Лекция: Кольца. Теорема о конечном целостном кольце. Кольцо многочленов. Подкольцо. Идеал кольца. Главный идеал кольца. Кольцо главных идеалов. Деление с остатком многочленов над полем. Теорема о кольце многочленов над полем. Вычеты по модулю идеала. Фактор-кольцо.

Лектор - доцент Селезнева Светлана Николаевна

Лекции по “Избранным вопросам дискретной математики”.
3-й курс, группа 318,
факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.su

Кольца

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 **абелевой 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 $a, b \in S$ равенство $a \cdot b = 0$ влечет, что или $a = 0$, или $b = 0$;

- **целостным кольцом**, если оно коммутативно, ассоциативно, с единицей и без делителей нуля;

- **полем**, если в нем $S \neq \{0\}$, и множество $S \setminus \{0\}$ с операцией умножения $\cdot$ образует абелеву (мультипликативную) группу.

Примеры колец

Примеры.

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, что $2 \cdot 2 = 0$.

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 будет 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.
Откуда 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* $R = (\mathbb{Z}_p; +(\mathrm{mod}\ p), \cdot(\mathrm{mod}\ p))$ *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.

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

где p – простое число.

Многочлены над кольцом

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

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

где $a_n, a_{n-1}, \ldots, a_1, a_0 \in S$, а x – символ переменной, $x \notin S$.
При этом элементы $a_i \in S$ называются **коэффициентами** при **степенях** x^i. Если при какой-то степени x^i коэффициент $a_i = 0$, 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 $f(x) \in R[x]$ наибольшее число n, такое что коэффициент $a_n \neq 0$ 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

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

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

Теорема 2. *Если* $f, g \in R[x]$, *то*

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

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 абелевой 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 $R[x]$.
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. 3) 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

$$f g = 0.$$

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

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

Рассмотрим индекс $l = n + m$. Тогда

$$a_n b_m = 0,$$

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

Кольцо многочленов

Теорема 5. *Если R – целостное кольцо, и $f(x), g(x) \in R[x]$, $f, g \neq 0$, то*

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

Подкольцо кольца

Пусть $R = (S; +, \cdot)$ – кольцо, и $T \subseteq S$.

Структура $K = (T; +, \cdot)$ называется **подкольцом** кольца R, если множество T с операциями сложения $+$ и умножения $\cdot$ является кольцом.

Теорема 6. *Пусть $R = (S; +, \cdot)$ – кольцо. Множество $T \subseteq S$ с алгебраическими операциями сложения $+$ и умножения $\cdot$ на нем является подкольцом кольца R тогда и только тогда, когда для любых элементов $a, b \in T$ верно $a - b \in T$.*

Доказательство. Применим критерий подгруппы.

□

Пример подкольца

Пример. В кольце $R = (\mathbb{Z}; +; \cdot)$ сложения и умножения целых чисел множество четных чисел

$$\mathbb{Z}_{even} = \{2z \mid z \in \mathbb{Z}\}$$

с операциями сложения и умножения является подкольцом, т.к. для любых четных чисел $v_1, v_2 \in \mathbb{Z}_{even}$ верно

$$v_1 - v_2 \in \mathbb{Z}_{even}.$$

Идеал кольца

Пусть $R = (S; +, \cdot)$ – кольцо, и $T \subseteq S$.

Структура $J = (T; +, \cdot)$ называется **идеалом** кольца R, если

1) J является *подкольцом* кольца R;
2) для любых элементов $a \in R$ и $h \in J$ верно

$$a \cdot h \in J \text{ и } h \cdot a \in J.$$

Пример идеала кольца

Пример. Подкольцо $J = (\mathbb{Z}_{even}; +, \cdot)$ сложения и умножения четных чисел кольца $R = (\mathbb{Z}; +; \cdot)$ сложения и умножения целых чисел является его идеалом, т.к. для любых целях чисел $z \in \mathbb{Z}$ и четных чисел $v \in \mathbb{Z}_{even}$ их произведение $z \cdot v$ четно, т.е.

$$z \cdot v \in \mathbb{Z}_{even}.$$

Главный идеал кольца

Пусть $R = (S; +, \cdot)$ – кольцо коммутативное и ассоциативное кольцо с единицей, и $J = (T; +, \cdot)$, $T \subseteq S$, – его идеал.

Идеал J называется **главным идеалом** кольца R, если найдется такой элемент $a \in S$, что

$$J = \{a \cdot s \mid s \in S\}.$$

Т.е. это множество всех элементов кольца R, „кратных“ элементу a.

Главный идеал по элементу $a \in R$ обозначается как (a).

Пример главного идеала кольца

Пример. Идеал $J = (\mathbb{Z}_{even}; +, \cdot)$ сложения и умножения четных чисел кольца $R = (\mathbb{Z}; +; \cdot)$ сложения и умножения целых чисел является его главным идеалом по элементу $2 \in \mathbb{Z}$, т.к.

$$\mathbb{Z}_{even} = \{2z \mid z \in \mathbb{Z}\}.$$

Т.е. $J = (2)$.

Кольцо главных идеалов

Кольцо $R = (S; +, \cdot)$ называется **кольцом главных идеалов**, если

1) кольцо R является целостным;
2) каждый его идеал является главным.

Деление с остатком многочленов над полем

Мы докажем, что кольцо многочленов над **полем** является кольцом главных идеалов.

Но сначала докажем вспомогательную теорему о делении с остатком многочленов над полем.

Теорема 7 (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

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

Деление с остатком многочленов над полем

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

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

Откуда

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

Деление с остатком многочленов над полем

Доказательство единственности: пусть найдутся такие многочлены $q_1(x), r_1(x), q_2(x), r_2(x) \in F[x]$, 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, в частности, целостное кольцо, верно $r_2(x) - r_1(x) = 0$. Получаем

$$g(x)(q_1(x) - q_2(x)) = 0.$$

Откуда из целостности поля F верно $q_1(x) - q_2(x) = 0$. $\square$

Пример деления с остатком многочленов над полем

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

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

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

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

Кольцо главных идеалов

Теорема 8. *Кольцо многочленов над полем является кольцом главных идеалов.*

Доказательство. Пусть $F = (S; +, \cdot)$ – поле, и $F[x]$ – кольцо многочленов над полем F.
По теореме о наследовании свойств в кольце многочленов кольцо $F[x]$ является целостным кольцом (т.к. наследуется свойство целостности поля F).
Осталось доказать, что каждый идеал кольца $F[x]$ является главным идеалом.
Рассмотрим J – идеал кольца многочленов $F[x]$. Выберем в идеале J многочлен $g(x) \in J$, $g(x) \neq 0$, с минимальной степенью среди всех ненулевых многочленов этого идеала.
Докажем, что

$$J = (g).$$

Кольцо главных идеалов

Доказательство. Пусть $f(x) \in J$, $f(x) \neq 0$. Поделим с остатком многочлен $f(x) \in F[x]$ на многочлен $g(x) \in F[x]$:

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

Тогда

$g(x) \cdot q(x) \in J$ (почему?), и $r(x) = f(x) - g(x) \cdot q(x) \in J$ (почему?).

Т.к. $g(x) \in J$ – многочлен идеала J с минимальной степенью среди ненулевых его многочленов, верно $r(x) = 0$.

Т.е. $f(x) = g(x) \cdot q(x)$.

□

Классы вычетов по модулю идеала

Пусть $R = (S; +, \cdot)$ – кольцо, и $J = (T; +, \cdot)$, $T \subseteq S$ – его идеал.

Т.к. $J = (T; +, \cdot)$ – является, в частности, подкольцом кольца R, то $H = (T; +)$ – нормальная подгруппа аддитивной абелевой группы $G = (S; +)$ кольца R.

Пусть $a \in R$. **Классом вычетов по модулю идеала** J кольца R называется смежный класс аддитивной группы G кольца R по нормальной ее подгруппе H и обозначается $[a]_J$. Т.е.

$$[a]_J = a + J = \{a + h \mid h \in J\}.$$

Пример классов вычетов по модулю идеала

Пример. В кольце $R = (\mathbb{Z}, +, \cdot)$ сложения и умножения целых чисел рассмотрим идеал $J = (\mathbb{Z}_{even}, +, \cdot)$ сложения и умножения четных чисел.
Тогда есть всего два класса вычетов кольца R по модулю идеала J:

$$[0]_J = 0 + J = J = \{2z \mid z \in \mathbb{Z}\},$$

и

$$[1]_J = 1 + J = \{1 + 2z \mid z \in \mathbb{Z}\}.$$

Классы вычетов по модулю идеала

Т.к. подгруппа $H = (S; +)$ идеала $J = (T; +, \cdot)$ является **нормальной** подгруппой аддитивной абелевой группы $G = (S; +)$ кольца $R = (S; +, \cdot)$, $T \subseteq S$, то (по теореме) фактор-множество классов вычетов по модулю идеала J с операцией их сложения

$$[a]_J + [b]_J = [a + b]_J, \text{ где } a, b \in R,$$

является группой (фактор-группой G/H).

Эта фактор-группа G/H является абелевой (почему?).

Классы вычетов по модулю идеала

Пусть $R = (S; +, \cdot)$ – кольцо, и $J = (T; +, \cdot)$, $T \subseteq S$, – его идеал.
Введем операцию **умножения** классов вычетов по модулю идеала J. Если $a, b \in R$, то положим

$$[a]_J \cdot [b]_J = [a \cdot b]_J.$$

Теорема 9. *Введенная операция умножения классов вычетов по модулю идеала корректна*.
Доказательство. Пусть $a, b \in R$. Тогда

$$\begin{aligned}
[a]_J \cdot [b]_J &= \{a + h_1 \mid h_1 \in J\}\{b + h_2 \mid h_2 \in J\} = \\
&= \{(a + h_1)(b + h_2) \mid h_1, h_2 \in J\} = \\
&= \{ab + ah_2 + h_1 b + h_1 h_2 \mid h_1, h_2 \in J\} = \\
&= \{ab + h \mid h \in J\} \text{ (почему?) } = [ab]_J.
\end{aligned}$$

Фактор-кольцо

Теорема 10. *Множество классов вычетов по модулю идеала* $J = (T; +, \cdot)$ *кольца* $R = (S; +, \cdot)$, $T \subseteq S$, *с операциями их сложения и умножения является кольцом.*

Доказательство. Свойства кольца.

1) Множество классов вычетов по модулю идеала с операцией их сложения является абелевой группой – по теореме 3.3 это фактор-группа аддитивной абелевой группы кольца R по нормальной ее подгруппе идеала J;

2) Дистрибутивность – верно по дистрибутивности операций сложения $+$ и умножения $\cdot$ кольца R.

□

Кольцо вычетов по модулю идеала J кольца R называется **фактор-кольцом** кольца R по модулю идеала J и обозначается R/J.

Задачи для самостоятельного решения

1. Поделить с остатком многочлен $f(x)$ на многочлен $g(x)$, если

1) $f(x) = x^4 + x^2 + 1$, $g(x) = x^2 + 1$, $f, g \in \mathbb{F}_2[x]$;
2) $f(x) = x^3 + 2x^2 + 2$, $g(x) = 2x^2 + 1$, $f, g \in \mathbb{F}_3[x]$;
3) $f(x) = 3x^4 + 2$, $g(x) = 4x^2 + 1$, $f, g \in \mathbb{F}_5[x]$;
4) $f(x) = 5x^3 - 3$, $g(x) = 4x - 5$, $f, g \in \mathbb{F}_7[x]$.

2. Является ли $J = (T; +, \cdot)$ идеалом кольца $R = (S; +, \cdot)$, если

1) R – кольцо целых чисел с операциями сложения и умножения по модулю 3, а T – множество всех целых чисел, кратных 3;
2) R – кольцо целых чисел с операциями сложения и умножения по модулю 4, а T – множество всех целых чисел, дающих при делении на 4 остаток 1?

При положительном ответе дополнительно выяснить, является ли этот идеал главным.

Задачи для самостоятельного решения

3. 1) Если J_1 и J_2 – идеалы кольца R, то будут ли идеалами $J_1 \cup J_2$, $J_1 \cap J_2$, $J_1 \setminus J_2$?
2) Если J_1 и J_2 – **главные** идеалы коммутативного и ассоциативного кольца с единицей R, то будут ли идеалами $J_1 \cup J_2$, $J_1 \cap J_2$, $J_1 \setminus J_2$?
При положительном ответе дополнительно выяснить общий вид элементов новых главных идеалов.

4. Построить фактор-кольцо кольца целых чисел с операциями сложения и умножения относительно его идеала, содержащего все целые числа, кратные 5. Сколько элементов в полученном фактор-кольце? Является ли полученное фактор-кольцо **полем**?

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.

Конец лекции