Кольца. Области целостности. Поля

Лектор: Завьялов Олег Геннадьевич
кандидат физико-математических наук, доцент

Определение

Кольцом называется непустое множество R вместе с бинарными операциями, называемыми умножением и сложением, которые обозначаются соответственно $\cdot$ и $+$, удовлетворяют условиям:

1) Множество R замкнуто относительно сложения, если $x \in R$ и $y \in R$, то $x + y \in R$.
2) Сложение в R ассоциативно, $x + (y + z) = (x + y) + z$ для всех $x, y, z \in R$.
3) Множество R содержит аддитивную единицу (нейтральный элемент относительно сложения), так что $x + 0 = 0 + x = x$ для всех $x \in R$.
4) Для каждого элемента x из R множество R содержит элемент $-x$, обратный x относительно сложения, что $x + (-x) = -x + x = 0$.
5) Сложение в R коммутативно, $x + y = y + x$ для всех x и $y \in R$.
6) Множество R замкнуто относительно умножения, если $x \in R$ и $y \in R$, то $x \cdot y \in R$.

Определение

7. Умножение в R ассоциативно, $x\cdot(y\cdot z) = (x\cdot y)\cdot z$ для всех $x, y, z \in R$.
8. Для всех $x, y, z \in R$ выполняются законы дистрибутивности

$$x\cdot(y + z) = (x\cdot y) + (x\cdot z)$$

и

$$(y + z)\cdot x = (y\cdot x) + (z\cdot x).$$

Если во множестве R существует элемент 1 (мультипликативная единица, нейтральный элемент относительно умножения) такой, что $1\cdot r = r\cdot 1 = r$ для всех $r \in R$, то множество R называется ***кольцом с единицей***.

Если $r \cdot r' = r' \cdot r$ для всех $r, r' \in R$, то множество R называется ***коммутативным кольцом***.

Кольцо R является группой относительно сложения и полугруппой относительно умножения.

Примеры колец относительно обычных операций сложения и умножения: целые, действительные, рациональные и комплексные числа. Множество $(n \times n)$ –матриц для фиксированного целого числа n и множество полиномов.

Только матрицы не образуют коммутативное кольцо.

Определение.

Областью целостности называется коммутативное кольцо с единицей, не совпадающей с 0, так что из условия $ab = 0$ с следует $a = 0$ или $b = 0$.

Множество целых, действительных, рациональных чисел являются областями целостности. Множество (2×2) – матриц не является областью целостности, т.к. произведение двух ненулевых матриц может быть нулевой матрицей.

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Важное замечание:

Области целостности обладают свойством сокращения относительно умножения, если $ab = ac$ и $a \neq 0$, то $b = c$.

Кольца не обязательно содержат взаимно обратные элементы, поэтому не всегда возможно умножить обе части уравнения $ab = ac$ на a^{-1} и получить $b = c$.

Теорема

Пусть R – коммутационное кольцо с единицей. Кольцо R является областью целостности тогда и только тогда, когда из $ab = ac$ следует, что $b = c$ для всех b, c и ненулевых элементов $a \in R$.

Когда число n не является простым, рассмотрим подмножество $R = \{[x]: x$ – взаимно простое с $n\}$.

Теорема:

Это множество образует группу относительно умножения.

Доказательство:

Произведение двух целых чисел, взаимно простых с n, является числом , взаимно простым с n.

Единица 1 есть число, взаимно простое с n. Если число b - взаимно простое с n, то сравнение $bx = 1$ имеет единственное решение, поэтому для элемента $[b]$ существует обратный элемент.

Относительно сложения множество R не образует даже полугруппу, поскольку сумма двух чисел. Взаимно простых с n, не обязательно является числом, взаимно простым с n.

Определение

Пусть R и R' - кольца и пусть $f: R \to R'$ -функция из R в R'. Функция f называется ***гомоморфизмом колец*** тогда и только тогда, когда

$$f(a+b) = f(a) + f(b),$$

$$f(a \cdot b) = f(a) \cdot f(b)$$

для всех $a, b \in R$. Сложение и умножение в соответствующих кольцах одинаково определены.

Если гомоморфизм колец $f: R \to R'$ - инъекция, то его называют ***мономорфизмом***.

Если гомоморфизм колец $f : R \to R'$ - сюръекция, то его называют ***эпиморфизмом***.

Гомоморфизм колец $f : R \to R'$ называют ***изоморфизмом***, если функция $f: R \to R'$ - биекция.

При описании гомоморфизма из кольца R с единицей в кольцо R' с единицей требуется, чтобы мультипликативная единица кольца R_8 отображалась на мультипликативную единицу кольца R'.

Изоморфные кольца имеют одинаковую алгебраическую структуру и отличаются только именованием своих элементов.

Теорема.

Для всех a из кольца R выполняется соотношение $a \cdot 0 = 0$.

Определение.

Подмножество R' кольца R называется ***подкольцом*** кольца R, если R' – это кольцо с той же самой операцией.

Пример.

Целые числа образуют подкольцо кольца рациональных чисел.

Рациональные числа образуют подкольцо кольца действительных чисел.

Множество $(n \times n)$ - матриц с целочисленными элементами образуют подкольцо кольца $(n \times n)$ матриц с рациональными элементами.

{[0], [2], [4]} – подкольцо кольца Z_6.

Определение.

Полем называется коммутативное кольцо с единицей, не совпадающей с 0, каждый ненулевой элемент которого имеет обратный элемент относительно умножения.

Теорема.

Поле является областью целостности. Конечная область целостности является полем.

Пусть A – область целостности. В частности, A может быть множеством целых чисел Z. Рассмотрим множество упорядоченных пар

$$P = \{(a, b) : (a, b) \in A \times A \text{ и } b \neq 0\}$$

и определим отношение $\sim$ на P следующим образом:

Определение.

Если пары (a, b) и (c, d) принадлежит P, то $(a, b) \sim (c, d)$ тогда и только тогда, когда $ad = bc$.

Пример.

Если $A = Z$, то класс эквивалентности $[(2, 3)]$ содержит такие упорядоченные пары:

(2, 3), (4, 6), (6, 9), …, (-2, -3), (-4, -6), …,

которые соотвествуют представлениям рациональных чисел в виде 2/3, 4/6, 6/9, …, (-2/3), (-4/6), …

Все они являются различными представлениями одного и того же рационального числа $[(2, 3)]$.

Теорема.

Отношение на множестве P есть отношение эквивалентности.

Определение.

Для заданных элементов a, b, c, d из области целостности A сложение на F определено соотношением

$$a/b + c/d = (ad + bc) / bd ,$$

а умножение на F – соотношением

$$(a/b)(c/d) = ac / bd.$$

Операции сложения и умножения на F определены корректно, не зависят от выбора представителей классов эквивалентности:

Теорема.

а) Сложение в F определено корректно;

б) Умножение в F определено корректно.

Теорема.

Множество классов эквивалентности F является коммутативным кольцом с аддитивной единицей 0/1 и мультипликативной единицей 1/1.

Лемма.

Для a и b из A имеем $a/b = 0/1$ тогда и только тогда, когда $a = 0$.

Доказательство:

Очевидно, что равенство a/b = 0/1 имеет место тогда и только тогда, когда $a = a(1) = b(0) = 0$.

Теорема.

Коммутативное кольцо ***F*** является полем.

Теорема.

Отображение $f : A \rightarrow F$, определенное соотношением

$$f(a) = a / 1,$$

является мономорфизмом, при этом область целостности A вложена в поле F или поле F содержит область целостности A.

Теорема.

Поле F называется есть наименьшее поле, в которое область целостности A может быть вложена.

Определение.

Поле F называется полем частных области целостности A. Если A – множество целых чисел Z, то поле F - множество рациональных чисел, обозначаемое Q.

Определение.

Подмножество I кольца R называется идеалом кольца R, если

а) I – подкольцо кольца R;

б) если x принадлежит I и r принадлежит R, то $x \cdot r$ и $r \cdot x$ принадлежат I.

Определение.

Пусть R – коммутативное кольцо. Идеал I кольца R называется ***главным идеалом***, порожденным элементом a, если I состоит из всех произведений a на элементы кольца R,

то есть $I = \langle a \rangle = \{ar: r \in R\}$.

Теорема.

Каждый непустой идеал I кольца целых чисел называется главным идеалом.

Пример.

Кольцо Z целых чисел и два главных идеала, порожденными целыми числами 8 и 12:

$$\langle 8\rangle = \{8r : r \in Z\} = \{\ldots, -24, -16, -8, 0, 8, 16, 24, \ldots\};$$

$$\langle 12\rangle = \{12s : s \in Z\} = \{\ldots, -24, -12, 0, 12, 24, \ldots\}.$$

Пересечение множеств $\langle 8\rangle \cap \langle 12\rangle$ есть множество

$$\{\ldots, -48, -24, 0, 24, 48, \ldots\},$$

которое является главным идеалом, порожденным целым числом 24. 24 – наименьшее общее кратное чисел 8 и 12.

Теорема.

Если s и t – ненулевые целые числа и $\langle s \rangle$ и $\langle t \rangle$ - соответствующие главные идеалы в кольце Z, то

а) если $\langle s \rangle \subseteq \langle t \rangle$, то $t \mid s$;

б) $\langle s \rangle \cap \langle t \rangle = \langle u \rangle$, где $u = НОК(s, t)$.

Пример.

Если $\langle a, b\rangle$ - наименьший идеал, содержащий a и b, то $\langle a, b\rangle = \langle$НОД $(a, b)\rangle$.

Пример.

$$\langle 8, 12\rangle = \{-16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\} = \langle \text{НОД}(8, 12)\rangle,$$

так как НОД(8, 12) = 4 и $\langle 4\rangle = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$.

Пусть I – наименьший идеал, содержащий целые числа a и b. Тогда каждый элемент идеала I имеет вид $am + bn$, где m и n – целые числа. Идеал I порожден элементами a и b.

Идеал I порожден наименьшим положительным целым числом такого вида.

Теорема.

Идеал I кольца R с единицей совпадает с R тогда и только тогда, когда 1 (мультипликативная единица кольца R) принадлежит идеалу I.

Теорема.

Поле не содержит собственных идеалов.

Теорема.

В кольце целых чисел идеал $\langle a \rangle$ является простым идеалом тогда и только тогда, когда a – простое число.

Определение.

Область целостности D является областью главных идеалов, если каждый идеал в области D является главным идеалом.

Z (область целостности целых чисел) является областью главных идеалов.

Определение.

Если A – коммутативное кольцо с единицей, то пусть A^* обозначает множество $\{a \in A :$ существует $b \in A^*$ такое, что $ab = 1\}$. Подмножество A^* является группой относительно умножения, которая называется ***группой делителей единицы*** кольца A. Каждый элемент множества A^* называется ***делителем единицы*** кольца A. В кольце с единицей элемент s называется неприводимым, если он ненулевой, не равен единице и не может быть выражен как произведение двух элементов, не являющихся делителями единицы.

В области целостности Z: $ab = 1$ тогда и только тогда, когда $a = b = 1$ или $a = b = -1$, поэтому 1 и -1 – делители единицы области целостности Z.

В поле каждый ненулевой элемент является делителем единицы, так как $a \cdot a^{-1} = 1$ для $a \neq 0$.

Пример.

Множество $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$ – коммутативное кольцо с единицей [1] и нулем [0].

Таблица умножения в Z_6 :

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Таблица показывает, что $[3] \odot [2] = [0]$, но $[3] \mid [0]$ и $[2] \mid [0]$, так что [3] и [2] — ненулевые делители элемента [0]. Таким образом, Z_6 не является областью целостности.

Области целостности.
Определение.

Область целостности D является гауссовым кольцом, если выполнены условия:

а) если элемент области D не нуль и не делитель единицы, то его можно представить в виде произведения конечного числа неприводимых элементов;

б) если элемент области D имеет разложения $p_1 \dots p_r$ и $q_1 \dots q_s$ в виде произведения неприводимых элементов, то $r = s$ и q_j можно перенумеровать, так что p_i и q_i для всех i будут отличаться делителем единицы, то есть $p_i = a_i \cdot q_i$ для некоторого делителя единицы a_i .

Пример.

Множество целых чисел является гауссовым кольцом.

Простое число, у которого нет нетривиальных множителей. Простое число неприводимо.

p - простое число тогда и только тогда, когда из того что $p \mid ab \Rightarrow$ что $p \mid a$ или $p \mid b$.

Пусть A – множество всех комплексных чисел

$$a + b\sqrt{5}\ i$$

A - область целостности

$$21 = 3 \cdot 7 = \left(1 + 2\sqrt{5}\ i\right)\left(1 - 2\sqrt{5}\ i\right)$$

Все множители неприводимые $\Rightarrow$ A не является гауссовым кольцом, ни один из этих множителей не является простым по определению простого числа.

Определение.

Коммутативное кольцо A с единицей называется упорядоченным кольцом тогда и только тогда, когда существует непустое подмножество A^+ кольца A, называют подмножеством положительных элементов кольца A таких, что

а) если $a, b \in A^+$, то $a + b \in A^+$;

б) если $a, b \in A^+$, то $a \cdot b \in A^+$;

в) для заданного элемента $a \in A$ выполняется одно и только одно из альтернативных условий:

(1) $a \in A^+$;

(2) $a = 0$;

(3) $-a \in A^+$.

Коммутативное кольцо с единицей, которое содержит такое множество A^+ , удовлетворяет аксиоме трихотомии:

Если a $\in A^+$, то $a>0$. Если $-a \in A^+$, то $a<0$.

Теорема.

Каждое упорядоченное кольцо является областью целостности. Для любого заданного $a \neq 0$ имеем $a^2 > 0$. В частности, $1^2 > 0 \Rightarrow 1>0$.

Определение.

Упорядоченная область целостности A называется вполне упорядоченной тогда и только тогда, когда любое непустое множество S множества A^+ имеет первый элемент, то есть существует такой элемент $s \in S$, Что если $t < s$, то $t \notin S$.

Теорема.

Если A – вполне упорядоченная область целостности, то не существует такой элемент c области A, что $0 < c < 1$.

Определение.

В упорядоченной области целостности пусть $\overline{n+1} = \overline{n} + 1$

где 1 – мультипликативная единица.

Теорема.

В любой неупорядоченной области целостности A для подмножества положительных элементов A^+ следующие утверждения эквивалентны:

1) Первый принцип индукции.

2) Принцип полного упорядочения.

3) Второй принцип индукции.

Теорема.

Любые две вполне упорядоченные области целостности являются изоморфными, поэтому они изоморфны Z.

Определение.

Область целостности называется минимальной областью тогда и только тогда, когда она не содержит никакой подобласти, кроме самой себя.

Минимальную область можно найти, построив пересечение всех подобластей области целостности.

Теорема.

Любые две упорядоченные минимальные области целостности изоморфны. Они изоморфны целым числам $\Rightarrow$ вполне упорядочены.

Полиномы.
Определение.

Пусть A - коммутативное кольцо с единицей и пусть *S* – множество всех последовательностей (a_0, a_1, a_2, …) элементов кольца *A* таких, что если $f \in S$, то существует целое число N_f, так что $a_j = 0$ для всех $j > N_f$. Если $f \in S$, то *f* – ***полином***, или ***полиномиальная форма*** над кольцом *A*.

Например,

$$(1,0,0,0,0,\ldots) \quad \text{и} \quad (1,1,1,0,0,0,\ldots)$$

принадлежат S, но

$$(1,1,1,1,1,1,1,1,\ldots) \quad \text{и} \quad (1,0,1,0,1,0,1,0,1,\ldots)$$

множеству S не принадлежат. Если $A = Z$, то

$$(0,-5,2,0,0,\ldots) \quad \text{и} \quad (3,7,5,8,0,0,\ldots)$$

являются полиномами из S.

Определение.

Пусть A – коммутативное кольцо с единицей и пусть

$f = (a_i)^* = (a_0 , a_1 , a_2 , \ldots)$ и $g = (b_i)^* = (b_0 , b_1 , b_2 , \ldots)$ принадлежат S, множеству полиномов над кольцом.

Сумма полиномов $f + g = (a_i + b_i)^* = (a_0 + b_0 , a_1 + b_1 , \ldots)$

Произведение полиномов $fg = (c_k)^*$, где

$$c_k = \sum_{i+j=k} a_i \cdot b_j$$

Теорема.

Пусть $f , g \in S$, S – подмножество полиномов над коммутативным кольцом A с единицей. Тогда $f + g \in S$ и $f \cdot g \in S$

Теорема.

Если S – множество полиномов над коммутативным кольцом A с единицей, то S – также коммутативное кольцо с единицей. Его единицей является (1, 0, 0, 0, …), а нулевым элементом - (0, 0, 0, 0, …).

Определение.

а) Пусть A – коммутативное кольцо с единицей, пусть $f \in S$ и $f = (a_i)^*$.

Для $f \neq 0$ пусть $\deg(f)$ равно наибольшему целому числу k такому, что $a_k \neq 0$. Функция $\deg(f)$ называется ***степенью полинома*** f . Множество S называется кольцом полиномов над кольцом A. Множество S обозначается $A[x]$.

Произвольный элемент множества $A[x]$ называется ***полиномом*** над кольцом A. Любой полином степени 0 или равный нулю называется ***константой***.

Теорема.

б) Пусть $f = (a_0 , a_1 , a_2 , \ldots)$ принадлежит $A[x]$. Члены последовательности a_i называются ***коэффициентами полинома*** f .

Если $f \neq 0$ и $n = \deg(f)$, то a_n называют ***старшим коэффициентом*** полинома f .

Если $a_n = 1$, то полином f называется ***нормированным***.

Если $f \neq 0$ обладает свойством: наибольший общий делитель всех его ненулевых коэффициентов равен единице, то f называется ***примитивным полиномом***.

в) Два элемента f и g множества $A[x]$ равны ($f = g$) , если равны их соответствующие коэффициенты: если $f = (a_0 , a_1 , a_2 , \ldots)$ и

$g = (b_0 , b_1 , b_2 , \ldots)$, то $f = g$ тогда и только тогда, когда $a_i = b_i$ для любого неотрицательного целого числа i .

г) Полином f делит полином g в то м случае, если существует такой полином h , что $f \cdot h = g$.

f и h являются делителями полинома g .

Например, если

$$f = (0, 1, 1, 0, 1, 0, 0, \ldots),$$

то $\deg(f) = 4$. Если

$$g = (1, 0, 0, 0, \ldots),$$

то $\deg(g) = 0$ и g — константа. Тождественно нулевой полином

$$(0, 0, 0, \ldots)$$

не имеет степени.

Теорема.

Пусть A – коммутационное кольцо с единицей, пусть $A[x]$ – кольцо полиномов над кольцом A и пусть f и g принадлежит $A[x]$.

а) Если f , $g \neq 0$, то $\deg(f + g) \leq \max(\deg(f), \deg(g))$.

б) Либо $fg = 0$, либо $\deg(fg) \leq \deg(f) + \deg(g)$.

в) Если A – область целостности, то либо $fg = 0$, либо $\deg(fg) = \deg(f) + \deg(g)$.

г) Если A – область целостности, то $A[x]$ - также область целостности.

Теорема.

Существует мономорфизм из A в $A[x]$, кольцо полиномов над кольцом A, для которого образ кольца A является подкольцом кольца $A[x]$.

Если A – область целостности, то каждый делитель единицы в $A[x]$ соответствует делителю единицы в A согласно мономорфизму.

Определение.

Символ Кронекера δ_{ij} для целых чисел i и j определяется:

$$\delta_{ij} = \begin{cases} 0, & \text{åñëè } i \neq j; \\ 1, & \text{åñëè } i = j. \end{cases}$$

Например, если $f = (a_0, a_1, a_2, \ldots)$, где $a_i = \delta_{i3}$, то

$$f = (0, 0, 0, 1, 0, 0, \ldots).$$

Если $g = \sum_{j=1}^{5} (\delta_{ij})^*$, то

$$g = (0, 1, 1, 1, 1, 1, 0, 0, \ldots).$$

Теорема.

Если $x = (0, 1, 0, 0, 0, \ldots) = (c_i)^*$, где $c_i = \delta_{ij}$, то для каждого $k > 0$: $x^k = (a_0 , a_1 , a_2 , \ldots)$, где $a_i = \delta_{ij}$

Определение.

Пусть A – коммутативное кольцо с единицей и пусть $A[x]$ – множество полиномов над кольцом A. Символ x называют переменной над кольцом A.

С каждым полиномом

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in A[x]$$

связана функция из A в A вида

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

или

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0,$$

которую называют ***полиномиальной функцией***.

Пусть $A(x) = \{f(x) : f \in S\}$.

Степень функции f(x) совпадает со степенью соответствующего полинома $f \in A[x]$. Элемент f множества $A[x]$ называют ***полиномиальной формой***.

Определение.

Пусть A – коммутативное кольцо с единицей. Если

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

и

$$g(x) = b_n x^n + \cdots + b_2 x^2 + b_1 x + b,$$

где некоторые из a_i и b_i из A могут быть 0, включая a_n или b_n, то

$$f(x) + g(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

и

$$f(x)g(x) = c_m x^m + \cdots + c_2 x^2 + c_1 x + c_0,$$

где $c_k = \sum_{i+j=k} a_i b_j$.

$f(x) = g(x)$ только тогда, когда $f(b) = g(b)$ для всех $b \in A$.

Решением уравнения $f(x) = 0$ называется элемент $a \in A$ такой, что $f(a) = 0$.

Теорема.

Если $f(x)$ и $g(x)$ – полиномиальные функции над областью целостности A, степень $f(x)$ равна n, а степень $g(x)$ равна m, то:

а) степень $f(x) + g(x)$ меньше или равна $\max\{m, n\}$;

б) степень $f(x) \cdot g(x)$ равна $m + n$.

Теорема.

Если f - полином степени n над бесконечной областью целостности и $f(x)$ – соответствующая полиномиальная функция, то уравнение $f(x) = 0$ имеет не более n решений.

Следствие.

Пусть $f(x) = a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0$ – полиномиальная функция над бесконечной областью целостности A.

Если $f(a) = 0$ для всех $a \in A$, то $a_0 = a_1 = a_2 = \ldots = a_n = 0$.

Теорема.

Пусть f и g – полиномы над бесконечной областью целостности A. Тогда $f = g$ тогда и только тогда, когда соответствующие полиномиальные функции $f(x)$ и $g(x)$ обладают таким свойством, что $f(b) = g(a)$ для всех $b \in A$.

Теорема.

Пусть A – бесконечная область целостности. Определим q :

$A[x] \to A(x)$ соотношение $q(f) = f(x)$. Тогда функция q является изоморфизмом.

Пример.

Множество $Z_5 = \{[0], [1], [2], [3], [4]\}$ классов вычетов по модулю 5 является полем, поэтому .лредставляет собой область целостности. По теореме Ферма, если для простого числа p имеем $a \not\equiv 0 \pmod{p}$, то $a^{p-1} \equiv 1 \pmod{p}$. Тогда $a^p \equiv a \pmod{p}$ для любого целого числа a, даже если $a \equiv 0 \pmod{p}$. Для $p = 5$ имеем $a^5 \equiv a \pmod{5}$ для всех $a \in Z$. Это сравнение равносильно $[a]^5 = [a]$ или $[a]^5 - [a] = [0]$ для любого целого числа a. Таким образом, если $g(x) = x^5 - x$, то $g(x) = [0]$ выполняется для любого x из Z_5. Однако, если h — полином, равный нулю, то $h(x) = [0]$ для всех x из Z_5. Полиномы g и h не равны, но $g(b) = h(b)$ для всех b из области целостности Z. Таким образом, над конечной областью целостности равенство полиномиальных форм не эквивалентно равенству полиномиальных функций. С другой стороны, поскольку множество целых чисел бесконечно, то понятия равенства для полиномиальных форм и полиномиальных функций над Z совпадают.

Последний слайд лекции

!!.