# Основы теории конечных полей.

## Основные алгебраические структуры.

**Опр. H.1.1** Пусть A и B непустые множества. Декартовым произведением называется множество всех пар , где .

Пример Н.1.1 Пусть . Тогда. Если множество и конечны и содержат соответственно n и m элементов (обозначается как , то

**Опр. H.1.2** Если – непустое множество, то декартово произведение называется декартовым квадратом и обозначается

**Опр. H.1.3** Отображение называется алгебраической операцией, определенной на множестве А.

Символ алгебраической операции обозначим . Символ обозначает, что на множестве определена алгебраическая операция .

**Опр. H.1.3** означает, что каждой паре элементов множества отвечает элемент , то есть множество замкнуто относительно операции Иначе говоря, , где

**Опр. H.1.4** Операция называется ассоциативной, если выполнено соотношение .

**Опр. H.1.5** Операция называется коммутативной, если выполнено соотношение .

**Опр. H.1.6** Структура называется группой, если выполнены требования:

1. операция ассоциативна;
2. существует элемент такой чтовыполнено соотношение . Элемент называется нейтральным;
3. для любого элемента существует элемент , такое что . Элемент называютэлементов обратным и обозначают . Такой элемент единственный. Очевидно, что , то есть элементы и взаимно обратны.

Если операция является сложением элементов группы, то группа называется аддитивной; если умножением, то мультипликативной.

Если операция коммутативна, то группа называется коммутативной или абелевой. Аддитивными абелевыми группа являются:

1. множества всех целых, вещественных, рациональных, комплексных чисел; множество всех целых четных чисел;
2. множество всех трехмерных векторов, координатами которых служат числа из множеств, перечисленных в пункте 1;
3. множество всех матриц фиксированного размера ;
4. множество всех многочленов с коэффициентами из множеств, упомянутых в пункте 1.

Все эти группы абелевы; нейтральный и обратный по сложению элементы очевидны.

Мультипликативными группами являются:

1. множество всех рациональных, вещественных или комплексных чисел, из которых удален 0;
2. множество всех неособенных квадратных матриц фиксированного n-ого порядка с элементами из множеств целых, вещественных, рациональных, комплексных чисел;

Для групп пункта а) нейтральный элемент равен единице; обратный очевиден. Группы пункта а) являются абелевыми группами.

Группа пункта b)коммутативна; нейтральный элемент – единичная матрица ; обратный элемент есть обратная матрица.

В группе обычным образом определяется степень элемента:

При этом выполняются свойства:

.

**Опр. H.1.7** Порядком элемента в группе называется наименьшее натуральное число ), такое что . Если такого числа нет, то порядок элемента считают бесконечным.

При этом пишут или .

**Теорема H.1.1**. Пусть группа конечна и . Тогда каждый элемент имеет порядок и является делителем числа n ( n – порядок группы).

В более общей формулировке теорема принадлежит французскому математику Жозефу Луи Лагранжу.

**Опр. H.1.8** Пусть на пустом множестве определены две операции. Одна условно называется сложением, другая умножением. Структура называется кольцом, если для нее выполняются требования:

1. сложение коммутативно, то есть ;
2. сложение ассоциативно, то есть ;
3. существует элемент такой, что ;
4. для любого элемента существует элемент такой, что . При этом и называется элементом, противоположным ;
5. операции сложения и умножения связаны законом дистрибутивности:

Эти пять условия называются аксиомами кольца.

Если операция умножения ассоциативна, то есть , то кольцо называется ассоциативным.

Если операция умножения коммутативна, то кольцо называется коммутативным. Если в ассоциативном кольце существует нейтральный по умножению элемент (единица), то кольцо называется ассоциативным кольцом с единицей.

Как следует из определения кольца, любое кольцо является ассоциативной абелевой группой.

**Опр. H.1.9** Пусть – ассоциативное кольцо с единицей . Если для некоторого элемента существует элемент такой , что , то элемент называется обратимым, а – обратный к элемент.

Приведем примеры колец.

Множество целых чисел - ассоциативно-коммутативное кольцо с единицей 1; обратимы два числа 1 и -1.

Множество рациональных, множество вещественных чисел, множество комплексных чисел – ассоциативно-коммутативные кольца с единицей. Обратимы все ненулевые элементы.

Множество всех трехмерных векторов. Их проекции - числа из множеств или . Сложение обычное, умножение – векторное произведение векторов. Множество - кольцо. Оно не является ассоциативным, так как ; не является коммутативным, так как . В кольце нет элемента такого, что хотя бы потому, что .

Множество всех квадратных матриц порядка - ассоциативное кольцо с единицей (единичной матрицей ). Обратимы все неособенные матрицы , то есть те, для которых.

Опр. H.1.10 Ассоциативно-коммутативное кольцо с единицей называется полем, если каждый его ненулевой элемент обратим.

Очевидно, поле образуют множество рациональных, вещественных или комплексных чисел.

Поле называется аддитивной группой, а поле, из которого исключен нулевой элемент - мультипликативной группой.

## Кольцо и поле . Модулярная арифметика.

**Опр. H.2.1** Пусть – целое число, а –натуральное число, причем . Разделить число на число означает найти целое число и неотрицательное число , , такие что .Число называется частным (неполным частным), а число – остатком от деления на .

Число называется «делимое», число – «делитель». Если остаток , то говорят, что число делится на число без остатка, или .

**Опр. H.2.2** Два целых числа и называются сравнимыми по модулю , если их разность является делителем числа

Этот факт записывается в виде:

H.2.1

или

H.2.2

Все числа сравнимые с по содержатся во множестве

Пусть – натуральное число , . Введем множество  
 . Оно является множеством всех остатков от деления любого целого числа на .

Определим на действия сложения и умножения по модулю . Тогда множество станет ассоциативно-коммуникативным кольцом с единицей 1.

Обратимыми в кольце являются все те и только те элементы, для которых наибольший общий делитель (НОД) чисел и равен 1.   
(НОД ()=1)

Обратный элемент в этом случае можно найти методом перебор или применить расширенный алгоритм Евклида (см. Сергиенко Е.Н.)

**Пример H.2.1** Найти все обратимые элементы кольца . Найти элементы обратные к ним.

**Решение.** Числа 1,3,7,9 взаимно просты с числом 10. Очевидно, . Проверим для каких ненулевых элементов кольца выполняется равенство .

Имеем

; ; ; ;; ;.

Следовательно, .

Так как обратный элемент единственный, то . Действительно,

Пример H.2.2 В кольце вычислить:

а) б) в) ; г) .

Решение.

а) , так как .

б) .

в)

г) Это равенство означает, что в кольце могут быть «ненулевые делители нуля» .

Если n – простое число p, то Все ненулевые элементы в взаимно просты с p, поэтому обратимы. Значит – поле.

Пример H.2.3 В поле для всех ненулевых элементов найти обратные.

Решение.

Имеем . Методом перебора легко установить, что

В поле ненулевых делителей нуля нет. Если , то или , или .

## Многочлены над полем

**Определение H.3.1** Многочленом степени n над полем называется выражение вида

где

– ненулевая константа поля. У многочлена ненулевой степени равно ().

Сложение, вычитание и умножение многочленов выполняется по обычным школьным правилам, но действие с коэффициентами выполняются по модулю p. Поэтому многочлены на полем образуют кольцо.

**Определение H.3.2** Разделить многочлен на многочлен означает найти два многочлена и такиe, что выполняется тождество

,

причем .

Многочлен называется частным (неполным частным), а многочлен - остатком.

Если , то говорят, что многочлен делится нацело (без остатка) на многочлен .

В этом случае и многочлены называется делителями . Если , то делители называются нетривиальными , в противном случае – тривиальными.

Если , то есть если ., то

.

В дальнейшем будем считать, что .

Деление многочленов при ручном счете выполняется уголком.

**Пример H.3.1** Разделить над полем многочлен на многочлен

**Решение**

Итак, , , )

Определение H.3.3 Пусть дан многочлен , , над полем . Элемент (число) называется корнем многочлена , если число .

Согласно определению H.3.1 , где . Если – корень , то , оттуда имеем равенство , или равенство , то есть . Это значит, что если – корень , то , то есть делится на без остатка.

В общем случае имеем . Это равенство и есть теорема Безу: остаток от деления многочлена на линейный множитель равен значению многочлена при .

**Определение H.3.4** Многочлен над полем называется приводимым над полем если его можно разложить в произведение двух или более нетривиальных многочленов над полем . В противном случае многочлен называется неприводимым.

**Утверждение H.3.1** Если многочлен имеет корень , то он приводим.

**Утверждение H.3.2** Если многочлен степень 2 или 3 приводим, то он имеет корень.

**Утверждение H.3.3** Все многочлены первой степени неприводимы.

Заметим, что для многочленов степени 4 приводимость не означает наличие корня в поле . Например над полем , но многочлен в поле корней не имеет ( как и ).

Неприводимыми многочленами над полем являются:

при n=2 ;

при n=3 , ;

при n=4 , , .

# Поля Галуа GF(pm)

Пусть задано поле и натуральное число n. Рассмотрим все многочлены степени над полем . Выберем неприводимый многочлен степени n и определим действия над многочленами: сложение и умножение на числа по обычным правилам, а действие над коэффициентами по modp.

Назовем два произвольных многочлена P(x) и Q(x) над полем сравнимыми по mod, если равны их остатки при делении на .

Факт сравнимости обозначают .

Очевидно, что каждый многочлен P(x) сравним с остатком от деления P(x) на .

Рассмотрим множество всех многочленов над полем , степени которых . Количество таких многочленов равно . Действие умножение определим формулой , где . Это значит, что есть остаток от деления на . Описанное множество многочленов образует кольцо. Примем без доказательства утверждение: это множество многочленов образует поле, обозначаемое GF(pm) (поле Галуа). Кроме указанных свойств , каждый ненулевой элемент имеет в поле обратный элемент : .

**Пример H.4.1** Перечислить все элементы поля .

**Решение**

Имеем

Составим таблицу произведений элементов этого поля. Числа 0 и 1, в силу очевидности, включать в нее не будем. Модуль .

Таблица Н. 4.1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  | 1 |  |  |
|  |  |  |  |  | 1 |  |
|  |  |  |  |  |  | 1 |
|  | 1 |  |  |  |  |  |
|  |  | 1 |  |  |  |  |
|  |  |  | 1 |  |  |  |

Из таблицы Н. 4.1 видно, что каждый ненулевой элемент из поля имеет обратный ().

Известен другой способ представления элементов поля. Найдем элементы поля, сравнимые в последовательными степенями.

Имеем: , где – остаток от деления на .

Итак

Далее можно действовать так:

;

;

;

.

Действия с элементами поля выполняют, используя полученные соотношения.

**Пример H.4.2** В поле выполнить действия:

**Решение:**

Имеем

(;

(;

;

.

Изложим еще один способ представления элементов поля, практически равносильный предыдущему.

Пусть имеется поле с модулем .В поле многочлен не имеет корней.

Пусть символ обозначает некоторый абстрактный корень . Это значит, что объект

определяется свойством:

Присоединим к полю и потребуем, чтобы множество было полем. Согласно определению поля множество содержит все степени . Изучим их. Имеем:

+1, так как то .

, так как 2

+1

+1+

+1

Легко видеть, что множество содержит все 16 многочленов от степени и что сумма двух таких многочленов есть элемент множества . Каждый ненулевой элемент имеет обратный, который находится по формуле

Этот способ генерации поля называется расширением поля . От предыдущего способа от в итоге отличается только буквой ().