Семинар №7 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь

Определение 1 Евклидово кольцо . . . 1
Лемма 1 О единице . . . 1
Теорема 1 О главных идеалах . . . 2
Определение 2 НОД . . . 2
Определение 3 Взаимно простые элементы . . . 2
Теорема 2 О представимости НОД . . . 2
Лемма 2 Лемма к алгоритму Евклида . . . 2
Теорема 3 О решении диофантова уравнения . . . 4
Определение 4 Прямая сумма колец . . . 4
Теорема 4 КТО . . . 4

Определение 1 (Евклидово кольцо)
По определению, коммутативное кольцо R называется евклидовым, если для него выполнены следующие свойства.

1. Кольцо R не имеет делителей нуля.
2. Для каждого ненулевого элемента кольца определена числовая характеристика — норма, которая принимает целые неотрицательные значения.
3. Определено деление с остатком. Возможность деления с остатком означает, что для любых элементов a, b кольца, $b \neq 0$, существуют такие q, r, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$. Элемент r называется остатком от деления a на b.
4. $\forall\ a, b \in R, a \neq 0, b \neq 0 N(ab) > max(N(a), N(b))$

Лемма 1 (О единице)
Евклидово кольцо является кольцом с единицей.

Доказательство Выберем такой ненулевой элемент e' евклидова кольца R, что $N(e')$ принимает минимально возможное положительное значение.
Разделим произвольный элемент a на e' с остатком: $a = qe' + r$.
По определению верно одно из двух: либо $N(r) < N(e')$, либо $r = 0$. Первое невозможно в силу минимальности нормы e'. Значит, $a = qe'$. В частности, $e' = ee'$.
Но тогда для любого $a \in R$ имеем $ae' = aee'$, иначе говоря $e'(a - ae) = 0$. Поскольку кольцо R целостное и $e' \neq 0$, получаем $a - ae = 0$. Значит, e является единицей кольца R.

Пример 1
Нашими основными примерами евклидовых колец является кольцо целых чисел (в нем норма — это модуль числа) и кольцо многочленов (вскоре мы узнаем, что коэффициенты многочлена не обязаны быть действительными, вместо этого они могут лежать в произвольном поле*), в котором за норму можно принять степень многочлена.*
В определении деления с остатком мы не требовали единственности неполного частного и остатка. Это требование не нужно для доказательства основных свойств евклидовых колец. Отметим, однако, что для кольца многочленов, как и для кольца целых чисел, неполное частное и остаток определены однозначно.

Теорема 1 (О главных идеалах)
Евклидовы кольца — это кольца главных идеалов.

Определение 2 (НОД)
Пусть a, b — два элемента евклидова кольца R. Наибольшим общим делителем a и b называют такой элемент d, что $a = qd, b = rd$, и для любого общего делителя d' ($a = q'd', b = r'd'$) выполнено $d = d'd''$ для какого-то $d'' \in R$.

Замечание 1
Согласно этому определению ничто не мешает существованию нескольких наибольших общих делителей.Скажем, 5 *и* -5 *являются наибольшими общими делителями чисел* 10 *и* 15 *в кольце* $\mathbb{Z}$*. Нетрудно показать, что все они будут отличаться на некий элемент* обратимый *элемент кольца. Иногда такие элементы называют делителями единицы. Мы будем обозначать наибольший общий делитель через* (a, b) *и понимать под этим традиционным обозначением любой из наибольших общих делителей.*

Определение 3 (Взаимно простые элементы)
Элементы евклидова кольца R называются взаимно простыми, если их наибольший общий делитель равен единице.

Теорема 2 (О представимости НОД)
Наибольший общий делитель двух элементов евклидова кольца можно представить как их линейную комбинацию с коэффициентами из кольца.

$$(a, b) = ra + qb$$

В евклидовых кольцах существует простой способ нахождения наибольшего общего делителя и решения уравнения $xa+yb = (a, b)$, который называется *расширенным алгоритмом Евклида.*

Лемма 2 (Лемма к алгоритму Евклида)
Для любых элементов a, b, q евклидова кольца выполнено $(a, b) = (a - qb, b)$.

На этом основывается то, что называется алгоритмом Евклида.
Пусть $a > b$, тогда, разделив с остатком, получим $a = qb + r$, откуда $r = a - qb$, а значит, $(a, b) = (r, b)$.
На каждом таком шаге минимальная из норм двух элементов уменьшается, поэтому алго-

ритм придет к концу. Тогда мы будем иметь НОД.

Задача 1
Найти НОД двух многочленов: $x^5 - 1$ и $x^3 - 1$.

Решение

$$\begin{aligned} x^5 - 1 &= x^2 \cdot (x^3 - 1) + (x^2 - 1) & (x^5 - 1, x^3 - 1) \\ x^3 - 1 &= x \cdot (x^2 - 1) + (x - 1) & (x^3 - 1, x^2 - 1) \\ x^2 - 1 &= (x + 1) \cdot (x - 1) + 0 & (x^2 - 1, x - 1) \\ & & x - 1 \end{aligned}$$

Таким образом, $(x^5 - 1, x^3 - 1) = x - 1$.

Теперь познакомимся с такой вещью, как *расширенный алгоритм Евклида*.
Решим уравнение $ax + by = d,\ d = (a, b)$. такие уравнения называются *диофантовыми*.

Мы будем вычислять последовательность троек (a_i, x_i, y_i), для которых сохраняется

$$a_i = x_i a + y_i b$$

Начальные значения такие:

$$a_0 = a,\ x_0 = 1,\ y_0 = b$$

$$a_0 = b,\ x_0 = 0,\ y_0 = 1$$

Дальнейшие значения вычисляем, деля с остатком a_{i-2} на a_{i-1}:

$$a_i = a_{i-2} - q_{i-1} a_{i-1}$$

$$x_i = x_{i-2} - q_{i-1} x_{i-1}$$

$$y_i = y_{i-2} - q_{i_1} y_{i-1}$$

Задача 2
Представить число 1 = (12,17) как линейную комбинацию 12 и 17.

Решение

i	a	x	y	q
0	12	1	0	
1	17	0	1	0
2	12	1	0	1
3	5	-1	1	2
4	2	3	-2	2
5	1	-7	5	

Последняя строчка как раз говорит, что $1 = -7 \cdot 12 + 5 \cdot 17$

Замечание 2
Часто это пригождается для поиска обратных в кольцах вычетов.
Например, чтобы найти 7^{-1} в $\mathbb{Z}/(19)$, нужно найти такой x, что

$$x \cdot 7 - 1 \in (19) \Longleftrightarrow 7x + 19y = 1$$

Решив это диофантово уравнение, получим $x = 7^{-1}$.

Решим исходное линейное уравнение полностью.

Утверждение 1
Множеством решений однородного уравнения

$$ax + by = 0, \quad a, b \in R,\ a \neq 0, b \neq 0$$

являются такие пары:

$$x = t\frac{b}{d},\ y = -t\frac{a}{d} \quad d = (a, b),\ t \in R$$

Утверждение 2
Неоднородное уравнение $ax + by = c$ разрешимо тогда и только тогда, когда c делится на (a, b).

С помощью расширенного алгоритма Евклида можно найти частное решение уравнения $ax + by = d$. Если $c = kd$, то, умножив на k наше решение, получим решение $ax + by = c$. Имея частное решение неоднородного уравнения и общее решение однородного, можно найти общее решение, как в линале:

Теорема 3 (О решении диофантова уравнения)
Если c кратно $d = (a, b)$, то множество решений уравнения $ax + by = c$ таково:

$$x = x_0 + t\frac{b}{d},\ y = y_0 + t\frac{a}{d} \quad t \in R$$

Пример 2
Возвращаясь к уравнению $12x + 17y = 1$*, получаем общее решение*

$$x = -7 + t,\ y = 5 - t \quad t \in \mathbb{Z}$$

Теперь рассмотрим, как можно обобщить КТО для колец.

Определение 4 (Прямая сумма колец)
$R_1 \oplus R_2$ есть декартово произведение носителей с покомпонентным сложением и умножением, аналогично прямому произведению групп.

Теорема 4 (КТО)
Для взаимно простых элементов p_1, p_2 евклидова кольца R имеет место изоморфизм колец $R/(p_1p_2) \cong R/(p_1) \oplus R/(p_2)$.

С помощью КТО можно решать системы сравнений по модулю взаимно простых чисел. Об этом можно прочитать в учебнике в параграфе 10.5
Но сейчас рассмотрим задачу, где мы используем теорему в обратную сторону

Задача 3
Найти решения уравнения $x^2 - 1 = 0$ в кольце $\mathbb{Z}/(143)$.

Решение $143 = 11 \cdot 13$ — произведение двух взаимно простых чисел. Значит, согласно КТО, $\mathbb{Z}/(143) \cong \mathbb{Z}/(11) \oplus \mathbb{Z}/(13)$.

$x^2 - 1 = (x+1)(x-1)$. В нашем кольце $-1 \neq 1$, поэтому, так как кольцо многочленов евклидово $\Rightarrow$ область целостности, то $x^2 - 1 = 0 \Leftrightarrow x = \pm 1$ — ровно два различных корня.
Единицей в сумме колец будет $(1,1)$, поэтому решения уравнения в $\mathbb{Z}/(143)$ — это пары (x_1, x_2), где x_1 и x_2 — решения уравнения в кольцах $\mathbb{Z}/(11)$ и $\mathbb{Z}/(13)$ (каждое в своем кольце).
Всего таких пар 4: $(1,1), (-1,-1), (1,-1), (-1,1)$.
Первые две из них — это 1 и -1 в кольце $\mathbb{Z}/(143)$.
Осталось найти остальные. Они находятся из систем сравнений:

$$\begin{cases} x \equiv 1 & \mod 11 \\ x \equiv -1 & \mod 13 \end{cases} \qquad \begin{cases} x \equiv -1 & \mod 11 \\ x \equiv 1 & \mod 13 \end{cases}$$

Эти решения — противоположные вычеты, поэтому достаточно решить только одну систему.
Это можно сделать руками с помощью алгоритма Евклида, но здесь можно просто увидеть, что $x = 12$ — решение первой системы.
Итого получается 4 решения в $\mathbb{Z}/(143)$: $\pm 1, \pm 12$.

Замечание 3
В изложении этой задачи мы пытались избежать термина «поле», так как его мы еще не проходили (оно есть в оригинале в учебнике).
В решении мы пользовались тем, что у уравнения $(x+1)(x-1)$ всего два корня ± 1, но почему мы так не сказали изначально для кольца $\mathbb{Z}/(143)$ и почему там решения 4?
Мы так говорили в связи с тем, что в кольце нет делителей нуля. Если это так, то $(x-1)(x+1) = 0 \Leftrightarrow \left[\begin{array}{l} x-1=0 \\ x+1=0 \end{array}\right.$
Это выполняется в $\mathbb{Z}/(13)$ и $\mathbb{Z}/(13)$. Пусть в кольце вычетов есть делители нуля. Это значит, что для некоторых ненулевых чисел выполняется $a \cdot b = n \cdot p$, где p — число, остатки по модулю которого мы берем, $a, b < p$. Но если p — простое, то такое невозможно.
В отличие от колец, на сумму которых мы его разбиваем, кольцо $\mathbb{Z}/(143)$ имеет делители нуля, например 11 и 13 (на самом деле, еще -11 и -13 и все). Поэтому мы и не могли говорить, что есть только два корня.

Задача 4
Найти все нильпотентные элементы в кольце $\mathbb{Z}_3[x]/(x^2-1)$.

Решение Сперва разложим многочлен на простые $x^2 - 1 = (x-1)(x+1)$. Теперь мы можем применить КТО, сказав, что $\mathbb{Z}_3[x]/(x^2-1) \cong \mathbb{Z}_3[x]/(x-1) \bigoplus \mathbb{Z}_3[x]/(x+1)$. Рассмотрим, например, левое слагаемое. Любой многочлен степени k из $\mathbb{Z}_3[x]/(x^2-1)$ представим как $p_k(x) = (x-1) \cdot p_{k-1}(x) + c$ (деление с остатком). Заметим, как найти c: $p_k(1) = (1-1) \cdot p_{k-1}(x) + c = c$. Значит, существует изоморфизм $\varphi : p \to p(1)$ между $\mathbb{Z}_3[x]/(x-1)$ и $\mathbb{Z}_3$. Значит исходное кольцо изоморфно ${\mathbb{Z}_3}^2$, в котором лишь тривиальный нильпотентный элемент — ноль. Значит и в исходном кольце только ноль является нильпотентным элементом.