# Лекция 1

**Определение:** Кольцо – множество с операциями «+» и «\*».

**Свойства:**

«+»: коммутативная, ассоциативная, дистрибутивная, существует обратный элемент

«\*»: дистрибутивная. НЕ ВСЕГДА коммутативная, ассоциативная с нейтральным элементом.

*- кольцо целых чисел.*

*– кольцо остатков по модулю n.*

*A, B; A × B = . «+», «\*» - покомпонентные.*

**Свойства гомоморфизма колец:**

Пусть  и  — произвольные кольца. Если — гомоморфизм (), то

1) образ нуля кольца  при отображении  есть нуль кольца , то есть ;

2) образ единицы кольца  при отображении  есть единица кольца , то есть ;

3) для всякого элемента  кольца образ элемента, противоположного элементу , равен элементу, противоположному образу элемента , то есть ;

4) если кольца  и  являются полями, то для всякого элемента  кольца  образ элемента, обратного к элементу  по умножению, равен элементу, обратному к образу элемента , то есть .

**Изоморфизм** – биективный гомоморфизм

**Китайская теорема об остатках для колец:**

*Если НОД (m, n) = 1*

*//идемпотент*

**Задача для самостоятельного решения:**Кольцо матриц (не коммутативное кольцо). Какие матрицы идемпотентны? *()*

**Теорема***: Кольцо R изоморфно прямому произведению тогда и только тогда, когда в R существует нетривиальный идемпотент.*

*ОЧЕВИДНО, т. к. существуют пары (0, 1) и (1, 0).*

*Пусть e – идемпотентный элемент.*

*//множество кратностей e, x пробегает все элементы R.*

*2)*

3) Пусть – аналогично

4) Придумаем биекцию, согласованную с операциями:

Биекция:(обоснование) построим обратное отображение

R

*Проверим взаимообратность :*

*5)*

**Пример:**

*\*

*– кольцо*

*- мн-во элементов, обратимых в A.*

*// с p взаимнопросты все числа до p, кроме 1 и самого p*

*, (*

**Проблема дискретного логарифмирования:** *.*

**Шифрование открытым ключом:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Собеседник1* | *Действия собеседников* | *Собеседник2* |
| *1.* |  | *Задаются числа n, a* |  |
| *2.* | *Генерация* |  |  |
| *3.* |  |  | *Генерация* |
| *4.* |  |  |  |
| *5.* |  |  |  |

**Задача:**

Дано:

Как найти в нём элемент наибольшего порядка?

рациональные простые числа.

Как устроены порядки элементов в

Если , то в есть элемент порядка

Если то max равен

множество

– кольцо

Многочлен – формально сумма

**Каждый многочлен задает функцию**

Получилось отображение

Пусть А – конечное кольцо

Разные многочлены могут задать одну и ту же функцию.

(или любое бесконечное F)

- инъективна

Если конечно, то точно не инъективно.

Сюръективна ли Т. е. любую ли функцию из А в А можно задать многочленом? Спойлер: нет.

# Лекция 2.

Отображение, которое каждому многочлену сопоставим задаваемую функцию, т. е.

фукнция из в

(Не знаю зачем мы столько раз пишем одно и то же…)

Для эта функция инъективна.

точно не инъективна

## Рассмотрим домашнюю задачу с прошлой лекции:

Можно ли задать такое отображение , что :

?

Нет, нельзя!

Доказательство:

Пусть - такой многочлен, что , , по теореме Безу

# Доказать:

Для доказательства рассмотрим :

Деление с остатком в кольце многочленов ()

Что такое деление с остатком на ?

*– условие того, что R – остаток от деления многочлена в произвольном кольце*

Если , то деление с остатком точно существует:

Для : как свести к делению с остатком многочлена меньшей степени, чем n?

Рассмотрим деление столбиком многочлена :

Первым шагом имеем: , ? — это нечто, что мы ищем(какой-то коэффициент, на который надо домножить делитель, чтобы ушла старшая степень – вспоминаем деление столбиком). А вот и деление столбиком подъехало:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  | ?? – новое нечто, которое надо бы искать |

Не во всяком кольце . Необходимо, чтобы старший коэффициент был обратим.

**Теорема.** Деление с остатком , если старший коэффициент обратим.

Доказательство – алгоритм деления столбиком. (оЧеВиДнО)

**Утв.:** Если – не делитель нуля, следовательно, разложение единственно.

Докажем утверждение:

*, если – не делитель нуля; утверждение доказано.*

Рассмотрим пример:

, т.к. )

**Теорема Безу().** Пусть

*-* корень

**Доказательство.** Старший коэффициент — это 1 деление с остатком.

*Пусть , тогда:*

Ч.т.д.

По т. Безу

Пусть - тоже корень

Верно, если в кольце нет делителей нуля.

**Итог:** если в кольце нет делителей нуля, то многочлен имеет не более n корней.

**Теорема.** Конечное кольцо без делителей нуля – поле.

**Доказательство.**

*Пусть и* – хотим доказать, что а обратим.

Умножим весь набор на a. Получим набор .

Докажем, что в новом наборе все элементы различны (тогда среди них найдётся единичка):

Предположим, что

’

Но и

Противоречие‼!

**Конечные поля**

где p – простое.

поле.

**Теорема.** многочлены

Тогда такие, что не имеют общего делителя положительной степени.

**Доказательство.**

Необходимость очевидна (на самом деле нет, но так сказал Игорь Вадимович, поэтому как только он уточнит этот вопрос, док-во появится здесь).

Докажем достаточность (Без использования однозначного разложения на многочлены)

где P и Q- все возможные многочлены.

Если - все хорошо.

Если в W есть любая const – тоже все хорошо.

Если есть в кармане пачка сигарет, значит все не так уж плохо на сегодняшний день.

Пусть (- многочлен наименьшей возможной степени. Если – всё будет хорошо.

Если экзамен принимает Артамкин - все плохо (на самом деле нет, но шанс получить неуд. выше, чем найти в кармане пачку сигарет).(Если экзамен принимает Митин, значит все не так плохо на сегодняшний день)

Докажем от противного, что : пусть

Делим с остатком на D.

(по определению)

Противоречие‼!

Итог:

**Определение.** называется неприводимым, если его нельзя разложить в произведение многочленов меньшей(ненулевой) степени.

какие там есть неприводимые многочлены?

Замечание: текущая версия лекции 2 требует определённых дополнений и пояснений, которые будут внесены после предэкзаменационной консультации.

# Лекция 3

Рассмотрим отображения

Сколько существует таких отображений?

Очевидно,

Как вывести формулу для количества отображений? (хз, но она у нас есть. Пусть это будет ОчЕвИдНо)

Сколько отображений из

Ответ:

Рассмотрим множество многочленов степени не выше m-1

Докажем, что это инъекция

Пусть

Пример

|  |  |
| --- | --- |
| 00 | 0 |
| 01 | 1 |
| 10 | 1 |
| 11 | 0 |

Как построить многочлен отображений? Узнаем позже.

Докажем по индукции, что для любого отображения задается многочлен от переменных где каждая переменная будет в степени

База. Была доказана ранее(сколько отображений из )

Предположим, что утверждение верное при s=n.

Пусть

Вообще не ебу правильно ли это и че я тут вообще написал, помогите

**Многочлен Жегалкина**

Пример

|  |  |
| --- | --- |
| *000* | *0* |
| *001* | *0* |
| *010* | *1* |
| *011* | *1* |
| *100* | *1* |
| *101* | *0* |
| *110* | *1* |
| *111* | *1* |

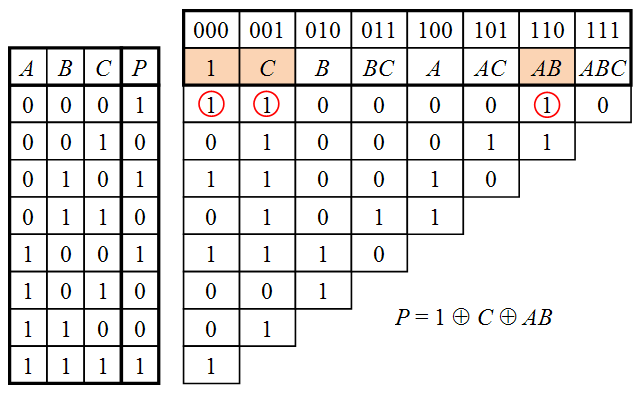
Как можно представить многочлен Жегалкина по методу треугольника (по фэн-шую прим. Строганова)?

Метод треугольника позволяет преобразовать таблицу истинности в полином Жегалкина путём построения вспомогательной треугольной таблицы в соответствии со следующими правилами:

1. Строится полная таблица истинности, в которой строки идут в порядке возрастания двоичных кодов от 000…0 до 111…1.
2. Строится вспомогательная треугольная таблица, в которой первый столбец совпадает со столбцом значений функции в таблице истинности.
3. Ячейка в каждом последующем столбце получается путём сложения по модулю 2 двух ячеек предыдущего столбца — стоящей в той же строке и строкой ниже.
4. Столбцы вспомогательной таблицы нумеруются двоичными кодами в том же порядке, что и строки таблицы истинности.
5. Каждому двоичному коду ставится в соответствие один из членов полинома Жегалкина в зависимости от позиций кода, в которых стоят единицы. Например, ячейке 111 соответствует член ABC, ячейке 101 — член AC, ячейке 010 — член B, ячейке 000 — член 11 и т.д.
6. Если в верхней строке какого-либо столбца стоит единица, то соответствующий член присутствует в полиноме Жегалкина.

Фактически, этот метод является модификацией метода построения по таблице истинности, описанного выше. По сравнению с ним он удобнее тем, что расчёты занимают мало места и в них сложнее ошибиться, но метод треугольника требует бо́льшего количества операций.

Пример преобразования таблицы истинности в полином Жегалкина для функции трёх переменных P(A,B,C)P показан на рисунке.



**Булевы функции**

**Способы задания**

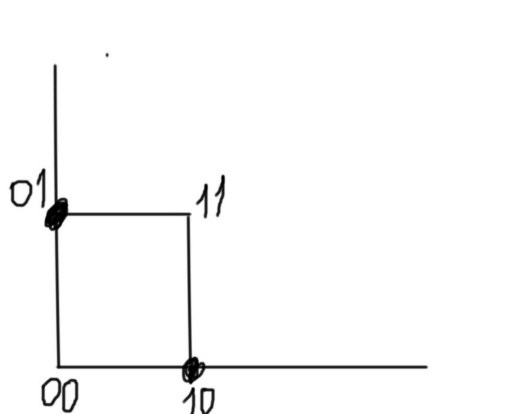
1. **Таблица истинности**

|  |  |  |
| --- | --- | --- |
| **x** | **y** | **F** |
| 0 | 0 | **0** |
| 0 | 1 | **1** |
| 1 | 0 | **1** |
| 1 | 1 | **0** |

1. **Вектор**

F=(0110)

1. **Графически**

****

1. **Многочлен Жегалкина**

**Некоторые булевы функции**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | y |  |  |  |  |  |  |  |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |

А потом случился карантин ☹