Лекция 9. Кольца. Теорема о конечном целостном кольце. Характеристика кольца. Кольцо многочленов. Наследование свойств кольца в кольце многочленов. Деление с остатком многочленов над полем.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.su

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.su

Кольцо

Пусть на множестве S заданы две алгебраические операции: сложение $+$ и умножение $\cdot$.
Структура $R = (S; +, \cdot)$ называется **кольцом**, если
1) множество S с операцией сложения $+$ является **коммутативной группой**, т.е.
а) операция сложения $+$ коммутативна и ассоциативна;
б) существует нулевой (нейтральный) элемент 0 относительно операции сложения $+$;
в) для каждого элемента $a \in S$ найдется противоположный (симметричный) элемент $-a \in S$ относительно операции сложения $+$;
2) выполнены свойства **дистрибутивности**, т.е. для любых элементов $a, b, c \in S$ верно

$$a \cdot (b + c) = a \cdot b + a \cdot c;$$
$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Виды колец

Пусть $R = (S; +, \cdot)$ — кольцо. Кольцо R называется

– **коммутативным** (**ассоциативным**) кольцом, если операция умножения $\cdot$ коммутативна (ассоциативна);

– **кольцом с единицей**, если в нем есть единичный элемент $1 \in S$ (т.е. нейтральный элемент по умножению $\cdot$);

– **кольцом без делителей нуля**, если для любых элементов $a, b \in S$ из равенства $a \cdot b = 0$ следует $a = 0$ или $b = 0$;

– **целостным кольцом**, если $S \neq \{0\}$, и оно коммутативно, ассоциативно, с единицей и без делителей нуля;

– **полем**, если $S \neq \{0\}$, и множество $S \setminus \{0\}$ с операцией умножения $\cdot$ образует коммутативную (мультпликативную) группу.

Примеры колец

1. Кольцо $R_1 = (\mathbb{Z}; +, \cdot)$ сложения и умножения целых чисел является коммутативным, ассоциативным кольцом с единицей и без делителей нуля, т.е. целостным кольцом. Но не полем, т.к., например, для элемента 2 нет обратного по умножению элемента в множестве целых чисел.

2. Кольцо $R_2 = (\mathbb{Z}_4; + \pmod 4, \cdot \pmod 4)$ сложения и умножения остатков по модулю 4 является коммутативным, ассоциативным кольцом с единицей, но с делителями нуля, т.к. в этом кольце верно $2 \cdot 2 = 0$.

3. Кольцо $R_3 = (\mathbb{Z}_2; + \pmod 2, \cdot \pmod 2)$ сложения и умножения остатков по модулю 2 является коммутативным, ассоциативным кольцом с единицей и с обратным элементом по умножению для каждого его элемента, кроме нуля 0, т.е. является полем.

Теорема о конечном целостном кольце

Теорема 1 (о конечном целостном кольце). *Конечное целостное кольцо является полем.*

Доказательство. Пусть кольцо $R = (S; +, \cdot)$ является конечным ($S \neq \{0\}$) и целостным.

Тогда для множества $S \setminus \{0\}$ с операцией умножения $\cdot$ верно:

1) операция $\cdot$ коммутативна и ассоциативна;

2) существует единичный (нейтральный) элемент 1 по умножению $\cdot$.

Осталось только доказать, что для каждого элемента $a \in S \setminus \{0\}$ найдется обратный к нему элемент a^{-1} относительно умножения, т.е. что верно

$$a \cdot a^{-1} = 1.$$

В силу коммутативности операции умножения также $a^{-1} \cdot a = 1$.

Теорема о конечном целостном кольце

Доказательство. Пусть $S \setminus \{0\} = \{b_1, b_2, \ldots, b_k\}$. Рассмотрим элементы

$$a \cdot b_1, a \cdot b_2, \ldots, a \cdot b_k.$$

В этой последовательности все элементы ненулевые, т.к. в кольце R нет делителей нуля. Докажем от противного, что в ней все элементы разные: пусть для некоторых элементов b_i и b_j, $b_i \neq b_j$, верно $a \cdot b_i = a \cdot b_j$.
Тогда по свойствам кольца

$$a \cdot b_i - a \cdot b_j = 0, \ a \cdot (b_i - b_j) = 0.$$

Т.к. $a \neq 0$, и в кольце R нет делителей нуля, верно $b_i = b_j$ — противоречие.
Значит, среди элементов последовательности встречаются **все** элементы множества $S \setminus \{0\}$, поэтому $a \cdot b_l = 1$ для некоторого элемента $b_l \in S$. Т.е. $b_l = a^{-1}$. □

Простые поля

Следствие 1.1 *Кольцо* $R = (\mathbb{Z}_p; + \pmod p, \cdot \pmod p)$ *сложения и умножения остатков по модулю* p*, где* p *— простое число, является полем.*

Будем обозначать это конечное поле как $\mathbb{F}_p$ и называть **простым полем** из p элементов, т.е.

$$\mathbb{F}_p = (\mathbb{Z}_p; + \pmod p, \cdot \pmod p),$$

где p — простое число.

Характеристика кольца

Пусть $R = (S; +, \cdot)$ — кольцо.
Наименьшее натуральное число n (если оно существует), что для каждого элемента $a \in S$ верно $na = 0$, называется **характеристикой** кольца R.

В этом случае говорят, что кольцо R — с **положительной** характеристикой.

Если таких натуральных чисел нет, то говорят, что кольцо R — с **нулевой** характеристикой.

Характеристика кольца

Теорема 2. *Характеристика конечного целостного кольца положительна и является простым числом*.

Доказательство. Рассмотрим единицу e конечного целостного кольца R. Тогда в последовательности

$$e, 2e, \ldots, ne, \ldots$$

найдутся такие натуральные числа i и j, $i < j$, что

$$ie = je.$$

Отсюда, $(j - i)e = 0$. Тогда для каждого элемента $a \in R$ верно

$$(j - i)a = (j - i)(e \cdot a) = ((j - i)e) \cdot a = 0.$$

Т.е. кольцо R — с положительной характеристикой.

Характеристика кольца

Доказательство.
Пусть n — положительная характеристика конечного целостного кольца R. Докажем от противного, что она является простым числом.
Пусть $n = k \cdot m$, где $k, m > 1$. Тогда

$$0 = ne = (k \cdot m)e = (ke) \cdot (me).$$

Т.к. в целостном кольце R нет делителей нуля, верно $ke = 0$ или $me = 0$, что противоречиит тому, что n — наименьшее из таких чисел.

□

Характеристика конечного поля

Следствие 2.1. *Характеристика каждого конечного поля положительна и является простым числом*.

Многочлены над кольцом

Пусть $R = (S; +, \cdot)$ — кольцо.
Многочленом $f(x)$ над кольцом R называется формальное выражение

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i,$$

где $a_n, a_{n-1}, \ldots, a_1, a_0 \in S$, а x — переменная, $x \notin S$.
При этом элементы $a_i \in S$ называются **коэффициентами** при **степенях** x^i. Если для какой-то степени x^i верно $a_i = 0$, то при записи это слагаемое можно пропускать.

Два многочлена $f(x) = \sum_{i=0}^{n} a_i x^i$ и $g(x) = \sum_{i=1}^{n} b_i x^i$ над одним и тем же кольцом R называются **равными**, если $a_i = b_i$ для каждого индекса $i = 0, 1, \ldots, n$.

Многочлены над кольцом

Множество многочленов переменной x над кольцом R обозначается как $R[x]$.

Для многочлена $f(x) \in R[x]$ такое наибольшее число n, что $a_n \neq 0$, называется его **степенью** и обозначается $\deg(f)$. Если $\deg(f) = n$, то степень x^n называется **старшей степенью**, а коэффициент при ней a_n — **старшим коэффициентом** многочлена $f(x)$.
По определению полагают, что степень многочлена $0 \in R[x]$, все коэффициенты которого нулевые, равна $-\infty$, т.е.

$$\deg(0) = -\infty.$$

Если степень многочлена равна 0 или $-\infty$, то такой многочлен называется **постоянным**. Такой многочлен является элементом кольца:

$$f(x) = a_0 \in R.$$

Операции над многочленами

Для многочленов $f(x) = \sum_{i=0}^{n} a_i x^i$ и $g(x) = \sum_{j=0}^{m} b_j x^j$ над кольцом R их **суммой** назовем многочлен

$$(f+g)(x) = \sum_{k=0}^{\max(n,m)} c_k x^k \in R[x],$$

где $c_k = a_k + b_k \in R$;

а их **произведением** назовем многочлен

$$(f \cdot g)(x) = \sum_{l=0}^{n+m} d_l x^l \in R[x],$$

где $d_l = \sum_{i+j=l} a_i b_j \in R$.

Предложение 1. *Если* $f, g \in R[x]$, *то*

$$\deg(f+g) \le \max(\deg(f), \deg(g)),$$
$$\deg(f \cdot g) \le \deg(f) + \deg(g).$$

Кольцо многочленов

Теорема 3. *Множество $R[x]$ многочленов над кольцом R с операциями сложения и умножения многочленов является кольцом.*

Доказательство. Свойства кольца.

1) Множество $R[x]$ с операцией сложения многочленов $+$ является коммутативной группой:

а) коммутативность и ассоциативность сложения многочленов: по коммутативности и ассоциативности операции сложения в кольце R;

б) существование нулевого многочлена по сложению: $0 \in R[x]$;

в) для каждого многочлена $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ найдется противоположный многочлен по сложению: $-f(x) = \sum_{i=1}^{n} (-a_i) x^i \in R[x]$.

2) Дистрибутивность: по свойствам дистрибутивности в кольце R.

Кольцо многочленов

Кольцо многочленов переменной x над кольцом R обозначается как $R[x]$.
Какие свойства кольца R наследуются в кольце $R[x]$?

Теорема 4. *Пусть R — кольцо, а $R[x]$ — кольцо многочленов над кольцом R. Тогда*

– если кольцо R — коммутативно (ассоциативно), то кольцо $R[x]$ — коммутативно (ассоциативно);

– если кольцо R — с единицей, то кольцо $R[x]$ — с единицей;

– если кольцо R — целостное, то кольцо $R[x]$ — целостное.

Кольцо многочленов

Доказательство. Докажем от противного наследование отсутствия делителей нуля: пусть для многочленов $f(x) = \sum_{i=0}^{n} a_i x^i \neq 0$, $\deg f = n$, и $g(x) = \sum_{j=0}^{m} b_j x^j \neq 0$, $\deg g = m$, верно

$$f \cdot g = 0.$$

Т.е. для каждого индекса $l = 0, 1, \ldots, n + m$ верно

$$\sum_{i+j=l} a_i \cdot b_j = 0.$$

Рассмотрим индекс $l = n + m$. Тогда

$$a_n \cdot b_m = 0,$$

противоречие, т.к. $a_n \neq 0$, $b_n \neq 0$, и в кольце R нет делителей нуля. $\square$

Кольцо многочленов

Следствие 4.1. *Если R — целостное кольцо, и $f(x), g(x) \in R[x]$, то*

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Деление с остатком многочленов над полем

Теорема 5 (о делении с остатком многочленов над полем).
Пусть F — поле, и $F[x]$ — кольцо многочленов над полем F. Тогда для любых многочленов $f(x), g(x) \in F[x]$, $f(x) \neq 0$, $g(x) \neq 0$, найдутся такие однозначные многочлены $q(x), r(x) \in F[x]$, что

$$f(x) = g(x) \cdot q(x) + r(x), \ \deg(r) < \deg(g).$$

Деление с остатком многочленов над полем

Доказательство существования таких многочленов $q(x), r(x) \in F[x]$ проведем индукцией по степени $\deg(f)$.

Базис индукции: $0 \leq \deg(f) < \deg(g)$. Положим $q(x) = 0$, $r(x) = f(x)$. Тогда

$$f(x) = 0 \cdot g(x) + f(x), \ \deg(f) < \deg(g).$$

Деление с остатком многочленов над полем

Доказательство. *Индуктивный переход*: пусть для всех многочленов $f(x) \in F[x]$ степени, меньшей n, и для всех многочленов $g(x) \in F[x]$, $\deg(g) \leq \deg(f)$, теорема верна. Расммотрим многочлен $f(x) \in F[x]$, $\deg(f) = n$:

$$f(x) = \sum_{i=0}^{n} a_i x^i, \ a_n \neq 0.$$

Пусть

$$g(x) = \sum_{j=0}^{m} b_j x^j, \ b_m \neq 0,$$

$\deg(g) = m \leq n = \deg(f)$.

Деление с остатком многочленов над полем

Доказательство. Тогда для многочлена

$$f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} \cdot g(x) = \sum_{k=0}^{n-1} \left(a_k - \frac{a_n b_k}{b_m} \right) x^k$$

верно предположение индукции, т.к. $\deg(f_1) \leq n-1$. Поэтому найдутся такие многочлены $q_1(x), r(x) \in F[x]$, что

$$f_1(x) = g(x) \cdot q_1(x) + r(x), \ \deg(r) < \deg(g).$$

Отсюда

$$f(x) = g(x) \cdot \left(\frac{a_n}{b_m} x^{n-m} + q_1(x) \right) + r(x), \ \deg(r) < \deg(g),$$

т.е. $q(x) = \frac{a_n}{b_m} x^{n-m} + q_1(x)$.

Деление с остатком многочленов над полем

Доказательство единственности: пусть найдутся такие многочлены $q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$, что

$$f(x) = g(x) \cdot q_1(x) + r_1(x),\ \deg(r_1) < \deg(g);$$
$$f(x) = g(x) \cdot q_2(x) + r_2(x),\ \deg(r_2) < \deg(g).$$

Тогда

$$g(x) \cdot q_1(x) + r_1(x) = g(x) \cdot q_2(x) + r_2(x),$$

и

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

Т.к. $\deg(r_2 - r_1) < \deg(g)$ и F — поле, а значит, и целостное кольцо, верно $r_2(x) - r_1(x) = 0$. Далее из целостности поля F верно $q_1(x) - q_2(x) = 0$.

□

Деление с остатком многочленов над полем

Пример. Поделим с остатком многочлен $f(x) = x^4 \in \mathbb{F}_2[x]$ на многочлен $x^2 + 1 \in \mathbb{F}_2[x]$:

$$\begin{array}{l|l} x^4 & x^2+1 \\ \underline{x^4 + x^2} & \hline x^2+1 \\ \quad x^2 & \\ \quad \underline{x^2 + 1} & \\ \quad\quad 1 & \end{array}$$

Т.е. частное — многочлен $q(x) = x^2 + 1$, остаток — многочлен $r(x) = 1$, $0 = \deg(r) < \deg(f) = 2$, и

$$x^4 = (x^2 + 1)(x^2 + 1) + 1.$$

Задачи для самостоятельного решения

1. Доказать, что если R — коммутативное и ассоциативное кольцо с простой характеристикой p, то

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

для всех $a, b \in R$ и всех целых n, $n \geq 1$.

2. Останется ли теорема 5 верной, если вместо многочленов над полем рассматривать многочлены над целостным кольцом. Ответ пояснить.

3. Поделить с остатком многочлен $f(x) = x^7 + 1 \in \mathbb{F}_2[x]$ на многочлен $g(x) = x^5 + x^3 + x + 1 \in \mathbb{F}_2[x]$.

4. Поделить с остатком многочлен $f(x) = 2x^5 + x^4 + 4x + 3 \in \mathbb{F}_5[x]$ на многочлен $g(x) = 3x^2 + 1 \in \mathbb{F}_5[x]$.

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Гл. 1, с. 24–26, 29–30, 33–35.

Конец лекции