприводимых многочленов в разложении . Тогда этот многочлен называется минимальным многочленом для .*

Среди всех многочленов, одним из корней которых является , этот многочлен имеет наименьшую степень. Каждый элемент поля имеет свой минимальный многочлен.

**Пример 2 (продолжение).** Минимальным многочленом для 1 является . Минимальным многочленом для элементов  и  является многочлен . Разложением многочлена  в произведении неприводимых в данном случае является



(в поле  имеет место равенство ).

**Задачи.**

Все рассматриваемые многочлены предполагаются принадлежащими кольцу .

1. Разделите с остатком многочлен  на многочлен .

2. Найдите наибольший общий делитель , если , . Далее, найдите многочлены  и  такие, что .

3. Найдите все неприводимые многочлены 3-й, 4-й и 5-й степеней в кольце .

Разложите следующие многочлены в произведение неприводимых многочленов.

4. .

5. .

6. .

Через  будем обозначать идеал, порождённый многочленом . Этот идеал состоит из всех многочленов, делящихся на .

7. Выпишите таблицу умножения для элементов фактор-кольца . Будет ли это кольцо полем?

Найдите наименьший идеал, содержащий многочлены  и .

8.**.**

9.**.**

10.Выпишите таблицу умножения для элементов фактор-кольца , взяв в качестве представителей смежных классов многочлены степени не выше второй. Будет ли это кольцо полем?

11. Выпишите таблицу умножения для элементов фактор-кольца , взяв в качестве представителей смежных классов многочлены степени не выше второй. Будет ли это кольцо полем?

12. Задайте явным образом изоморфизм полей  из задач 10 и 11.