**Теория алгебраических структур**

**Теория групп**

**Полугруппы, моноиды, группы**

**Опр.** Говорят, что на множестве *M* задана бинарная операция ∗, если любой упорядоченной паре *< a, b >* элементов из *M* ставится в соответствие элемент *(a ∗ b) ∈ M.*

**Примеры.**

1. - бинарная операция (-числовое множество).
2. - бинарная операция (- множество векторов).
3. - не является бинарной операцией: векторам ставится в соответствие число ( - множество векторов).

Бывают унарные операции – транспонирование матрицы; и операции для любого упорядоченного набора из *n* элементов.

**Свойства операции:**

1. - операция коммутативная.
2. - операция ассоциативная.

**Утв.** Если бинарная операция ассоциативна, то результат ее применения к последовательности элементов не зависит от расстановки скобок.

Символика: мультипликативная (∗ → ·) и аддитивная (∗ → +).

В мультипликативной символике:

В аддитивной символике:

Если множество *M* конечное, то результат бинарной операции можно задать таблицей Кэли.

Таблица Кэли:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ∗ |  |  | … |  |
|  |  |  | … |  |
|  |  |  | … |  |
| … | … | … | … | … |
|  |  |  | ... |  |

**Опр.** 1. Полугруппой называется множество M c заданной на нем ассоциативной бинарной операцией:

Единичный элемент *e*: .

Единственность единичного элемента докажем от противного.

Пусть

**Опр. 2**. Моноид - это полугруппа с единицей

Элемент называется обратимым, если

(*а* - обратимый элемент, - обратный элемент к ).

Единственность обратного элемента:

Пусть

**Опр.** 3. Группа - это моноид, в котором каждый элемент обратим.

Если операция коммутативна, то соответственно полугруппа, моноид, группа коммутативны или абелевыми.

**Опр.** Полугруппа, моноид, группа называются конечными, порядка p, если состоят из p элементов.

Соответственно определяются полугруппа, моноид, группа бесконечного порядка.

Проверка, какой структурой является множество с заданной бинарной операцией

|  |  |  |
| --- | --- | --- |
| Полугруппа | Моноид | Группа |
| 1.Замкнутость относительно операции \* | | |
| 2.Ассоциативность \* | | |
|  |  | |
|  |  | 4. |

**Опр.** Подполугруппа – замкнутое относительно заданной бинарной операции подмножество

Подмоноид - замкнутое подмножество

**Опр.** Подгруппа - замкнутое подмножество

**Примеры**

1. - группа, . Подгруппа: < четные, +, 0 > и
2. Группы также: , комплексные числа.
3. Квадратные матрицы порядка n: - моноид, для любого элемента.
4. Группы: .
5. Матрицы - нулевая матрица, - группа.
6. Квадратные матрицы - моноид: для вырожденных матриц - обратной матрицы.
7. Квадратные матрицы - некоммутативная группа, если .Замкнутость: .
8. Множество всех биекций множества *X* в себя: . Операция - композиция: - некоммутативная группа.
9. Свободная группа - элементы - слова.

- пустое слово.

Операция \*- приписывание одного слова к другому:

,

для аналогично.

1. Конечную полугруппу можно задать таблицей Кэли:

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

Всего полугрупп из двух элементов 16.

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

Всего моноидов из двух элементов 4. (Можно выбрать )

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

Всего групп из двух элементов 2 - и

Пример группы из четырех элементов.

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

1. Группа классов вычетов по модулю . В каждом классе целые числа с одинаковым остатком от деления на .

Для класса

Построим таблицу Кэли для операции сложения. Получим группу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

- группа

Построим таблицу Кэли для операции умножения. Получим моноид.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \* |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Множество *M* вершин правильного n-угольника:

- поворот на 0

∗ - самосовмещение n-угольника :

1. поворот на

2. симметрии

**Для треугольника** (n=3) получим три поворота и три симметрии:

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

некоммутативная группа

Подгруппы:

1.

2.

3.

4.

5.

6.

**Группа самосовмещений квадрата**

2 1

3 4

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

Подгруппы:

1.

2.

3.

4.

5.

6.

7.

8.

9.

**Порождающее множество группы**

Пусть подгруппа .

**Опр.** Подгруппа, порожденная множеством *S* - минимальная подгруппа, содержащая *S.*

Обозначается .

Такая подгруппа единственная: .

**Утверждение:** - подгруппа G, если и - подгруппы G.

Доказательство.

3. Замкнутость:.

, .

Минимальная подгруппа *H*, содержащая множество *S*, образована пересечением всех подгрупп, содержащих *S*.

Подгруппа, порожденная множеством *S*, состоит из произведений элементов из *S* и обратных элементов.

**Циклические группы**

**Опр.** Циклическая группа - это группа , порожденная единственным элементом .

**Утверждение.** Циклическая группа , порожденная элементом состоит из целых степеней элемента .

.

Доказательство.

1. Замкнутость: . Рассмотрим следующие случаи:
2. – равенство следует из ассоциативности операции.
3. :
4. : - аналогично
5. : – аналогично.

Циклическая группа может быть конечной или бесконечной.

**Опр**. Если все степени элемента различны, то элемент – бесконечного порядка.

Если , домножим на , получим - - элемент конечного порядка , причем порядок равен наименьшему .

Все циклические группы коммутативны. Очевидно:

**Пример.**

1. Группа бесконечно порядка: .
2. Группа конечного порядка: повороты треугольника

**Утвердение.** Пусть *а* - элемент конечного порядка р, тогда порожденная им подгруппа *G =< a >* имеет порядок р (содержит р элементов).

Доказательство. Покажем, что группа состоит из р элементов:

1. Покажем, что все р элементов различны. Пусть Домножим на причем а это противоречит тому, что р- наименьшее число, большее 0, такое что все р элементов различны.
2. Покажем, что совпадет с одним из элементов множества Представим

**Теорема**. Каждая подгруппа циклической группы циклическая.

Доказательство.

Пусть имеется группа *G =< a >* и подгруппа *Н*. Выберем в H элемент с наименьшей положительной степенью: тогда очевидно, что . Докажем, что . Предположим, что это не так, т.е. такое, что *l* не делится нацело на p. Разделим с остатком: , что противоречит тому, что p порядок элемента *a* .

**Пример**. Группа бесконечно порядка: *G =< 1 >*, подгруппа  *=< 2 >.*

**Симметрические группы**

Рассмотрим множество

**Опр.** Симметрическая группа - это группа всех биекций множества Х в себя.

f : X → X.

В общем случае множество X может содержать любые элементов.

Элементы симметрической группы - подстановки (перестановки).

Симметрическая группа имеет n! элементов (подстановок):

**Пример**. 3! = 6 элементов

**Опр.** Цикл – перестановка такая, что .

**Опр.** Циклы и - независимые, если они не содержат общих элементов.

**Пример.**

(1 2 4)(3 5) - независимые циклы.

(1 2 4)(3 4 5) - не являются независимыми циклами.

Введем на множестве перестановок операцию умножение (композиция) перестановок:

- последовательное применение перестановок к каждому элементу.

**Пример.**

Порядок независимого цикла равен числу элементов в цикле: p()=5.

Порядок подстановки (наименьшее натуральное число p такое, что )

p() =НОК(#π1, #π2,...,#πk).

**Пример.** (т.к. -2=3-5). (остаток от деления на порядок-5)

**Транспозиции.**

**Опр**. Транспозиция - это цикл длины два.

Любую перестановку можно разложить в произведение транспозиций.

Пример разложения любого цикла:

или

**Пример**. – 2 способа разложения.

(1 2 3)=(1 3)(1 2)=(3 2)(3 1) - число транспозиций всегда одно и то же.

Перестановки делятся на четные и нечетные (с четным и нечетным числом транспозиций).

Четные перестановки образуют группу: - четная. – четная перестановка, если π четная. Если и- четные перестановки, то и - четная перестановка.

**Опр.** Два элемента множества - эквивалентные относительно перестановки π, если .

Это определение порождает отношение эквивалентности на множестве *Х*. Тогда существуют классы эквивалентности, которые порождают разбиение множества *Х*:

.

**Теорема.** Каждую перестановку можно представить произведением независимых циклов, причем единственным образом с точностью до перестановки циклов.

Док-во. Как представить показано выше – перемножить перестановки.

Док-во единственности. От противного. Пусть - независимые циклы. Выбираем i: . Пусть существует другое представление: . . Получаем, что Выбирая все элементы из , получим совпадение всех независимых циклов.

**Изоморфизм групп**

**Опр.** Две группы и изоморфны, если существует биекция , сохраняющая групповую операцию:

Пример 1.

и изоморфны: - биекция

Единица переходит в единицу:

Пример 2. Группа самосовмещений треугольника и группа изоморфны.

*Свойства изоморфизма:*

1. Единичный элемент переходит в единичный:

. Покажем, что выполняется равенство: .

2. Обратный элемент переходит в обратный:

Покажем, что .

**Теорема.** Все циклические группы одного порядка изоморфны.

1. Группы бесконечного порядка изоморфны группе

.

- биекция. Это - биекция и сохраняется групповая операция.

Биекция: .

Сохраняется групповая операция:

2. Группа *G* конечного порядка *n*

Докажем, что любая циклическая группа *G* конечного порядка *n* изоморфна группе классов вычетов по модулю *n*.

Пример группы:

Рассмотрим группы:

Биекция: .

Сохраняется групповая операция:

Теорема доказана.

***Покажем, сколько с точностью до изоморфизма групп второго, третьего и четвертого порядков.***

**Утверждение 1.** Групп второго порядка с точностью до изоморфизма одна, она циклическая: .

Доказательство. Составим таблицу Кэли

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

, т.к.

Пример группа второго порядка:

**Утверждение 2.** Групп третьего порядка с точностью до изоморфизма одна, она циклическая, порожденная любым не единичным элементом:

.

Доказательство. Составим таблицу Кэли

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

С‚ т.к. и т.к. .

Аналогично ,следовательно, группа **коммутативна.**

т.к.

Эта группа циклическая, также как и группа второго порядка.

Примеры группы третьего порядка:

- - группа вращений треугольника с операцией композиция;

- – группа классов вычетов по модулю 3 с операцией сложения.

***Группы четвертого порядка***

**Утверждение 3.** Любая группа четвертого порядка коммутативна.

Доказательство.

Пусть , и предположим, что какие-то два элемента не перестановочны . и , т.к. или Аналогично получаем . Пусть , а . Из того, что следует, что . А это противоречит предположению, что , следовательно, любая группа четвертого порядка коммутативна.

**Утверждение 4.** Групп четвертого порядка с точностью до изоморфизма две: **четвертная группа Клейна и циклическая.**

Доказательство.

1) Введем условие – все элементы группы сами себе обратные: Воспользуемся тем, что в группе в каждой строке и в каждом столбце все элементы различны (легко показать от противного).

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

Из второй строки: Из третьего столбца: . Следовательно, , , .

Эта группа называется четверная группа Клейна. Ее характерная особенность - все элементы сами себе обратны.

Примеры групп Клейна.

- Группа самосовмещений прямоугольника - группа Клейна.

Два поворота, две симметрии.

- – подгруппа перестановок, изоморфная группе самосовмещений прямоугольника:

2) Предположим, что не все элементы сами себе обратны. Пусть . Заполним таблицу Кэли, исходя из этого предположения и коммутативности группы четвертого порядка. Тогда . (Предполагая перестановочность других элементов, аналогично получим так же, как и вэтом случае, циклическую группу).

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

Из второй строки: Из четвертого столбца:

Очевидно, что . Из третьей строки: .

- циклическая группа

- циклическая группа

- циклическая подгруппа группы: .

Примеры. 1. Циклическая группа четвертого порядка - группа вращений квадрата

Подгруппа .

2. Циклическая группа четвертого порядка - группа классов вычетов по модулю 4:

Подгруппа .

**Теорема Кэли**. Всякая конечная группа изоморфна некоторой подгруппе симметрической группы.

Доказательство.

1) - биекция;

2) сохраняет групповую операцию.

Построим отображение (изоморфизм):

Покажем, что - действительно перестановка, т.е. все элементы нижнего уровня различны. Предположим, что это не так: , т.е. два элемента совпали. Но, т.к. группа, существуют обратные: а это по предположению различные элементы группы. Противоречие.

Покажем, что - биекция. сюрьективно, т.к. у каждого есть прообраз .

инъективно: если мы возьмем два различных элемента и Единичный элемент переходит в различные элементы, т.к. Следовательно, перестановки разные.

биективно.

Покажем сохранение групповой операции:

- из ассоциативности элементов группы.

**Смежные классы. Нормальный делитель (нормальные подгруппы)**

**Опр**. Левый смежный класс (ЛСК) группы *G* по подгруппе Н – множество элементов

*g* - фиксированный элемент группы *G, h* - пробегает все элементы группы Н.

Количество элементов совпадает с количеством элементов в Н.

**Опр.** Правый смежный класс (ПСК) группы G по подгруппе Н - множество элементов

Пример.

Три ЛСК:

1. 0+Н=Н=Н+0
2. 1+Н={1, 4, −2, 7, −5, ...}=Н+1
3. 2+Н={2, 5, −1, 8, −4, ...}=Н+2

Если операция коммутативна, то ЛСК=ПСК. Пересечение ЛСК пусто, а объединение дает все множество.

**Теорема***.* ЛСК образуют разбиение элементов группы *G*.

Доказательство.

Рассмотрим два ЛСК: и и предположим, что у них есть общий элемент: Т.к. все это - элементы группы, то существуют обратные:

домножим равенство на : , т.к. все три элемента , то из произведение также находится в *Н*. Любой элемент ЛСК является элементом класса , следовательно,

Аналогично, домножая на° , получим .

, т.е. два ЛСК, имеющих общий элемент, совпадают. Следовательно, ЛСК образуют разбиение: классы либо не пересекаются, либо совпадают.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | =H |
| ... |  |  |
|  |  |  |
| ... |  |  |

не принадлежит ни одному из уже построенных ЛСК.

ЛСК образуют разбиение, следовательно, в разных классах все элементы различны.

Аналогично ПСК образуют разбиение.

**Опр. 1**. Группа *Н* - нормальный делитель (нормальная подгруппа) группы *G*, если множества ЛСК и ПСК совпадают

**Опр. 2.** Группа *Н* - нормальный делитель (нормальная подгруппа) группы *G*, если

..

Доказательство эквивалентности двух определений.

Очевидно, что определение 2 →1. Покажем, что 1 →2. Так как и , а т.к. классы образуют разбиение, то

В коммутативной группе все подгруппы являются нормальными делителями.

**Пример 1.** Рассмотрим группу и

ее циклическую подгруппу

ЛСК ПСК

ЛСКПСК, следовательно, *Н* не является нормальным делителем.

**Пример 2**.

И циклическая подгруппа

ЛСК ПСК

ЛСК=ПСК, следовательно, *Н* - нормальный делитель. Здесь подгруппа индекса 2: она всегда нормальный делитель, т.к. смежные классов 2 - .

Индекс - число смежных классов.Для конечной группы число смежных классов равно отношению числа элементов группы к числу элементов ее нормального делителя

**Теорема Лагранжа***.* Порядок конечной группы делится на порядок любой ее подгруппы.

Доказательство следует из формулы

**Пример 1**. Группа самосовмещений квадрата:

- подгруппа. .

ЛСК=ПСК



*Н* - нормальный делитель.

**Пример 2.**

Легко убедиться, что ЛСКПСК и, следовательно, не является нормальным делителем.

**Сопряженные элементы**

**Опр.** Элемент *a* группы *G* сопряжен *b*, если .

Если *a* сопряжен к *b*, то *b* сопряжен к *a*.

, следовательно, *b* сопряжен к *a*.

**Теорема.** Подгруппа Н группы G - нормальный делитель тогда и только тогда, когда вместе с каждым своим элементом Н содержит и все сопряженные.

Доказательство.

1. Докажем, что если Н - нормальный делитель, то Н содержит вместе с любым своим элементом h и все сопряженные к нему. Н - нормальный делитель. Тогда . , домножим на для .

2. Докажем, что если Н содержит вместе с любым своим элементом h все сопряженные, то Н - нормальный делитель. Пусть для выполняется . Домножим равенство на . Следовательно, все элементы ПСК являются элементами ЛСК. Аналогично . Домножим равенство на , следовательно, элементы ЛСК являются элементами ПСК. Получим: ЛСК и ПСК совпадают, и Н - нормальный делитель:

**Фактор-группа**

Пусть H - нормальный делитель группы G.

G\H - фактор-множество группы G по нормальной подгруппе Н.

Введем операцию на множестве следующим образом:

. Очевидно, что . .

**Утверждение**. Фактор-множество G\H группы G по нормальной подгруппе Н является фактор-группой.

Доказательство.

1. Ассоциативность:

- следует из ассоциативности элементов группы G.

2.Единица принадлежит фактор-множеству и равна :

- существует единичный элемент.

3.Для каждого элемента множества G\H обратный элемент также принадлежит этому множеству и равен :

- все элементы G обратимы.

1⇒ G\H - группа.

**Пример 1**. .

В силу коммутативности сложения Н - нормальный делитель, следовательно, смежные классы совпадают.

1. 0 + H = H

2. 1 + H = {1, 4, −2, ...}

3. 2 + H = {2, 5, −1, ...}

Фактор-множество G\H = {H = E, 1 + H, 2 + H} является фактор-группой третьего порядка, и G\H - циклическая группа: G\H =< 1 + H >.

, следовательно, это взаимно обратные элементы: .

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

**Пример 2.** Группа самосовмещений квадрата:

.

- нормальный делитель.

ЛСК=ПСК

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

Каждый элемент сам себе обратен – четвертная группа Клейна.

**Гомоморфизм групп**

**Опр.** Отображение называется гомоморфизмом, если оно сохраняет групповую операцию:

.

Виды гомоморфизма:

• сюръективный (эпиморфизм);

• инъективный (мономорфизм);

• биективный (изоморфизм);

• (эндоморфизм);

• (естественный гомеоморфизм).

Свойства гомоморфизма:

1. - единичный элемент переходит в единичный.

2. - обратный элемент переходит в обратный.

Эти свойства уже были доказаны раньше (см. изоморфизм).

**Ядро и образ гомоморфизма**

**Опр.** Образ гомоморфизма:

Пусть , - образ. .

Если , то , - сюръективное отображение “на” .

**Теорема.** Образ гомоморфизма - подгруппа группы .

Доказательство.

1. Т.к. все элементы образа также элементы группы, то ассоциативность очевидна.
2. , т.к. . Единичный элемент переходит в единичный.

, следовательно, т.к. , то .

1. замкнутость:

,

(прообраз в ).

**Опр.** Ядро гомоморфизма - все элементы группы , которые переходят в единицу :

**Теорема**. Ядро - нормальная подгруппа группы G.

Доказательство.

Покажем, что - подгруппа группы G.

1) , т.к. . Единичный элемент переходит в единичный.

2) . Т.к. обратный элемент переходит в обратный.

3) замкнутость: ,

4) Покажем, что – нормальный делитель группы G. Используем доказанное ранее необходимое и достаточное условие того, что подгруппа является нормальным делителем: Ядро - нормальный делитель тогда и только тогда, когда вместе с каждым своим элементом оно содержит и все к нему сопряженные. Покажем, что для .

**Пример**. Фактор-группа /H, - группа самосовмещений квадрата, подгруппа

.

Группа самосовмещений квадрата:

2 1

3 4

Гомоморфизм групп: зададим следующим образом: каждому элементу группы G поставим в соответствие перестановку осей симметрии квадрата:

, L – подгрупп .

Отображение - не сюръективно, т.к. не у всех элементов есть прообраз; не инъективно, т.к., например, соответствует один и тот же элемент .

Отображение  - сюръективный гомоморфизми, т.к. у всех элементов есть прообраз; но не инъективный: соответствует один и тот же элемент .

Рассмотрим подгруппу в

Фактор-группа и соответствующие ей элементы :

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

Каждый элемент сам себе обратен – четвертная группа Клейна.

Отображение – группы в фактор-группу по ядру H.

Отображение фактор-группы по ядру в биективно - изоморфизм.

Напомним, что отображение  - сюръективный гомоморфизми

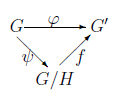
**Вывод.**

Природа всех сюръективных гомоморфизмов исчерпывается естественным гомоморфизмом, т.е. гомоморфизмом на группы на свою фактор-группу по ядру.

Обобщим этот результат.

**Теорема (основная теорема о гомоморфизмах)**.

Пусть – сюръективный гомоморфизм группы в группу с ядром ; - естественный гомоморфизм группы на свою фактор-группу по ядру (. Тогда отображение - изоморфизм. Причем выполняется .



**Задание группы образующими и определяющими соотношениями**

***Свободная группа.***

- алфавит и множество обратных символов -

Элементы группы - слова:

Групповая операция - приписывание одного слова к другому:

1. ассоциативность:
2. Λ - пустое слово - единичный элемент.
3. . Аналогично
4. Некоммутативная операция: .

***Определяющие соотношения***.

где - образующие элементы, *P, R, Q, ...* - определяющие соотношения.

(Пример: )

**Опр.** Эквивалентные слова и можно получить из за конечное число шагов, используя следующие преобразования:

1. Вставка в начало, середину или конец слова определяющих соотношений *P, R, Q*, или , или слов, тождественно равных единице Λ.

2. Удаление из начала, середины или конца слова определяющих соотношений *P, R, Q*, или , или слов, тождественно равных единице.

***Введем отношение предшествования на множестве слов:***

1)

2) , где *l* - длина слова.

3) - отношение предшествование определяется первыми несовпадающими символами.

**Пример 1.** –циклическая группа четвертого порядка (например, группа вращений квадрата)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  | *a* |
|  |  |  |  |  |

Подгруппа -

**Пример 2.**

1. Распознать группу - составить таблицу Кэли.

2. Сравнить с уже известными группами.

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

Подгруппа:

1. - нормальный делитель
2. . легко убедиться, что ЛСКПСК.

Примеры такой группы

1. Группа самосовмещений треугольника:

Подгруппы: ;

**Пример 3**. – четвертная группа Клейна

(группа самосовмещений прямоугольника и ромба).

**Пример 4.**  – циклическая группа порядка 6

(группа вращений правильного шестиугольника).

**Кольца и поля**

**Опр.** Кольцом называется непустое множество с заданными на нем бинарными операциями сложение и умножение, причем:

1) по сложению кольцо - коммутативная группа;

2) по умножению - полугруппа;

3) дистрибутивность

.

Кольцо с единицей – если существует единичный элемент по умножению .

Если операция умножения коммутативна, то и кольцо называется коммутативным.

**Опр.** Подкольцом называется подмножество , являющееся подгруппой по сложению и замкнутое по умножению.

**Опр.** Подкольцо кольца называется **идеалом**, если и выполняется и

*J,*

*J.*

**Пример 1.** - коммутативное кольцо с .

Подкольцо - . Подкольцо является идеалом.

**Пример 2**. кольцо матриц с элементами действительными числами -некоммутативное кольцо с единицей.

Для кольца матриц второго порядка

- подкольцо матриц вида идеалом не является, так как, например,

=:

- подкольцо матриц вида – левый идеал, но правым идеалом не является. Под определение идеала не подходит.

**Пример 3.** - кольцо функций одной переменной с операциями поэлементного сложения и умножения

**Пример 4.** - кольцо классов вычетов по .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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

**Кольцо с делителями нуля.**

**Опр.** Пусть в кольце и , а , тогда *a* -левый делитель нуля, *b* - правый делитель нуля, *K* - кольцо с делителями нуля.

**Пример 1**. - кольцо без делителей нуля.

**Пример 2**. Кольцо квадратных матриц порядка - с делителями нуля.

,

**Пример 3**. Кольцо функций с делителями нуля.

**Пример 4.** Кольцо классов вычетов

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

- правый и левый делители нуля -

Если – обратимый элемент кольца, - обратный элемент.

**Утверждение 1.** Обратимые элементы не могут быть делителями нуля.

Доказательство. От противного.

Пусть , но . И пусть для элемента существует обратный элемент . Домножим равенство на , получим: . Откуда , что противоречит предположению .

**Утверждение 2**. Все обратимые элементы кольца образуют группу по умножению.

Доказательство.

1)

2) , т. к. обратимы

3) замкнутость:

Следовательно,

Аналогично

4) ассоциативность следует из того, что это полугруппа по умножению.

**Опр.** Поле - коммутативное кольцо с единицей (по умножению), в котором каждый элемент, кроме нуля, обратим.

Поле и по сложению и по умножению (без нулевого элемента) коммутативная группа.

Поскольку обратимые элементы не могут быть делителями нуля, поле не может содержать делителей нуля.

**Пример 1**. - поле.

**Пример 2**. - поле.

**Пример 3**. - поле.

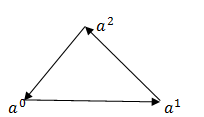
обратны по сложению

По умножению:

**Граф группы.**

Обозначим – множество элементов группы. Группу можно предствить графом где дуга , если – образующий элемент группы. Если идем в обратную сторону от образующей, то (так как ).

**Пример**:



– конечная циклическая группа, изображается правильным n-угольником.

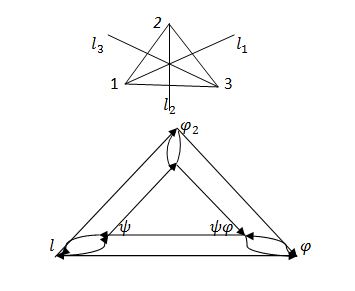
Бесконечная циклическая группа:

Элементы группы получаются сдвигом этой прямой на некоторое количество делений.

***Пример:*** =<1>

Можно представить графом группы с несколькими образующими элементами.

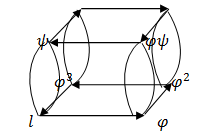
Группа самосовмещений треугольника:



Группы с двумя образующими можно изобразить в пространстве (группы диэдра)

Группа самосовмещений квадрата в пространстве.

Группа диэдра (2 плоскости):



**Таблица соответствий элементов в графе и в группе.**

|  |  |
| --- | --- |
| **Граф** | **Группа** |
| Вершина | Элемент группы |
| Дуга | Умножение на образующий элемент |
|  | Умножение на элемент, обратный к образующему |
| Путь | Слово из образующих |
| Цепь | Слово из образующих и обраных к ним элементов |
| Контур | Слово из образующих, тождественно равное единице |