**АЛГЕБРА-1**

**КОНСПЕКТ ЛЕКЦИЙ**

для студентов-заочников

направление подготовки «Педагогическое образование»

профиль «Математика»

2017/2018 учебный год

**МОДУЛЬ 1. Первоначальные понятия теории множеств и элементы комбинаторики.**

**Глава 1. Первоначальные понятия теории множеств.**

**§1.** Множество. Подмножество. Пустое множество.

**О.1.** Под *множеством* понимается любая совокупность объектов, называемых элементами множества.

Множества обозначаются большими латинскими буквами (), а их элементы – малыми ().

Если элемент принадлежит множеству , пишут . В противном случае будем писать .

Стандартные обозначения множеств:

 множество всех натуральных чисел,

 множество всех целых чисел,

 множество всех целых чисел, кратных ,

 множество всех рациональных чисел,

множество всех действительных чисел.

**О.2.** Два множества и называются *равными*, если они содержат одни и те же элементы, т.е.

1) если , то ,

2) если , то ,

Обозначается .

**О.3.** Если каждый элемент множества является элементом множества , т.е. если , то , , то говорят, что есть *подмножество* множества . Обозначается: .

Множество называется собственным подмножеством , если и . Обозначается: .

**О.4.** Множество называется *конечным*, если оно содержит конечное число элементов. Число элементов конечного множества называется его *мощностью* и обозначается .

Множество, не содержащее ни одного элемента, называется *пустым* и обозначается . Очевидно, что для любого множества

Способы задания множеств:

1. Перечисление элементов (только для конечных множеств).
2. Указание свойств.

**Пр.1.**  множество натуральных чисел, не превосходящих 6. Тогда

1. , .
2. , .

**§2.** Операции над множествами и их свойства.

Рассмотрим операции над множествами и их свойства.

****О.1.** *Объединением* множеств и называется множество , содержащее элементы, каждый из которых принадлежит хотя бы одному из множеств или .

Свойства объединения:

1. ;
2. ;
3. .

**Пр.1.** Пусть, . Найти .

*Решение.* Рассмотрим

*Ответ:*

**О.2.** *Пересечением* множеств и называется множество , содержащее элементы, каждый из которых принадлежит и множеству и множеству .

Свойства пересечения:

;

;

.

**Пр.2.** Пусть, . Найти .

*Решение.* Рассмотрим

*Ответ:*

**О.3.** *Разностью* множеств и называется множество , содержащее элементы, каждый из которых принадлежит множеству и не принадлежит множеству .

Свойства разности:

;

;

**Пр.3.** Пусть, . Найти

*Решение.* Рассмотрим

*Ответ:*

**О.4.** Если то разность называется *дополнением* множества в .

Свойства дополнения:

;

1. .

Дополнение в обозначается .

**О.5.** Пусть и множества. Пару , где , , будем называть *упорядоченной парой* и считать

*.*

**О.6.** *Декартовым* (*прямым*) произведением множеств и называется множество , содержащее все упорядоченные пары , где , .

**Пр. 4.** Пусть , . Найти

*Решение.* Рассмотрим

*Ответ:*

**Т.1.** Имеют место следующие свойства операций над множествами:

(1) идемпотентность и

(2) коммутативность и

(3)

ассоциативность и

(4)

дистрибутивность относительно и относительно .

(5) ,

(6) , законы де Моргана.

**Пр. 5.** Докажите тождество, проиллюстрируйте его с помощью диаграмм Эйлера-Венна: .

*Решение.* Чтобы доказать равенство двух множеств и , воспользуемся определением 2:

1. Пусть , тогда и . Если . Имеем и , значит , .
2. Пусть , тогда и Если , то . Имеем и , значит , .

Таким образом, .

Проиллюстрируем данное тождество на диаграммах Эйлера-Венна.



**§3.** Отображения и их свойства. Композиция отображений.

**О.1.** Пусть и произвольные множества. *Отображением* множества в множество называют всякое правило , по которому каждому элементу множества сопоставляют единственный элемент множества . Обозначается: .

Если элементу сопоставлен элемент , то называют образом элемента , а прообразом элемента , при отображении и обозначают .

**З.1.** Из О.1.следует, что существует единственный образ. Но для прообразов может быть много или не быть совсем.

**О.2.** Отображение называется:

1) *сюръективным* (или *сюръекцией*), если каждый элемент из является образом хотя бы одного элемента из , т.е.

или

2) *инъективным* (или *инъекцией*), если образы различных элементов множества являются различными элементами множества , т.е.

если , то



3) *биективным* (или *биекцией*), или взаимно однозначным отображением на , если оно сюръективно и инъективно, т.е.



**Пр.1.**

1. по правилу



сюръеция:

 не инъекция: , но .

 по правилу



инъекция:

 не сюръекция:

 по правилу

 инъекция, т.к.

сюръекция, т.к.

Следовательно, биекция, обозначается .

**О.3.** Отображения и называются *равными*, если

**О.4.** *Композицией* отображений и называется отображение , такое что

**

**Св-во 1.** Если , , , то

□ Доказательство см. в [4, глава 1, §2, утверждение 1, с. 14]. ■

**Св-во 2.** Если , сюръективны (инъективны/биективны), то сюръективно (инъективно/биективно).

□ Доказательство см. в [4, глава 1, §2, утверждение 2, с. 14]. ■

**Св-во 3.** Пусть . Если сюръективно, то сюръективно; если инъективно, то инъективно.

□ Доказательство см. в [4, глава 1, §2, утверждение 3, с. 15]. ■

**О.5.** Отображение называется *обратимым*, если

и .

Отображение называется *обратным* для .

**Т.1.** Отображение обратимо биекция

□ Доказательство см. в [4, глава 1, §2, утверждение 4, с. 15]. ■

**Глава 2. Элементы комбинаторики.**

**§1.** Подстановки.

**О.1.** Пусть . Обозначим через множество всех биекций множества на себя. Элементы из называются *подстановками* степени *n*.

Подстановки удобно записывать в виде таблицы, состоящей из двух строк, заключенных в скобки. В первой строке записываются элементы множества , во второй – соответствующие им образы.

Итак, пусть , тогда

,

где .

Отметим, что поскольку при перестановке любых двух столбцов таблицы отображение множества на себя не изменится, то в дальнейшем будем рассматривать подстановки с упорядоченной по возрастанию первой строкой, т.е.

,

где .

**Т.1.** Число различных подстановок степени *n* равно *n*!, т.е.

**Пр.1.** Множество всех подстановок степени 3.

**О.2.** Пусть . *Произведением* подстановок и называется отображение по правилу:

Так как биекции, то по свойству 2 §3 .

**Пр.2.** Пусть .

*Решение.* .

*Ответ:* .

**Св-во 1.**

**Св-во 2.** При  .

**О.3.** Подстановка называется *единичной* или *тождественной*.

**О.4.** Подстановка называется *обратной* к подстановке .

**Пр.2.** Пусть . Найти .

*Решение*. .

*Ответ:* .

**Пр.3.** Найти , если и

.

*Решение.* Выразим из уравнения . Умножим его на слева:

*,* , .

Теперь умножим последнее равенство на справа:

, , .

Найдем и :

Выполним умножение подстановок :

*Ответ:.*

.

**§2.** Четная и нечетная подстановки. Транспозиции. Разложение подстановки в произведение транспозиций.

**О.1.** Рассмотрим подстановку

,

где , , …, .

Вторая строка , …, этой подстановки образует перестановку на *n* символах. Будем говорить, что и образуют *инверсию* , , если:

> и стоит в перестановке раньше .

Подстановка называется *нечетной*, если она имеет нечетное число инверсий; *четной* – четное число инверсий. Тождественную подстановку, которая имеет 0 инверсий, считают четной.

**Пр.1.** Определить четность подстановки .

*Решение.* Определим число инверсий во второй строке подстановки

, , , ,

, .

Число инверсий 7 – нечетное, значит и подстановка нечетная.

*Ответ:* нечетная.

**О.2.** Подстановка, в которой меняются местами только два элемента, а все остальные остаются в естественном порядке

называется *транспозицией*. Обозначается:

Можно показать, что четность подстановки совпадает с четностью числа множителей в ее разложении в произведении транспозиций.



**Пр.2.**

**Т.1.** Число инверсий в любой транспозиции равно

,

где число символов, расположенных между и . Т.о. любая транспозиция является нечетной подстановкой.

**Т.2.** Подстановка, обратная к транспозиции, совпадает с ней самой.

Можно показать, что четность подстановки совпадает с четностью числа множителей в ее разложении в произведении транспозиций.

**Пр.3.** Разложить в произведение транспозиций и определить четность

.

*Решение.* Будем производить транспозиции в тождественной подстановке, пока не получим

,

значит Так как число транспозиций в разложении подстановки четно, то и сама подстановка четная.

*Ответ:* четная подстановка.

**§3.** Разложение подстановки в произведение независимых циклов.

**О.1.** Рассмотрим подстановку .

Будем выписывать последовательное перемещение символов в этой подстановке, начиная с 1 до тех пор, пока снова не получим 1:

.

Если множество всех символов, входящих в эту последовательность, совпадет с {1, 2, …, *n*}, то подстановка называется циклом.

В противном случае выбираем наименьшее натуральное число , но не принадлежащее последовательности, и, начиная с *k*, построим новую последовательность:

.

Такие перемещения символов будем называть *циклами*, а число различных элементов в каждом цикле – *длиной цикла*.

Так как любые два цикла не содержат общих элементов, то их называют *независимыми*. Любую подстановку можно однозначным образом разложить в произведение независимых циклов.

**О.2.** Пусть и число независимых циклов в . Число называется декрементом подстановки .

Несложно показать, что четность числа совпадает с четностью самой подстановки, и равен минимальному числу множителей в разложении этой подстановки в произведение транспозиций.

**Пр.1.** Определить четность подстановки, используя декремент. Разложить в произведение минимального числа транспозиций.

*Решение.* Будем выписывать последовательные перемещения символов в подстановке, начиная с 1:

, первый цикл

, второй цикл

, третий цикл

, четвертый цикл

, пятый цикл

Таким образом, Декремент нечетное число, значит и подстановка нечетная.

*Ответ:* нечетная подстановка.

**МОДУЛЬ 2. Числовые множества.**

**Глава 1.** **Теория делимости целых чисел.**

**§1.** Отношение делимости целых чисел и его свойства.

**О.1.** Пусть . Говорят, что *делится на* и пишут , если существует , такое что Можно также говорить, что *делит* и записывать

Число называется *кратным* числа , – *делителем* числа , – *частным* от деления на .

Рассмотрим несколько важных свойств делимости.

**Св-во 1.** , .

□ Доказательство см. в [1, глава 1, §1, с. 5, св. 1]. ■

**Св-во 2.** ПустьЕсли и , то .

□ Доказательство см. в [1, глава 1, §1, с. 5, св. 2]. ■

**Св-во 3.** Если и , то .

□ Доказательство см. в [1, глава 1, §1, с. 6, св. 4]. ■

**Св-во 4.** Если , то .

□ Доказательство см. в [1, глава 1, §1, с. 5, св. 5]. ■

**Св-во 5.** Если , , и , , то .

**Св-во 6.** , .

□ Доказательство см. в [1, глава 1, §1, с. 6, св. 7]. ■

**Св-во 7.** , .

□ Доказательство см. в [1, глава 1, §1, с. 6, св. 8]. ■

**Св-во 8.** Если , , то .

□ Доказательство см. в [1, глава 1, §1, с. 6, св. 10]. ■

**Св-во 9.** Если и , то .

□ Доказательство см. в [1, глава 1, §1, с. 6, сл.2]. ■

**§2.** Теорема о делении с остатком.

**Т.1 (о делении с остатком)**. Пусть , . Тогда : , причем . Кроме того, числа и определены однозначно.

□ Доказательство см. в [1, глава 1, §1, с. 7, теорема 1]. ■

**О.1.** Число называется *неполным частным*, а – *остатком* от деления на .

**Пр.1.** Выполните деление с остатком: –140 на 47.

*Решение.* Рассмотрим дробь . Ясно, что . Умножив все части данного неравенства на знаменатель 47, получим

.

Отнимаем из всех частей двойного неравенства его левую часть, имеем:

 или

, где .

Таким образом, , причем и

*Ответ:* .

**Пр.2.** Доказать, что , .

*Решение*. Любое при делении на 2 может давать остаток 0 или 1, т.е. иметь вид или , где соответственно.

Пусть , тогда

 Пусть , тогда

Следовательно, , .

**§3.** Наибольший общий делитель (НОД) и его свойства.

**О.1.** Пусть . Число называется *общим делителем* этих чисел, если , , …, .

**О.2.** Число называют *наибольшим общим делителем* чисел , если:

 (1) – общий делитель этих чисел;

 (2) делится на любой общий делитель этих чисел.

Обозначается: или .

Рассмотрим несколько важных свойств НОД.

**Св-во 1.** Если и , то .

□ Пусть . Так как общий делитель и , то по О.2 , т.е. . Отсюда . Аналогично из условий и общий делитель и имеем Таким образом, . ■

□ Доказательство см. в [1, глава 1, §2, с. 8, теорема 1]. ■

**З.1.** Так как все НОД отличаются друг от друга только знаками, условимся считать под НОД натуральное значение.

Например, общими делителями числе и является и , а .

**§4.** Алгоритм Евклида. Линейное представление НОД.

**Л. 1.** Если то

□ Доказательство см. в [1, глава 1, §2, с. 9, лемма 1]. ■

**Л. 2.** Если где , то

□ Доказательство см. в [1, глава 1, §2, с. 8, теорема 1]. ■

Алгоритм Евклида описывает способ нахождения НОД двух , .

Пусть , . Так как , то по лемме 1 .

Пусть , . Далее будем действовать по шагам:

1. Выполним деление на с остатком:

, где .

Если , т.е. , то по лемме 1 , т.е. процесс нахождения закончится на первом шаге.

Пусть . Тогда по лемме 2

1. Выполним деление на с остатком:

, где .

Если , т.е. , то по лемме 1 (последний ненулевой остаток).

Пусть . Тогда по лемме 2

1. Выполним деление на с остатком и т.д. Этот процесс не может продолжаться до бесконечности, т.к. все остатки от деления убывают и положительны.

В результате получим систему равенств вида:

Последний ненулевой остаток .

**Пр.1.** Найти , если , .

*Решение.* Применим алгоритм Евклида:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  \_ |  95 | 35 |
|  |  |  |  70 | 2 |
|  |  |  \_ |  35 |  25 |  |
|  |  |  25 | 1 |  |
|  |  \_ |  25 |  10 |  |  |
|  |  20 |  2 |  |  |
|  \_ |  10 | 5 |  |  |  |
|  10 | 2 |  |  |  |
|  |  0 |  |  |  |  |

Последний отличный от нуля остаток равен 5, значит .

*Ответ:* .

**Т.1 (о линейном представлении НОД).** Пусть и . Тогда : – линейное представление .

□ Доказательство см. в [1, глава 1, §2, теорема 6, с. 13]. ■

**Пр.2.** Найти линейное представление , если

, .

*Решение.* Запишем результаты последовательного деления из примера 1:

Для нахождения линейного представления из полученных равенств выражаем последовательно остатки 25, 10 и 5 через *a* = 95 и *b* = 35.

Из первого равенства имеем: .

Тогда из второго равенства: .

Наконец, из третьего равенства: .

Итак, линейное представление

*Ответ:* .

**§5.** Взаимно простые числа.

**О.1.** Пусть Эти числа будем называть взаимно простыми и записывать, если .

Например, .

**Т.1.** Пусть . Тогда

□ Доказательство см. в [1, глава 1, §3, теорема 1, с. 14]. ■

**Т.2.** Пусть . Если , , то .

□ Доказательство см. в [1, глава 1, §3, теорема 3, с. 15]. ■

**Сл.1.** Пусть . Если и , где , то .

□ Доказательство см. в [2, глава 1, §1, предложение 11, с. 12]. ■

**Пр.1.** .

**Т.3.** Пусть . Если и , то .

□ Доказательство см. в [1, глава 1, §3, теорема 5, с. 15]. ■

**§6.** Наименьшее общее кратное (НОК).

**О.1.** Пусть . Число называется *общим кратным* этих чисел, если , , …,

**О.2.** Число называют *наименьшим общим кратным* чисел , если:

 (1) – общее кратное этих чисел;

(2) любое общее кратное этих чисел делится на

Обозначается: или

**Св-во 1.** Если и , то .

□ Доказательство см. в [1, глава 1, §4, с. 17]. ■

**З.1.** В дальнейшем будем выбирать положительное значение НОК.

**Т.1.** Пусть . Тогда .

**Пр.1.** Найти , если , .

*Решение.* Так как , то

*Ответ:* 665.

**§7.** Простые числа. Решето Эратосфена.

**О.1.** Натуральное число называется *простым*, если оно делится либо на само себя, либо на 1, а других делителей у него нет. Числа, которые не являются простыми, называются *составными*.

Т.о.

**Т.1.** Пусть и – простое число. Тогда либо , либо

□ Доказательство см. в [1, глава 1, §4, теорема 4, с. 21]. ■

**Т.2.** Пусть и – простое число. Если , то хотя бы один из множителей ,

□ Доказательство см. в [1, глава 1, §4, теорема 5, с. 21]. ■

В III в. до н.э. греческий математик Эратосфен открыл способ выделения простых чисел из отрезка 1, 2, …, натурального ряда путем вычеркивания числа 1; всех чисел, кратных 2 (кроме 2); затем всех чисел, кратных 3 (кроме 3); и т.д., всех чисел, кратных .

**Пр. 1.** Найти все простые числа, не превосходящие 30.

*Решение.* Выпишем все числа натурального ряда от 1 до 30:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Вычеркнем число 1 – не простое. Оставляем число 2 – простое и вычеркиваем все числа, кратные 2 (каждое второе):

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Оставляем число 3 – простое и вычеркиваем все числа, кратные 3 (каждое третье, считая вычеркнутые):

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Оставляем число 5 – простое и вычеркиваем все числа, кратные 5 (каждое пятое, считая вычеркнутые):

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Так как , то процесс нахождения простых чисел закончен. Итак, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 – все простые числа, не превосходящие 30.

*Ответ:* 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

**Т.1 (Евклид).** Множество простых чисел бесконечно.

□ Доказательство см. в [1, глава 1, §4, теорема 8, с. 24]. ■

**§8.** Разложение составных чисел на простые множители.

**Т.1 (основная теорема арифметики).** Всякое натуральное число либо является простым, либо может быть представлено ив виде произведения простых чисел. Кроме того, это представление единственно с точностью до порядка записи множителей.

□ Доказательство см. в [1, глава 1, §4, теорема 7, с. 22]. ■

**О.1.** Рассмотрим разложение числа на простые множители. Упорядочим это разложение и соберем одинаковые степени:

,

где – различные простые числа, ,

Такое представление числа называют *каноническим.*

Используя канонические представления чисел, можно находить их НОД и НОК. Пусть и

… , … ,

где – различные простые числа; , , .Тогда

… , где ,

 … , где ,

**Пр.1.** Найдите канонические представления чисел, укажите их НОД и НОК: 51597 и 46305.

*Решение.* Разложим числа 1597 и 46305 на простые множители:

Итак, канонические представления чисел 51597 и 46305 имеют вид:

, .

Добавляя в записи чисел недостающие простые множители в нулевой степени, имеем: , .

Отсюда и

 .

*Ответ:* , ,

 ,

**Глава 4. Теория сравнений.**

**§1.** Сравнения и их свойства.

**О.1.** Пусть . Числа и будем называть *сравнимыми по модулю* (), если они имеют при делении на один и тот же остаток . Обозначается: .

Если остатки от деления и на разные, будем записывать: .

**Пр.1.** Выполним деление и на с остатком:

 и .

Тогда определению .

**Т.1.** Пусть . Тогда

□ Доказательство см. в [3, глава 7, теорема 75, с. 72]. ■

**Пр.2.** В примере 1 было установлено, что . И, согласно теореме 1, .

Рассмотрим несколько важных свойств сравнений.

**Св-во 1.**

1. ;
2. если , то ;
3. если и , то .

□ Доказательство см. в [3, глава 7, теоремы 76-78, с. 73]. ■

**Св-во 2.** Если , , то

1. ,
2. ,
3. .

□ Доказательство см. в [3, глава 7, теоремы 83 и 84, с. 74]. ■

**Сл.1.** Если , то

 , .

□ Доказательство см. в [3, глава 7, теоремы 76-78, с. 73]. ■

**Сл. 2.** Если , то , .

□ Доказательство см. в [3, глава 7, теорема 85, с. 75]. ■

**Cл. 3.** Члены сравнения можно переносить из одной части в другую с противоположным знаком.

□ Доказательство см. в [3, глава 7, теорема 87, с. 75]. ■

**Сл. 4.** К обеим частям сравнения можно прибавлять (отнимать) число, кратное модулю.

□ Доказательство см. в [3, глава 7, теорема 88, с. 75]. ■

**Св-во 3.** Если , то , .

□ Доказательство см. в [3, глава 7, теорема 79, с. 73]. ■

**Св-во 4.** Если и , то .

□ Доказательство см. в [3, глава 7, теорема 80, с. 74]. ■

**З.1.** Сокращать обе части сравнения на число, не взаимно простое с модулем, нельзя. Сравнение может получиться как верным, так и нет.

Например, ,

 – верное сравнение.

 **НО** ,

 – неверное сравнение.

**Св-во 5.** Если , то , .

□ Доказательство см. в [3, глава 7, теорема 81, с. 74]. ■

**Св-во 6.** Если , то , .

□ Доказательство см. в [3, глава 7, теорема 82, с. 74]. ■

**Пр.1.** Показать, что .

*Решение.* Имеем . Так как , то, возводя обе части данного сравнения в четвертую степень, получим:

.

Кроме того, . Теперь, почленно перемножая сравнения и , имеем:

**§2.** Классы вычетов по данному модулю.

Множество можно разбить на непересекающихся подмножеств в зависимости от остатка при делении на Эти подмножества называются *классами вычетов* по модулю . Все числа (*вычеты*) принадлежащие одному классу имеют одинаковые остатки при делении на (сравнимы по модулю ).

С помощью этих остатков и будем обозначать классы вычетов:

Остатки от деления на : (представители классов вычетов)

Классы вычетов по модулю :

Заметим, что *,*

 .

□ Доказательство см. в [3, глава 8, теорема 93, с. 78]. ■

Обозначим множество классов вычетов по модулю .

Определим на множестве операции сложения и умножения по правилам:,.

**Пр.1.** Составить таблицы сложения и умножения классов вычетов в .

*Решение.* Множество образуют классы вычетов по модулю 6. Класс вычетов состоит из всех целых чисел, дающих при делении на 6 один и тот же остаток. Поскольку при делении на 6 могут встречаться остатки 0, 1, 2, 3, 4, 5, то состоит из шести классов вычетов:

*,*

*,*

*,*

*,*

*,*

*.*

Таблицы сложения и умножения элементов заполняем по правилу: и , .

Например, . Так как , то . Таким образом, . Аналогично, . Из имеем . Значит, .

В результате получим:

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

**§3.** Полная система вычетов.

**О.1.** *Полной системой вычетов* (ПСВ) по модулю называется совокупность целых чисел, содержащая по одному представителю из каждого класса вычетов по модулю .

 Обычно в качестве представителей берутся:

наименьшие неотрицательные ,

наименьшие положительные

или наименьшие по абсолютной величине

вычеты.

**Пр.1.** Написать все три вида полной системы вычетов по модулю 6.

*Решение.*Множество , где

*,*

*,*

*,*

*,*

*,*

*.*

Если из каждого класса вычетов выбрать по одному представителю – вычету, то получим ПСВ по модулю 6.

Выберем из каждого класса вычетов в качестве представителей:

– наименьшие неотрицательные числа, получим полную систему наименьших неотрицательных вычетов: ;

– наименьшие положительные числа, получим полную систему наименьших положительных вычетов: ;

– наименьшие по абсолютной величине числа, получим полную систему наименьших по абсолютной величине вычетов: .

**Т.1.** Любая совокупность чисел , попарно не сравнимых по модулю , образует ПСВ по модулю .

□ Доказательство см. в [1, глава 3, §2, теорема 1, с. 109]. ■

**Т.2.** Пусть , Если – ПСВ по модулю , то – ПСВ по модулю .

□ Доказательство см. в [1, глава 3, §2, теорема 2, с. 109]. ■

**Пр2.** Показать, что числа 25, 46, 37, –20, –21, –17, 16, 18 составляют ПСВ по модулю 8.

*Решение.* Разделим каждое данное число на модуль 8 с остатком:

, , , ,

, , , .

Полученные остатки 0, 1, 2, 3, 4, 5, 6, 7 все различны и составляют полную систему наименьших неотрицательных вычетов по модулю 8. Следовательно, числа 25, 46, 37, –20, –21, –17, 16, 18 составляют ПСВ по модулю 8.

**§4.** Приведенная система вычетов.

**Л.1.** Все числа из имеют с один и тот же НОД, т.е. если , то

□ Доказательство см. в [1, глава 3, §3, теорема 1, с. 113]. ■

**З.1.** В виду Л.1 вместо можно писать .

**О.1.** Если , то класс вычетов называется *классом вычетов, взаимно простым* с .

**О.2.** *Приведенной системой вычетов* (ПрСВ) по модулю называется совокупность вычетов по модулю , взятых по одному из каждого взаимно простого с класса вычетов.

Чтобы составить ПрСВ по модулю нужно выписать ПСВ по модулю и выбрать из нее вычеты, взаимно простые с .

**Пр.1.** Написать все три вида приведенной системы вычетов по модулю 6.

*Решение.*Множество , где

*,*

*,*

*,*

*,*

*,*

*.*

В примере 1 §3 получены ПСВ по модулю 6:

ПСВ наименьших неотрицательных вычетов: ;

ПСВ наименьших положительных вычетов: ;

ПСВ наименьших по абсолютной величине вычетов: .

ПрСВ состоит из представителей классов вычетов, взаимно простых с модулем 6. Взаимно простыми с модулем 6 будут:

– среди наименьших неотрицательных вычетов числа, значит – приведенная система наименьших неотрицательных вычетов;

– среди наименьших положительных вычетов числа , значит – приведенная система наименьших положительных вычетов;

– среди наименьших по абсолютной величине вычетов числа , значит – приведенная система наименьших по абсолютной величине вычетов.

Пусть число классов, взаимно простых с равно .

**Т.1.** Любаясовокупность чисел , попарно не сравнимых по модулю и взаимно простых с , есть ПрСВ по модулю .

□ Доказательство см. в [1, глава 3, §3, теорема 2, с. 114]. ■

**Т.2.** Пусть . Если – ПрСВ по модулю , то – ПрСВ по модулю .

**Пр. 2.** Показать, что числа 19, 23, 25, –19 составляют ПрСВ по модулю 12.

*Решение.* Разделим каждое данное число на модуль 12 с остатком:

, , , ,

Полученные остатки 1, 5, 7, 11 все различны и составляют приведенную систему наименьших неотрицательных вычетов по модулю 12. Следовательно, числа 19, 23, 25, –19 составляют ПрСВ по модулю 12.

**§5.** Обратимые элементы во множестве классов вычетов.

**О.1.** Элемент называется *обратимым*, если

**Т.1.** Элемент обратим

□ Доказательство см. в [1, глава 3, §3, теорема 3, с. 114]. ■

**З.1.** Множество всех обратимых элементов совпадает с множеством всех классов, взаимно простых с , и обозначается .

**Пр.1.** Найти .

*Решение.* Множество , где

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

Для каждого найдем обратный элемент, т. е. такой элемент , что . Из таблицы умножения видно:

, т. е. – обратный элемент для ,

, т. е. – обратный элемент для .

Поскольку не существует , такого что , то для не существует обратного элемента в . Аналогично, обратных элементов не существует для классов вычетов и .

*Ответ:* , – обратимые элементы .

**§6.** Функция Эйлера.

**О.1.** Обозначим через число классов вычетов по модулю , взаимно простых с , т.е. число элементов ПрСВ по модулю . Функцию называют функцией Эйлера.

Выберем в качестве представителей наименьшие положительные вычеты . Тогда число натуральных чисел, не превосходящих и взаимно простых с .

**Т.1.** Если – простое число, то .

□ Доказательство см. в [1, глава 3, §3, с. 117]. ■

**Т.2.** Если , где – простое число и , то

.

□ Доказательство см. в [1, глава 3, §3, с. 118]. ■

**Т.3.** Если , то .

□ Доказательство см. в [1, глава 3, §3, теорема 1, с. 118]. ■

**Т.4.** Если – каноническое представление числа , то .

□ Доказательство см. в [1, глава 3, §3, с. 118]. ■

**Пр.1.** Найдите функцию Эйлера для чисел: 1) 7; 2) 16; 3) 63000.

*Решение.* 1) Поскольку – простое число, то по теореме 1:

.

1. Найдем каноническое представление числа 16: . Используя теорему 2, получим:

.

1. Найдем каноническое представление числа 63000:

.

По теореме 4 имеем:

Заметим, что вычислять можно было и по теореме 3, используя свойство мультипликативности функции Эйлера.

*Ответ:* 1) 6; 2) 12; 3) 14 400.

**§7.** Теоремы Эйлера и Ферма.

**Т.1 (Эйлерa).** Для любого , , верно

.

□ Доказательство см. в [3, глава 11, теорема 120, с. 97]. ■

**Т.2 (Ферма).** Пусть , – простое число, . Тогда

.

□ Доказательство см. в [3, глава 11, теорема 119, с. 97]. ■

**Сл.1.** Пусть , – простое число. Тогда

.

□ Доказательство см. в [3, глава 11, теорема 119’, с. 97]. ■

**Пр.1.** Найти остаток от деления: на 15.

*Решение.* Так как , то применяем теорему Эйлера:

.

Вычислив , имеем

.

Возьмем очевидное сравнение . Тогда

.

Но, возводя обе части сравнения в тридцать вторую степень, получим:

.

Кроме того, .

Теперь почленно перемножаем сравнения и :

 .

*Ответ:* 8.

**Глава 5.** **Комплексные числа.**

**§1.** Определение комплексных чисел. Алгебраическая форма записи комплексного числа.

**О.1.** *Комплексными числами*называются упорядоченные пары , для которых:

I.

II.

III.

IV.

**О.2.** Обозначит . Тогда, где*.*Выражение называется *алгебраической формой записи* комплексного числа .

Пусть . Тогда называется *действительной частью* числа и обозначается , *мнимой частью* числа и обозначается , называется *мнимой единицей*.

**О.3.** Комплексное число называется *сопряженным* числу . Обозначается: .

Операции над комплексными числами в алгебраической форме:

1. Сложение:

.

1. Вычитание:

.

1. Умножение (:





1. Деление:

**З.1.** Пусть Рассмотрим произведение

.

**Пр.1.** Записать и в алгебраической форме, найти , , , , ,, , .

*Решение.* Представим в алгебраической форме:

, где , .

Представим в алгебраической форме:

, где , .

Теперь выполним операции над комплексными числами:

1)

2)

3)

**

4)

*Ответ:* , , .

 , , .

,, , .

**Т.1.** Для любых верно:

1. .

□ Доказательство см. в [2, глава 2, §2, c. 30]. ■

**§2.** Тригонометрическая форма записи комплексного числа.

**О.1.** Возьмем на плоскости декартову систему координат и изобразим на ней комплексное число точкой

****

Плоскость, на которой изображаются комплексные числа, называется *комплексной*. Ось абсцисс называется *действительной* осью, а ось ординат – *мнимой*.

**О.2.** Длина отрезка называется *модулем* комплексного числа и обозначается .

**О.3.** Угол , на который нужно повернуть ось до совпадения ее направления с направление вектора , называется *аргументом* числа и обозначается Положительным направлением отсчета аргумента считается направление против часовой стрелки.



**З.1.** Аргумент комплексного числа определен неоднозначно, т.е. угол может быть отсчитан несколькими способами. Пусть наименьшее положительное значение аргумента. Тогда все возможные значения аргумента: .

**О.4.** Пусть , , , .

 Тогда . Такая форма числа называется *тригонометрической*.

**Пр.1.** Записать числа в тригонометрической форме.

1. ,

*Решение.*

** ,

1. Так как , то
2. Сначала найдем модуль . Из по теореме Пифагора

Теперь найдем аргумент :Из

, значит .

Поэтому и

1. Так как , то

*Ответ:* (1) (2)

**§3.** Операции над комплексными числами в тригонометрической форме.

Рассмотрим операции над комплексными числами в тригонометрической форме.

Пусть , . Тогда

1. , т.е. при умножении комплексных чисел в тригонометрической форме их модули умножаются, а аргументы складываются.

□ Доказательство см. в [2, глава 2, §2, п.5, c. 36]. ■

(2) . Если , то имеем формулу Муавра:.

□ Доказательство см. в [2, глава 2, §2, п.6, c. 36]. ■

(3) , т.е. при делении комплексных чисел в тригонометрической форме их модули делятся, а аргументы вычитаются.

□ Доказательство см. в [2, глава 2, §2, п.5, c. 36]. ■

(4) , .

□ Доказательство см. в [2, глава 2, §3, п.2, c. 40]. ■

**З.1.** Все значения лежат на окружности с центром в начале координат радиуса и делят окружность на *n* равных частей.

**З.2.** Операции сложения и вычитания комплексных чисел в тригонометрической форме не рассматриваем, поскольку их легче выполнять с комплексными числами, записанными в алгебраической форме.

**Пр.1.** Записать числа в тригонометрической форме и найти , и .

*Решение.* В примере 1 §2 получено, что

и

Теперь выполним над ними указанные операции:

.

.

1. ,

Пусть , тогда

.

Пусть , тогда

.

Пусть , тогда

.

Пусть , тогда

.

*Ответ:* , ,

 , ,, .

**МОДУЛЬ 3. «Основные алгебраические структуры».**

**Глава 6.** **Множества с бинарными операциями.**

**§1.** Бинарная алгебраическая операция.

**О.1.** Пусть *M* – множество. Говорят, что на *М* задана *бинарная алгебраическая операция* φ, если задано отображение , т. е. любой упорядоченной паре элементов из *M* соответствует однозначно определенный элемент

Части вместо пишут , еще чаще бинарную операцию (б.о.) обозначают специальным символом: \*, ∘, +, · и т.д.

**Пр.1.** Является ли б.о. закон на множестве ? На множестве ?

*Решение.* Если , то для любых имеем , причем является однозначно определенным натуральным числом. Следовательно, ○ – бинарная операция на множестве.

Пусть . Тогда но . Таким образом, ○ не является бинарной операцией на множестве *M*.

*Ответ:* является б.о. на множестве и не является б.о. на множестве *M* = {1,2}.

Б.о. на конечном множестве удобно записывать в виде таблицы.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ○ | *a* | *b* | … | *v* |
| *a* | *a*○*a* | *a*○*b* | … | *a*○*v* |
| *b* | *b*○*a* | *b*○*b* | … | *b*○*v* |
|  | … | … | … | … |
| *v* | *v*○*a* | *v*○*b* | … | *v*○*v* |

Таблицы такого вида называются *таблицами Кэли*.

**О.2.** Б.о. ○ на множестве *M* называется *ассоциативной*, если и

 *коммутативной,* если

**Пр.2.** Является ли б.о. на множестве коммутативной? Ассоциативной?

*Решение.* Так как , то бинарная операция ○ не является коммутативной на . Поскольку , то бинарная операция ○ не является ассоциативной на .

*Ответ:* не коммутативна, не ассоциативна.

**З.1.** Если б.о. задана с помощью таблицы Кэли, то коммутативность операции легко извлечь из симметричности таблицы.

**§2.** Нейтральный и симметричный элементы множества. Группоид. Полугруппа. Моноид.

**О.1.** Пусть *M* – непустое множество и ○ – б.о. на *М*. Элемент () называется *левым* (*правым*) *нейтральным элементом* относительно б.о. ○ на *M*, если

**О.2.** Если некоторый элемент является одновременно левым и правым нейтральным элементом относительно б.о. ○ на *М*, т. е.

то его называют *нейтральным элементом*.

**Пр.1.** Найти правый и левый нейтральные элементы относительно б.о. ○ на , если ,

*Решение.* Найдем правый нейтральный элемент относительно бинарной операции ○ на , т. е. такой , что По определению операции ○: Отсюда является правым нейтральным элементом относительно бинарной операции ○ на .

Найдем теперь левый нейтральный элемент относительно бинарной операции ○ на , т. е. такой , что. По определению операции ○: Несложно убедиться, что ни одно натуральное число не обладает таким свойством. Следовательно, левого нейтрального элемента относительно бинарной операции ○ на не существует.

*Ответ:* правый нейтральный элемент относительно б.о. ○ на , левого нейтрального элемента относительно б.о. ○ на не существует.

**Т.1.** Если множество *M* обладает левым и правым нейтральными элементами относительно б.о. ○ на *M*, то они совпадают между собой. В частности, если в *М* существует нейтральный элемент относительно б.о. ○, то он в *М* единственен.

□ Доказательство см. в [5, §1, лемма 1.1]. ■

**О.3.** Пусть *M* – непустое множество и *e* – нейтральный элемент относительно б.о. ○ на *М*.

Элемент называется *правым* (*левым*) *симметричным элементом* для , если

**Т.2.** Пусть *M* – непустое множество, *e* – нейтральный элемент в *М* относительно б.о. ○ и операция ○ ассоциативна на *М*. Если элемент имеет в *M* правый и левый симметричные элементы относительно б.о. ○, то они совпадают между собой. В частности, если для элемента в *M* существует симметричный элемент относительно б.о. ○, то он в *M* единственен.

□ Доказательство см. в [5, §1, лемма 1.1]. ■

**Пр.2.** Найти симметричные элементы для всех элементов множества ℕ относительно б.о. ○ на ℕ, заданной по правилу:

*Решение.* Нейтральным элементом относительно бинарной операции ○ на является . Действительно,

Для Следовательно, операция ○ ассоциативна на .

 Так как , то для симметричным элементом относительно бинарной операции ○ на является 1. Однако в множестве любое число *x* > 1 не обладает симметричным элементом относительно бинарной операции ○, так как

*Ответ:* симметричный элемент для относительно б.о. ○ на , остальные элемент из симметричными элементами не обладают.

**О.4.** Непустое множество *M* с заданной на нем б.о. ○ называется *группоидом*. Обозначается: (*M*,○).

**О.5.** Если (*M*,○) является группоидом и б.о. ○ ассоциативна на *M*, то группоид *M* называется *полугруппой*.

**О.6.** Если (*M*,○) является полугруппой и *M* обладает нейтральным элементом относительно б.о. ○, то полугруппа *M* называется *моноидом*.

**Пр.3.**

1. Пусть с заданной на нем б.о.: ,

Тогда является группоидом,

 не является полугруппой, т.к. б.о. не ассоциативна.

1. Пусть с заданной на нем б.о. :

Тогда является группоидом,

 является полугруппой,

 является моноидом.

**Т.1.** В полугруппе произведение элементов, где , не зависит от расстановки скобок и, значит, их вообще можно опустить.

□ Доказательство см. в [5, §1, теорема 1.1]. ■

**§3.** Группа. Примеры групп. Порядок элемента группы.

**О.1.** Непустое множество *G*, с заданной на нем бинарной операцией ○, называется *группой*, если выполняются следующие условия (аксиомы):

1) операция ○ ассоциативна на множестве *G*, т. е.

2) в *G* существует нейтральный элемент *e*, т. е.

3) каждый элемент в *G* обладает симметричным элементом в *G*, т. е.

 Вместо общей формы записи операции ○ в теории групп принято использовать обозначения операций:

+ – сложение (аддитивная форма записи) и

 ∙ – умножение (мультипликативная форма записи).

|  |  |
| --- | --- |
| (*G*,+) | (*G*,∙) |
| 1) ассоциативность:2) нейтральный элемент обозначают 0 и называют *нулевым* (*нулем*):3)симметричный элемент обозначают –*a* и называют *противоположным*:*G*  ̶ *аддитивная* группа. | 1) ассоциативность:2) нейтральный элемент обозначают 1 и называют *единичным* (*единицей*):3)симметричный элемент обозначают *a*–1 и называют *обратным*:*G* ̶ *мультипликативная* группа.­ |

**О.2.** Если б.о. ○ коммутативна на *G*, то группу (*G*,○) называют *абелевой*.

**О.3.** Если множество *G* состоит из конечного числа элементов, то группа (*G*,○) называется *конечной*. Число элементов конечной группы *G* будет обозначать |*G*| и называть *порядком* этой группы. Если множество *G* бесконечно, то группу (*G*,○) называют *бесконечной*.

**Пр.1.** Приведем примеры групп.

1. бесконечные аддитивные абелевы группы.
2. Множество всех классов вычетов по модулю конечная аддитивная абелева группа ():
3. Б.о. + ассоциативна на :

: .

1. нулевой элемент в :

 .

1. противоположный для ;

 .

1. Б.о. + коммутативна на :

 .

1. Множество всех подстановок степени *n* конечная мультипликативная группа ():
2. Б.о. ассоциативна на по св-ву 1§3 главы 1.
3. единичный элемент в :

.

Аналогично, .

1. обратный элемент для

 :

.

Аналогично, .

Группу называют *симметрической* группой степени . не абелева, т.к. б.о. не коммутативна.

(4) Множество всех комплексных чисел является бесконечной абелевой группой. Множество бесконечной мультипликативная абелева группа.

□ Доказательство см. в [2, глава 2, §1, с. 29]. ■

**Пр.2.** Пусть . Докажите, что является группой относительно операции , если

*Решение.* Пусть . Тогда , значит , и б.о. на множестве . Проверим выполнение всех аксиом группы:

1. Ассоциативность операции :

(\*)

(\*\*)

Так как правые части равенств (\*) и (\*\*) равны, то .

1. Существование нейтрального элемента относительно б.о. .

Найдем По определению операции

правый нейтральный элемент относительно б.о. .

Покажем, что является также левым нейтральным элементом относительно б.о. . Действительно, *.*

1. Существование для каждого элемента из симметричного относительно б.о. . Пусть . Найдем По определению операции :

Если бы то , откуда что невозможно. Поэтому , и левый нейтральный элемент для относительно б.о. . Покажем, что является и правым нейтральным элементом. Действительно,

Таким образом, является группой относительно операции .

В дальнейшем, если не оговорено противное, будем рассматривать мультипликативную форму записи и обозначение операции **·** опускать.

**О.4.** Пусть – элемент группы. Если существует , такой что , причем *n* является наименьшим натуральным числом с таким свойством, то *n* называют порядком элемента *a* и обозначают *.*

Если такого натурального числа не существует, то называется элементом бесконечного порядка и обозначают:

Полагаем, что и

Несложно доказать, что

 и

**Пр.2.** Найти порядки элементов в следующих группах:

1. аддитивная абелева группа, .
2. аддитивная абелева группа.
3. симметрическая группа 8 степени.
4. мультипликативная группа.

*Решение.* (1) Пусть . Если , то из, следует, что . Пусть . Так как то

1. Рассмотрим группу :

Так как , то

Так как , то

Так как , то

Так как , то

Так как , то

Так как , то

1. Пусть симметрическая группа 8 степени и

Порядок подстановки равен НОК длин циклов в разложении этой подстановки в произведение независимых циклов. Так как

 , то

 Рассмотрим мультипликативную группу , . Так как то

*Ответ:* (1) , .

(2)

 (3) .

 (4)

**§4.** Подгруппа. Критерий подгруппы. Изоморфизм групп.

**О.1.** Пусть группа и . Если является группой относительно той же операции, которая задана на , то называется *подгруппой* группы и обозначается .

Если , то подгруппу называют собственной подгруппой в и обозначают .

Отметим, что каждая группа *G* обладает единичной подгруппой и подгруппой *G*. Эти подгруппы называют *тривиальными*.

**З.1.** Очевидно, что не всякое является подгруппой в *G*. Например, группа, , но .

**Т.1. (критерий подгруппы).** Пусть*G* – группа и . Тогда *H* является подгруппой в *G* выполняются следующие условия:

(1)

(2)

□ Доказательство см. в [5, §1, лемма 1.3]. ■

**Пр.1.** Множество всех четных подстановок образуют подгруппу симметрической группы Группу будем называть *знакопеременной группой*, .

**З.2.** Нечетные подстановки в произведении дают четную подстановку, поэтому множество нечетных подстановок не является подгруппой группы

**Пр.2.** Пусть группа относительно операции : (см. пример 2 §3). Является ли множество c заданной на нем операцией , подгруппой группы

*Решение.* Будем использовать критерий подгруппы:

1. *.*
2. Возьмем , тогда

Следовательно, не является подгруппой группы .

*Ответ:* нет.

**О.3.** Пусть заданы две группы(*G*1,○) и (*G*2,\*). Группы *G*1 и *G*2 будем называть *изоморфными* и записывать *G*1*G*2, если существует биективное отображение : *G*1→ *G*2, называемое *изоморфизмом*, для которого сохраняется операция, т. е.

**Пр.3.** Пусть , . Тогда .

*Решение.* Зададим отображение по правилу . Сначала покажем, что биекция. Действительно,

1) 5, т.е. инъекция.

2) Так как , то сюръекция.

Теперь проверим сохранение операции: :

Таким образом, изоморфизм и .

**§4.** Кольцо. Подкольцо. Критерий подкольца. Характеристика кольца. Обратимые элементы кольца.

**О.1.** Непустое множество с заданными на нем б.о. + и называется кольцом, если выполняются следующие условия (аксиомы):

1) аддитивная абелева группа (аддитивная группа кольца);

2) б.о. дистрибутивна на относительно +, т.е.

 и

Следствия из аксиом кольца:

**Сл.1.**

□ Доказательство см. в [5, глава 1, §3, с. 14]. ■

**Сл.2.**

□ Доказательство см. в [5, глава 1, §3, с. 14]. ■

**Сл.3.**  и

□ Доказательство см. в [5, глава 1, §3, с. 14]. ■

**О.2.** Кольцо называется *коммутативным*, если б.о. коммутативна на , т.е.

Кольцо называется *ассоциативным*, если б.о. ассоциативна на , т.е.

**О.3.** Кольцо называется *кольцом с единицей*, если

Также, как и для мультипликативной группы, доказывается, что в кольце не может быть двух различных единиц (но может не быть ни одной).

**О.4.** Говорят, что кольцо *имеет делители нуля*, если

Если таких элементов нет, то кольцо без делителей нуля.

**О.5.** Коммутативное ассоциативное кольцо с единицей и без делителей нуля называется *областью целостности*.

**Пр.1.** Приведем примеры колец.

1. области целостности относительно б.о. + и .

□ Доказательство для см. в [2, глава 1, §3, с. 29]. ■

(2) Множество всех классов вычетов по модулю коммутативное и ассоциативное кольцо с единицей.

1) аддитивная абелева группа; (см. пр. 1, §3)

2) операция дистрибутивна относительно +: :

.

3) операция коммутативна и ассоциативна;

.

: .

4) единица кольца

 .

Если составное число, то имеет делители нуля. Например, , , но . Если простое число, то кольцо без делителей нуля.

**Пр.2.** Доказать, что множество является кольцом относительно бинарных операций и :

, .

Является ли кольцо коммутативным, ассоциативным, с единицей, имеет ли делители нуля?

*Решение.* Проверим все аксиомы кольца:

, т.е. б.о. на

.

Значит б.о. коммутативна на .

1. :

Значит б.о. ассоциативна на .

1. Найдем . По определению операции

, отсюда

Значит нейтральный элемент на .

1. Пусть . Найдем По определению операции

, отсюда

Значит симметричный элемент для .

Из пунктов 1)-4) следует, что абелева группа.

, т.е. б.о. на

1. :

 и

.

Из пунктов 1)-4) следует, что кольцо относительно бинарных операций и .

1. Так как в общем случае для

,

то кольцо б.о. не коммутативна на , значит, кольцо не коммутативно.

1. :

Значит б.о. ассоциативна на , и колько ассоциативно.

1. Найдем

По определению операции

, отсюда

Так как в общем виде , то не является кольцом с единицей.

1. Приведем примеры делителей нуля в кольце

, , : .

Значит кольцо с делителями нуля.

**О.6.** Пусть коммутативное ассоциативное кольцо с единицей. Если существует , такой что , причем *n* является наименьшим натуральным числом с таким свойством, то *n* называют характеристикой кольца и обозначают *.*

Если такого числа не существует, то говорят, что кольца имеет характеристику 0 и пишут: *.*

**Пр.3.** Найти:

(1) .

(2) .

*Решение.* (1) Рассмотрим кольцо . Так как , , то Аналогично,

(2) Рассмотрим кольцо . Так как

, то

*Ответ:* (1) (2)

**О.7.** Пусть кольцо и . Если является кольцом относительно тех же операций, которые заданы на , то называется *подкольцом* кольца .

**Т.1. (критерий подкольца).** Пусть кольцо и . Тогда является подкольцом ввыполняются следующие условия:

(1)

(2)

□ Доказательство см. в [5, глава 1, §4, с. 18]. ■

**Пр.4.** Показать, что является подкольцом кольца относительно бинарных операций и (см. пример 2):

, .

*Решение.* Так как , то . Будем использовать критерий подкольца:

1.
2. .

Следовательно, подкольцо кольца .

**О.8.** Пусть коммутативное и ассоциативное кольцо с единицей. Элемент называется *обратимым*, если

**Т.2.** Множество обратимых элементов коммутативного и ассоциативного кольца с единицей образует мультипликативную абелеву группу

**Пр.5.** Найти обратимые элементы:

(1) кольца . (2) кольца .

*Решение.* (1) Рассмотрим кольцо . Пусть . Если , то из следует, что Пусть . Так как не существует , то Итак,

(2) Рассмотрим кольцо . Так как обратим то .

Ответ: (1) (2).

**§5.** Поле. Подполе. Критерий подполя.

**О.1.** Непустое множество с заданными на нем б.о. + и называется *полем*, если выполняются следующие условия (аксиомы):

1) аддитивная абелева группа;

2) мультипликативная абелева группа;

3) б.о. дистрибутивна на относительно +, т.е.

Можно дать следующее эквивалентное определение.

**О.2.** *Полем* называется коммутативное ассоциативное кольцо с единицей, в котором всякий ненулевой элемент обратим.

Рассмотрим свойства поля.

**Св-во 1.** Любое поле содержит по крайней мере два различных элемента: 0 и 1.

□ Доказательство см. в [5, глава 1, §4, с. 16]. ■

**Св-во 2.** Любое поле не имеет делителей нуля.

□ Доказательство см. в [5, глава 1, §4, с. 16]. ■

**Пр. 1.** Рассмотрим примеры полей.

1. поля; кольцо не является полем, т.к. в нем обратимы только и .

□ Доказательство для см. в [2, глава 1, §3, с. 29]. ■

(2) Кольцо классов вычетов является полем тогда и только тогда, когда простое число. Поскольку в этом случае любой ненулевой будет обратим (см. теорему 1, §5, гл. 4). Если же составное число, то в есть делители нуля.

**О.4.** Пусть поле и . Если является полем относительно тех же операций, которые заданы на , то называется *подполем* поля .

**Пр. 2.** Так как поля (см. пример 1) и , то

 подполе поля , подполе поля , подполе поля

**Т.2. (критерий подполя).** Пусть поле и . Тогда является подполем полявыполняются следующие условия:

(1)

(2)

**Пр. 3.** Является ли подполем поля комплексных чисел ?

*Решение.* Очевидно, что . Будем использовать критерий подполя:

1. Пусть тогда , и

.

1. Пусть , тогда , , , и

.

Следовательно, не является подполем поля .

*Ответ:* нет.

**Литература:**

1. Алгебра и теория чисел: Учеб. пособие для студентов-заочников II курса физ.-мат. фак. пед. ин-ов / Н.А. Казачек, Г.Н. Перлатов, Н.Я. Виленкин и др. – 2-е изд. – М.: Просвещение, 1984. – 192 с.
2. Фаддеев Д.К. Лекции по алгебра: Учебное пособие 5-е изд., стер. – СПб.: Лань, 2007. – 416 с.
3. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384 с.
4. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: учебник в 2-х т. – Т.1. – М.: Гелиос АРВ, 2003. – 336 с.
5. Ведерников В.А., Демина Е.Н. Элементы теории групп: Учебное пособие. – М.: МГПУ, 2014. – 125 с.
6. Винберг Э.Б. Курс алгебры. – М.: Факториал Пресс, 2001. – 544 с.