Практическое занятие №10. Общее решение задачи расширенного алгоритма Евклида в евклидовых кольцах. Гомоморфизмы колец. Поля

Юрченков Иван Александрович

11 04 2022

# **Общее решение задачи расширенного алгоритма Евклида**

## **Постановка задачи**

Решить уравнение вида:

где – евклидово кольцо.

Пусть , тогда и , где и взаимно просты.

Тогда без потери общности, можем переписать уравнение в виде:

Если данное равенство, в пределах действий над евклидовым кольцом, с двух сторон сложить с обратным к в группе кольца по сложению, а именно элементом , тогда получим:

В полученном нами равенстве по свойству дистрибутивности умножения слева на элемент кольца, а также беря во внимание, что евклидово кольцо – *кольцо с единицей* и для него верно, что , вынесем налево элемент как сомножитель:

Так как евклидово кольцо является целостным, то в нем нет элементов – делителей нуля, поэтому один из сомножителей обязан равняться нулю по свойству кольца . Так как элемент , то , и следовательно нулю может быть равен только сомножитель .

Тогда прибавим к обеим частям равенства:

нейтральный по умножению в , получим:

Пусть исходя из расширенного алгоритма Евклида мы найдем пару решений для изначальной постановки задачи , тогда при заданном условии на и можно утверждать, что:

найденные корни и также являются решением и данного равенства.

Получаем систему решений:

Вычтем из первого равенства второе поэлементно (прибавим обратный к элементам в равенстве) и по аксиоме о дистрибутивности получим:

и по свойству кольца получаем, что серия решений обязана быть кратна , и симметрично (из-за того, что сумма двух элементов дает нейтральный по сложению в ).

Получаем:

где – полученная пара серии общего решения уравнения .

## **Пример**

Заданы следующие условия задачи:

Тогда найдем пару нормированных коэффициентов:

Из решения расширенным алгоритмом Евклида получим:

Получим ответ в виде серии решений:

где – произвольный элемент евклидова кольца.

# **Отображения в кольцах**

## **Определение**

**Гомоморфизм колец**. Отображение , где и – два кольца, называется гомоморфизмом, если:

Если более детально, то гомоморфизм колец переводит групповую операцию сложения двух элементов в кольце в операцию сложения отображений в другом кольце. И то же самое происходит с операцией умножения в кольце.

Примечательно, что в результате отображения операция умножения не сохраняет свои свойства в изначальном кольце, ровно как и свойство кольца не отображаются в новое, поскольку прообраз и образ – разные алгебраические структуры.

**Изоморфизм колец**. Изоморфизмом называют взаимно однозначный гомоморфизм колец.

В изоморфизме примечательно сохранение свойств умножения колец ровно как и свойств самих колец ввиду однозначной обратимости данного отображения.

## **Свойства**

1. Образ кольца является кольцом.

* Стоит принять во внимание, что **образом кольца** называется множество элементов, нашедшие свое место в новом кольце в результате гомоморфизма: .

1. Гомоморфизм колец задает гомоморфизм между их группами по сложению.

* Логичным является тот факт, что даже если отображение ничего не делает со свойствами группы по сложению, так как кольца выстраиваются на коммутативных Абелевых группах, то все равно не все элементы являются однозначно обратимыми, в следствие чего однозначного обратного отображения обозначить между кольцами невозможно.

1. Композиция гомоморфизмов – гомоморфизм.

## **Ядро гомоморфизма колец**

**Утверждение**. Ядро любого гомоморфизма колец является двусторонним идеалом.

**Ядро гомоморфизма колец** – множество элементов кольца-прообраза, ставшие нейтральными элементами кольца-образа по сложению в результате гомоморфизма колец:

**Доказательство**.

Гомоморфизм колец задает гомоморфизм между их группами по сложению, следовательно ядро является подгруппой по сложению.

**ч.т.д.**

# **Поля**

## **Определение поля**

**Полем** называется множество с заданным на нем двумя алгебраическими операциями, которые обозначают и (сложение и умножение соответственно) и тремя аксиомами:

А1: Поле является коммутативной группой по сложению.

* Данная аксиома напрямую наследуется от первой аксиомы колец.

А2: Ненулевые элементы поля образуют коммутативную группу по умножению.

* Данная аксиома является расширением аксиомы кольца по ассоциативности умножения до определения абелевой группы по умножению на носитель (элементы множества) поля, без нейтрального по сложению, как алгебраической структуры.

А3: Аксиома дистрибутивности:

* В следствие коммутативности операции умножения аксиома дистрибутивности более не нуждается в различии между порядками следования операций сложения и умножения.

Стоит обратить внимание также на то, что в поле также как и в кольце нейтральный элемент по сложению также присутствует и обозначается “”. Нейтральный элемент по умножению также присутсвует как и в кольце с единицей и обозначается как “”.

Поле обозначается точно так же как и другие ранее показанные алгебраические структуры с двумя заданными операциями на них:

## **Характеристика поля**

**Характеристикой поля** называется порядок единицы (нейтрального элемента по умножению) в коммутативной группе поля. Вспоминая определение порядка элемента коммутативной группы, данный термин можно обозначить в более удобном виде:

То есть *характеристика поля* – число применений операции сложения к нейтральному элементу группы поля по умножению для достижения им нейтрального элемента по сложению. Если такое найти невозможно, то характеристика равна .

**NB**.

* Если порядок в аддитивной группе поля конечен, то его называют *характеристикой поля* .
* Если порядок в аддитивной группе поля бесконечен, то *характеристика поля* .

Характеристика поля является важным числом для поля, и его значение может быть не любым при конечном порядке нейтрального элемента по умножению:

**Утверждение**. Если , тогда , где – простое число.

**Доказательство**.

Возьмем нейтральный элемент по умножению и применим к нему раз операцию сложения.

Предположим, что не является простым. Если оно не является простым, тогда раскладывается на множители.

Если раскрыть скобки, мы получим ровно единиц, так что с отношением между операциями в таком резком переходе проблем не возникает.

Поскольку поле это кольцо, а также поле удовлетворяет трем аксиомам групп по умножению, значит каждый элемент кроме нуля обратим по умножению, следовательно делителей нуля в данном множестве нет. Поэтому, одно из чисел или обязано быть нулём.

То есть либо единиц в сумме дают ноль, либо единиц в сумме дают ноль, что противоречит определению порядка, так как и , а **порядок элемента группы** – наименьшее натуральное число количества применений групповой операции к элементу группы.

**ч.т.д.**

## **Свойства полей**

1. Если поле имеет ненулевую характеристику, то характеристика является простым числом.
2. Поле является кольцом.
3. В поле всегда разрешимо уравнение: .

(Прибавить к обеим частям элемент обратный и домножить обе части на элемент обратный по умножению)

1. В поле всего два идеала: само поле и .

Из предположения, что в идеале находится один ненулевой элемент, следует, что в идеале находится все поле.

1. В каждом поле есть подполе, изоморфное или , где – простое число.
2. В поле с характеристикой отображение является автоморфизмом данного поля – отображением поля в самого себя.

## **Автоморфизм Фробениуса**

**Утверждение**.В поле с характеристикой отображение является автоморфизмом данного поля – отображением поля в самого себя.

1. Автоморфизм Фробениуса – гомоморфизм.

Рассмотрим данное отображение относительно двух элементов поля и покажем, что данное отображение является гомоморфизмом. Для этого необходимо показать сохранение операций сложения и умножения при переходе в другое поле:

Из коммутативности поля по умножению, второе условие доказывается элементарно:

тогда как со вторым уловием необходимо разобраться более детально.

Рассмотрим сумму элементов в степени:

Стоит обратить внимание, на то, что коэффициент перед а именно является натуральным по свойству сочетаний и также делится на , так как числитель содержит , и знаменатель не делится на . Поэтому данный коэффициент стоит раcценивать как количество применений групповой операции сложения элементов кольца .

Поскольку количество применений групповой операции сложения выполняется раз, а сам коэффициент по итогу делится нацело на : , где – простое число и характеристика поля , то сам коэффициент выполняет роль показателя количества раз применений подряд раз применения сложения к элементу поля. Это означает, что коэффициенты приводят элементы к нейтральному по сложению, то есть нулю. Тогда:

1. Ядро автоморфизма Фробениуса – содержит один элемент.

Для того, чтобы показать что доказанный гомоморфизм является изоморфизмом, необходимо показать, что данный гомоморфизм имеет нулевое ядро, или что существует биекция между элементами полей при отображении.

Нулевое ядро обозначает, что нейтральный элемент первого поля отображается в нейтральный элемент по сложению другого поля в результате отображения и никакой другой элемент поля-прообраза не отображается в нейтральный по сложению:

По свойству идеалов поля, идеалов у произвольного поля всего два: нулевой элемент и всё поле. По свойству гомоморфизма кольца – ядро гомоморфизма кольца является идеалом.

Раз единица поля при отображении не отображается в ноль, значит в результате гомоморфизма идеал порождает поле по структуре исходного поля по свойству втягивания. Следовательно ядро гомоморфизма – идеал, равный исходному полю, из чего следует что данный гомоморфизм является автоморфизмом данного поля.

**ч.т.д.**

## **Примеры полей**

1. Действительные числа относительно операции сложения и умножения.
2. Рациональные числа относительно операции сложения и умножения.
3. Комплексные числа относительно операции сложения и умножения.
4. *Алгебраические числа* над полем рациональных чисел.
5. Числа вида , , относительно обычных операций сложения и умножения. Это один из примеров квадратичного поля, которое образует подполе в .
6. Арифметика по простому модулю: относительно операции сложения и умножения по модулю , где – простое число.