Лекция 10. Идеалы, главные идеалы колец. Кольцо главных идеалов. Теорема о главном идеале кольца главных идеалов. Кольцо многочленов как кольцо главных идеалов. Построение конечных полей из p^n элементов, где p — простое число, $n \geq 2$.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.su

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 1. *Пусть $R = (S; +, \cdot)$ — кольцо. Множество $T \subseteq S$ с операциями сложения $+$ и умножения $\cdot$ 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.

□

Подкольцо кольца

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

$$Z_{\text{четн}} = \{2z \mid z \in \mathbb{Z}\}$$

с операциями сложения и умножения является подкольцом, т.к. для любых четных чисел $v_1, v_2 \in Z_{\text{четн}}$ верно

$$v_1 - v_2 \in Z_{\text{четн}}.$$

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

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

Идеал кольца

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

$$z \cdot v \in Z_{\text{четн}}.$$

Главный идеал кольца

Пусть $R = (S; +, \cdot)$ — 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).

Главный идеал кольца

Пример. Идеал $J = (Z_{\text{четн}}; +, \cdot)$ 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.

$$Z_{\text{четн}} = \{2z \mid z \in \mathbb{Z}\}.$$

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.

Кольцо главных идеалов

Теорема 2. *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 кольцо $F[x]$ является целостным кольцом (т.к. наследуется свойство целостности поля F).

Осталось доказать, что каждый идеал кольца $F[x]$ является главным.

Рассмотрим J — идеал кольца многочленов $F[x]$. Выберем в идеале J многочлен $g(x) \in J$, $g(x) \neq 0$, с наименьшей 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

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

Т.к. $g(x) \in J$ — многочлен идеала J с наименьшей степенью среди его ненулевых 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 коммутативной 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.

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

Классы вычетов по модулю идеала

Пример. В кольце $R = (\mathbb{Z}, +, \cdot)$ сложения и умножения целых чисел рассмотрим идеал $J = (Z_{\text{четн}}, +, \cdot)$ 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 коммутативной группы $G = (S; +)$ кольца $R = (S; +, \cdot)$, $T \subseteq S$, 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 коммутативной.

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 3. *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 4. *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 коммутативной группой: это фактор-группа аддитивной коммутативной 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 как R/J.

Обратимые элементы кольца

Пусть $R = (S; +, \cdot)$ — коммутативное, ассоциативное кольцо с единицей 1.
Элемент $a \in S$ называется **обратимым** (в кольце R), если в кольце R найдется обратный к нему элемент, т.е. такой элемент $b = a^{-1} \in S$, что

$$a \cdot b = 1.$$

Иначе, элемент $a \in S$ называется **не обратимым** элементом (кольца R).

Пример. В кольце $R = (\mathbb{Z}, +, \cdot)$ сложения и умножения целых чисел есть только два обратимых элемента: 1 и -1, остальные элементы — не обратимы.

Простые элементы кольца

Пусть $R = (S; +, \cdot)$ — коммутативное, ассоциативное кольцо с единицей 1.
Элемент $a \in S$ называется **простым**, или **неразложимым** (в кольце R), если он не обратим в этом кольце, и в любом разложении вида

$$a = b \cdot c, \text{ где } b, c \in R,$$

или элемент b — обратим, или элемент c — обратим.
Не обратимый элемент $a \in S$ называется **разложимым** (в кольце R), если найдутся такие не обратимые элементы $b, c \in R$, что

$$a = b \cdot c.$$

Простые элементы кольца

Пример. В кольце $R = (\mathbb{Z}, +, \cdot)$ сложения и умножения целых чисел элемент 3 является простым, т.к. он не обратим, и возможны только его разложения

$$3 = 3 \cdot 1 = (-3) \cdot (-1),$$

в которых элементы 1 и -1 обратимы; а элемент 10 является разложимым, т.к. он не обратим, и

$$10 = 2 \cdot 5,$$

и элементы 2 и 5 не обратимы.

Теорема о фактор-кольце кольца главных идеалов

Теорема 5. *Пусть* $R = (S; +, \cdot)$ — *кольцо главных идеалов, и* $J = (c)$ — *его главный идеал по элементу* $c \in S$.
Фактор-кольцо R/J *кольца* R *по идеалу* $J = (c)$ *является полем тогда и только тогда, когда* c — *простой элемент кольца* R.
Доказательство. Пусть $R = (S; +, \cdot)$ — кольцо главных идеалов, и

$$J = (c) = \{c \cdot s \mid s \in S\}$$

его главный идеал по элементу $c \in S$.
1. Если $c \in S$ — обратимый элемент кольца R, то для единицы 1 верно $1 \in J = (c)$ (почему?).
Отсюда $J = R$ (почему?).
Поэтому фактор-кольцо R/J состоит из одного элемента $J = R = e$, и, значит, не поле.

Теорема о фактор-кольце кольца главных идеалов

Доказательство.
2. Если $c \in S$ — разложимый элемент кольца. т.е. $c = a \cdot b$, где $a, b \in S$ — не обратимые элементы кольца R, то докажем от противного, что для класса вычетов $[a]_J \in R/J$ нет обратного элемента в фактор-кольце R/J.
Пусть для некоторого элемента $x \in R$ верно $[a]_J \cdot [x]_J = [1]_J$.
Тогда

$$(a + J)(x + J) = a \cdot x + J = 1 + J = a \cdot x + (c) = 1 + (c).$$

Отсюда найдется такой элемент $y \in R$, что $a \cdot x + c \cdot y = 1$.
Но $c = a \cdot b$, поэтому

$$a \cdot x + a \cdot b \cdot y = 1, \text{ и } a \cdot (x + b \cdot y) = 1$$

противоречие, т.к. элемент a не обратим в кольце R.

Теорема о фактор-кольце кольца главных идеалов

Доказательство.

3. Если $c \in S$ — простой элемент кольца R, то докажем, что для каждого класса вычетов $[a]_J \in R/J$, где $[a]_J \neq [0]_J = J$, найдется обратный к нему элемент в фактор-кольце R/J.

Рассмотрим множество

$$T = \{a \cdot x + c \cdot y \mid x, y \in S\}.$$

Докажем, что оно является идеалом кольца R.

1) Множество T с операциями сложения $+$ и умножения $\cdot$ является подкольцом кольца R по критерию подкольца, т.к.

$$(ax_1+cy_1)-(ax_2+cy_2) = a(x_1-x_2)+c(y_1-y_2) = ax_3+cy_3, \text{где } x_3, y_3 \in R.$$

2) Если $z \in S$, то

$$(ax + cy) \cdot z = axz + cyz = ax_1 + cy_1, \text{ где } x_1, y_1 \in R.$$

Значит, T — идеал кольца R.

Теорема о фактор-кольце кольца главных идеалов

Доказательство. Т.к. R — кольцо главных идеалов, найдется такой элемент $b \in S$, что $T = (b)$.
Заметим, что

$$c = a \cdot 0 + c \cdot 1 \in T.$$

Поэтому, $c = b \cdot d$ для некоторого элемента $d \in R$.
Но в кольце R элемент c — простой, поэтому или элемент b — обратим, или элемент d — обратим в кольце R.

Теорема о фактор-кольце кольца главных идеалов

Доказательство. Рассмотрим два случая.
1) Если b — обратимый элемент кольца R, то для единицы 1 верно $1 \in T$ (почему?). Отсюда найдутся такие элементы $x, y \in R$, что

$$a \cdot x + c \cdot y = 1.$$

И $([a]_J)^{-1} = [x]_J$, т.к. в этом случае

$$[a]_J \cdot [x]_J = [a \cdot x]_J = a \cdot x + J = 1 + J = [1]_J.$$

2) Если d — обратимый элемент кольца R, то $b = c \cdot d^{-1}$. Заметим, что

$$a = a \cdot 1 + c \cdot 0 \in T.$$

Поэтому, $a = b \cdot d_1$ для некоторого элемента $d_1 \in R$. Отсюда

$$a = b \cdot d_1 = (c \cdot d^{-1}) \cdot d_1 = c \cdot d_2, \text{ где } d_2 \in R.$$

Или $a \in (c) = J$, и $[a]_J = J = [0]_J$ — противоречие. Значит, этот случай невозможен. □

Простые и разложимые элементы кольца многочленов

Пример. Пусть $\mathbb{F}_p$ — поле из p элементов, где p — простое число, и $\mathbb{F}_p[x]$ — кольцо многочленов над полем $\mathbb{F}_p$.

Обратимыми элементами кольца $\mathbb{F}_p[x]$ являются ненулевые постоянные многочлены (многочлены степени 0), т.е. многочлены

$$1, 2, \ldots, p-1 \in \mathbb{F}_p[x].$$

Если многочлен $f(x)$ — **простой** элемент кольца $\mathbb{F}_p[x]$, то в любом разложении $f(x) = g(x) \cdot h(x)$ или $\deg(g) = 0$, или $\deg(h) = 0$. При этом многочлен $g(x)$ **неприводим** в кольце $\mathbb{F}_p[x]$ (или над полем $\mathbb{F}_p$).
Если многочлен $f(x)$ — **разложимый** элемент кольца $\mathbb{F}_p[x]$, то найдутся такие многочлены $g(x), h(x) \in \mathbb{F}_p[x]$, что $\deg(g) \geq 1$, $\deg(h) \geq 1$, и $f(x) = g(x) \cdot h(x)$. При этом многочлен $g(x)$ **приводим** в кольце $\mathbb{F}_p[x]$ (или над полем $\mathbb{F}_p$).

Неприводимые и приводимые многочлены над полем

Пример. В кольце $\mathbb{F}_2[x]$ многочлен $f(x) = x^2 + 1$ — приводим, т.к.

$$x^2 + 1 = (x + 1)(x + 1),\ \deg(x + 1) = 1,$$

а многочлен $g(x) = x^2 + x + 1$ — неприводим, т.к. его разложение с неопределенными коэффициентами $a, b \in \mathbb{F}_2$

$$x^2 + x + 1 = (x + a)(x + b)$$

приводит к несовместной в поле $\mathbb{F}_2$ системе уравнений:

$$\begin{cases} a + b = 1, \\ a \cdot b = 1. \end{cases}$$

Теорема о фактор-кольце кольца многочленов над полем

Теорема 6. *Пусть* $\mathbb{F}_p[x]$ *— кольцо многочленов над полем* $\mathbb{F}_p$, *где* p *— простое число, и многочлен* $g(x) \in \mathbb{F}_p[x]$.
Фактор-кольцо $\mathbb{F}_p[x]/(g)$ *кольца* $\mathbb{F}_p[x]$ *по модулю главного идеала* (g) *является полем тогда и только тогда, когда* $g(x)$ *— неприводимый многочлен в кольце* $\mathbb{F}_p[x]$.

Доказательство.

По теореме 2 кольцо $\mathbb{F}_p[x]$ является кольцом главных идеалов.
По теореме 5 фактор-кольцо $\mathbb{F}_p[x]/(g)$ является полем тогда и только тогда, когда $g(x)$ — простой, т.е. неприводимый многочлен в кольце $\mathbb{F}_p[x]$.

□

Конечные поля из p^n элементов

Пусть $g(x)$ — неприводимый в кольце $\mathbb{F}_p[x]$ многочлен, где $\mathbb{F}_p$ — поле из p элементов.
Тогда по теореме 6 фактор-кольцо $\mathbb{F}_p[x]/(g)$ — поле.

Элементы этого поля — классы вычетов $[f]_{(g)}$, $f(x) \in \mathbb{F}_p[x]$, по модулю идеала (g), т.е.

$$[f]_{(g)} = \{f(x) + g(x) \cdot h(x) \mid h(x) \in \mathbb{F}_p[x]\}.$$

В каком случае два многочлена $f_1(x), f_2(x) \in \mathbb{F}_p[x]$ принадлежат одному классу вычетов $[f]_{(g)}$? В том и только в том случае, когда у них **одинаковые** остатки при делении на многочлен $g(x)$.
Следовательно, элементов в поле $\mathbb{F}_p[x]/(g)$ столько, сколько **различных остатков** при делении на многочлен $g(x)$.

Конечные поля из p^n элементов

Пусть $\deg(g) = n$, т.е.

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

Тогда каждый остаток $r(x)$ при делении $g(x)$ имеет вид:

$$r(x) = \sum_{j=0}^{n-1} b_j x^j,$$

где $b_0, b_1, \ldots, b_{n-1}$ — какие-то элементы поля $\mathbb{F}_p$.
Когда коэффициенты $b_0, b_1, \ldots, b_{n-1} \in \mathbb{F}_p$ пробегают **все** свои возможные значения, мы получаем **все** возможные остатки при делении на многочлен $g(x)$.
Возможных остатков всего p^n. А значит, столько же элементов в поле $\mathbb{F}_p[x]/(g)$.

Конечные поля из p^n элементов

Поле $\mathbb{F}_p[x]/(g)$ состоит из p^n элементов вида

$$[r] = [r]_{(g)} = \{r(x) + g(x) \cdot h(x) \mid h(x) \in \mathbb{F}_p[x]\},$$

где $r(x)$ — многочлен степени, не превосходящей $(n-1)$, из кольца $\mathbb{F}_p[x]$.
Операции сложения и умножения в поле $\mathbb{F}_p[x]/(g)$:

$$[r_1] + [r_2] = [r_1 + r_2],$$

$$[r_1] \cdot [r_2] = [r_1 \cdot r_2],$$

с возможным **приведением по модулю** многочлена $g(x)$.
Для каждого простого числа p существует конечное поле из p элементов. Поэтому если найдется неприводимый над этим полем многочлен степени n, можно построить конечное поле из p^n элементов.

Поле из 4-х элементов

Пример. Построим поле из $4 = 2^2$ элементов.
В кольце $\mathbb{F}_2[x]$ многочлен $g(x) = x^2 + x + 1$ — неприводим.
Элементами поля $\mathbb{F}_2[x]/(g)$ будут классы вычетов:

$$[0] = 0, [1] = 1, [x] = a, [x + 1] = b,$$

где $[0] = 0$ — нулевой и $[1] = 1$ — единичный элементы.
Таблицы сложения и умножения элементов в поле $\mathbb{F}_2[x]/(g)$:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Например:

$$a + b = [x] + [x + 1] = [x + x + 1] = [1] = 1,$$
$$a \cdot b = [x] \cdot [x + 1] = [x(x + 1)] = [x^2 + x] = [g(x) + 1] = [1] = 1.$$

Задачи для самостоятельного решения

1. Доказать, что множество $Z_{a,b} = \{a \cdot x + b \cdot y \mid x, y \in \mathbb{Z}\}$, где $a, b \in \mathbb{Z}$, является идеалом кольца $(\mathbb{Z}; +, \cdot)$ сложения и умножения целых чисел. Является ли этот идеал главным?

2. Пусть F — поле, и $g(x), h(x) \in F[x]$. Показать, что главный идеал (f) содержится в главном идеале (g) тогда и только тогда, когда многочлен $f(x)$ делится на многочлен $g(x)$.

3. Построить таблицы сложения и умножения элементов в фактор-кольце $\mathbb{F}_2[x]/(f)$, где $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Является ли это фактор-кольцо полем?

4. Построить таблицы сложения и умножения элементов в фактор-кольце $\mathbb{F}_3[x]/(f)$, где $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$. Является ли это фактор-кольцо полем?

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Гл. 1, с. 26–27, 31, 36, 38, 40–41.

Конец лекции