Лекция 10. Кольца, поля. Теорема о конечном целостном кольце. Характеристика кольца. Кольцо многочленов. Деление с остатком многочленов над полем. Неприводимые многочлены над полем. Критерий неприводимости многочленов степени 2 и 3.

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

Факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Кольцо

Пусть на множестве S заданы две алгебраические операции: сложение $+$ и умножение $\cdot$.
Структура $K = (S; +, \cdot)$ 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 $K = (S; +, \cdot)$ — кольцо. Кольцо K называется

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

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

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

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

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

Примеры колец

1. Кольцо $K_1 = (\mathbb{Z}; +, \cdot)$ 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 $K_2 = (\mathbb{Z}_4; + \pmod 4, \cdot \pmod 4)$ 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 $K_3 = (\mathbb{Z}_2; + \pmod 2, \cdot \pmod 2)$ 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 $K = (S; +, \cdot)$ 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 $S \setminus \{0\} = \{b_1, b_2, \ldots, b_m\}$. Рассмотрим элементы

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

В этой последовательности все элементы ненулевые, т.к. в кольце K 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 K нет делителей нуля, верно $b_i = b_j$ — противоречие.
Значит, среди элементов последовательности встречаются все элементы множества $S \setminus \{0\}$, поэтому $a \cdot b_k = 1$ для некоторого элемента $b_k \in S \setminus \{0\}$. Т.е. $b_k = a^{-1}$. $\square$

Простые поля

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

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

Характеристика кольца

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

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

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

Характеристика кольца

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

Доказательство. Рассмотрим единицу e конечного целостного кольца K. Т.к. кольцо K — конечно, в последовательности

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

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

$$ie = je.$$

Поэтому $(j - i)e = 0$. Для каждого элемента $a \in K$ верно

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

Значит, кольцо K — с положительной характеристикой.

Характеристика кольца

Доказательство.
Пусть n — положительная характеристика конечного целостного кольца K. 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 K 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 $K = (S; +, \cdot)$ — кольцо.
Многочленом $f(x)$ над кольцом K называется 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 K называются **равными**, если $a_i = b_i$ для каждого индекса $i = 0, 1, \ldots, n$.

Многочлены над кольцом

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

Для многочлена $f \in K[x]$ 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.
По определению полагают, что степень многочлена $0 \in K[x]$, 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:

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

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 K их **суммой** назовем многочлен

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

где $c_k = a_k + b_k \in K$;

а их **произведением** назовем многочлен

$$(f \cdot g)(x) = \sum_{k=0}^{n+m} d_k x^k \in K[x],$$

где $d_k = \sum_{i+j=k} a_i b_j \in K$.

Утверждение 1. *Если* $f, g \in K[x]$, *то*

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

Кольцо многочленов

Утверждение 2. *Множество $K[x]$ многочленов над кольцом K с операциями сложения и умножения многочленов является кольцом.*

Доказательство. Свойства кольца.

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

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

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

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

2) Дистрибутивность: по свойствам дистрибутивности в кольце K.

Кольцо многочленов

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

Предложение 3. *Пусть K — кольцо, а $K[x]$ — кольцо многочленов над кольцом K. Тогда*

1) если кольцо K — коммутативно (ассоциативно), то кольцо $K[x]$ — коммутативно (ассоциативно);

2) если кольцо K — с единицей, то кольцо $K[x]$ — с единицей;

3) если кольцо K — целостное, то кольцо $K[x]$ — 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 $k = 0, 1, \ldots, n + m$ верно

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

Рассмотрим $k = n + m$. Тогда

$$a_n \cdot b_m = 0,$$

противоречие, т.к. $a_n \neq 0$, $b_m \neq 0$, и в кольце K нет делителей нуля.

Кольцо многочленов

Утверждение 4. *Если K — целостное кольцо, и $f, g \in K[x]$, $f \neq 0$, $g \neq 0$, то*

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

Деление с остатком многочленов над полем

Теорема 3 (о делении с остатком многочленов над полем).
Пусть F — поле и $F[x]$ — кольцо многочленов над полем F. Тогда для любых многочленов $f, g \in F[x]$, $f \neq 0$, $g \neq 0$, найдутся такие однозначные многочлены $q, r \in F[x]$, что

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

Деление с остатком многочленов над полем

Доказательство существования таких многочленов $q, r \in F[x]$ 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

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

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

$$f(x) = g(x) \cdot \left(a_n b_m^{-1} x^{n-m} + q_1(x)\right) + r(x),\ \deg(r) < \deg(g),$$

т.е. $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$.

Деление с остатком многочленов над полем

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

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

Наибольший общий делитель многочленов

Пусть F — поле.

Многочлен над полем называется **нормированным**, если его старший коэффициент равен единице.

Нормированный многочлен $g \in F[x]$ называется **наибольшим общим делителем** многочленов $f_1, f_2 \in F[x]$, если
1) многочлены $f_1(x)$ и $f_2(x)$ делятся на многочлен $g(x)$;
2) многочлен $g(x)$ делится на каждый многочлен, на который делятся одновременно многочлены $f_1(x)$ и $f_2(x)$.

Наибольший общий делитель многочленов $f_1(x)$ и $f_2(x)$ будем обозначать как НОД(f_1, f_2).

Алгоритм Евклида

Теорема 4 (алгоритм Евклида). *Пусть F — поле, $f_1, f_2 \in F[x]$ — ненулевые многочлены, и*

$$
\begin{aligned}
&f_1(x) = f_2(x)q_1(x) + r_1(x),\ \deg(r_1) < \deg(f_2),\\
&f_2(x) = r_1(x)q_2(x) + r_2(x),\ \deg(r_2) < \deg(r_1),\\
&r_1(x) = r_2(x)q_3(x) + r_3(x),\ \deg(r_3) < \deg(r_2),\\
&\ldots;\\
&r_{s-2}(x) = r_{s-1}(x)q_s(x) + r_s(x),\ \deg(r_s) < \deg(r_{s-1}),\\
&r_{s-1}(x) = r_s(x)q_{s+1}(x).
\end{aligned}
$$

Тогда если $a \in F$ — старший коэффициент многочлена $r_s(x)$, то НОД$(f_1, f_2) = a^{-1}r_s(x)$.

Алгоритм Евклида

Доказательство. Пусть

$$
\begin{aligned}
&f_1(x) = f_2(x)q_1(x) + r_1(x),\ \deg(r_1) < \deg(f_2),\\
&f_2(x) = r_1(x)q_2(x) + r_2(x),\ \deg(r_2) < \deg(r_1),\\
&r_1(x) = r_2(x)q_3(x) + r_3(x),\ \deg(r_3) < \deg(r_2),\\
&\ldots;\\
&r_{s-2}(x) = r_{s-1}(x)q_s(x) + r_s(x),\ \deg(r_s) < \deg(r_{s-1});\\
&r_{s-1}(x) = r_s(x)q_{s+1}(x).
\end{aligned}
$$

1) Просматривая равенства «снизу вверх» получаем, что на многочлен $r_s(x)$ делятся многочлены $f_1(x)$ и $f_2(x)$.
2) Если на многочлен $h(x)$ одновременно делятся многочлены $f_1(x)$ и $f_2(x)$, то, просматривая равенства «сверху вниз», получаем, что на многочлен $h(x)$ делится и многочлен $r_s(x)$.
Значит, НОД$(f_1, f_2) = a^{-1}r_s(x)$. □

Алгоритм Евклида

Пример. По алгоритму Евклида найдем наибольший общий делитель многочленов $f_1(x) = x^4 + x$ и $f_2(x) = x^2 + 1$ из кольца $\mathbb{F}_2[x]$.
Тогда

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

Значит, НОД$(x^4 + x, x^2 + 1) = x + 1$.

Наибольший общий делитель многочленов

Теорема 5. *Если F — поле и $f_1, f_2 \in F[x]$ — ненулевые многочлены, то существует единственный многочлен $g \in F[x]$, являющийся наибольшим общим делителем многочленов f_1 и f_2.*

Доказательство.

1. Существование показано в алгоритме Евклида.

Наибольший общий делитель многочленов

Доказательство.
2. Докажем единственность. Пусть $g_1, g_2 \in F[x]$ — наибольшие общие делители многочленов f_1 и f_2.
Т.к. g_1 — наибольший общий делитель f_1 и f_2, а g_2 — их делитель, найдется такой многочлен $q_1 \in F[x]$, что

$$g_1(x) = g_2(x)q_1(x).$$

Аналогично, найдется такой многочлен $q_2 \in F[x]$, что

$$g_2(x) = g_1(x)q_2(x).$$

Тогда

$$g_1(x) = g_2(x)q_1(x) = (g_1(x)q_2(x))q_1(x),$$

откуда

$$g_1(x)(1 - q_1(x)q_2(x)) = 0.$$

Наибольший общий делитель многочленов

Доказательство.
Но F — поле, значит, целостное кольцо, и $g_1 \neq 0$, поэтому

$$q_1(x)q_2(x) = 1.$$

Следовательно, $q(x)$ и $q_1(x)$ — постоянные ненулевые многочлены.
Многочлены $g_1(x)$ и $g_2(x)$ нормированы, поэтому $q(x) = q_1(x) = 1$. Т.е. $g_1(x) = g_2(x)$ — однозначность доказана.

□

Обратимые многочлены над полем

Обратимыми многочленами над полем F называются ненулевые постоянные многочлены (многочлены степени 0).

Например, обратимыми многочленами над полем $\mathbb{Z}_p$, где p — простое число, являются постоянные многочлены

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

Неприводимые многочлены над полем

Многочлен $f \in F[x]$ называется **неприводимым** над полем F (или в кольце $F[x]$), если в любом представлении

$$f(x) = g(x) \cdot h(x)$$

либо g — постоянный многочлен, либо h — постоянный многочлен.

Приводимые многочлены над полем

Многочлен $f \in F[x]$ называется **приводимым** над полем F (или в кольце $F[x]$), если найдутся такие непостоянные многочлены $g, h \in F[x]$, что

$$f(x) = g(x) \cdot h(x)$$

Неприводимые и приводимые многочлены над полем

Пример. Над полем $\mathbb{Z}_2$ 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 $a, b \in \mathbb{Z}_2$

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

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

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

Корень многочлена

Пусть K — кольцо, $f \in K[x]$,

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

и $c \in K$.
Значением многочлена $f(x)$ **в точке** c называется элемент

$$f(c) = \sum_{i=0}^{n} a_i c^i \in K.$$

Если $f(c) = 0$, то c называется **корнем** многочлена $f(x)$.

Корень многочлена

Теорема 6. *Пусть F — поле. Элемент $c \in F$ является корнем многочлена $f \in F[x]$ тогда и только тогда, когда многочлен $f(x)$ делится на многочлен $(x - c)$.*

Доказательство. Поделим с остатком многочлен $f(x)$ на многочлен $(x - c)$:

$$f(x) = (x - c)q(x) + r(x),\ \deg(r) < 1.$$

Т.к. степень многочлена $r(x) \in F[x]$ меньше 1, он является постоянным многочленом: $r(x) = b \in F$.

$\Rightarrow$. Если c — корень многочлена $f(x)$, то

$$0 = f(c) = b.$$

$\Leftarrow$. Если многочлен $f(x)$ делится на многочлен $(x - c)$, то $b = 0$. Поэтому $f(c) = 0$.

Кратные корни многочлена

Пусть F — поле. Элемент $c \in F$ называется **корнем кратности** k $(k \geq 1)$ многочлена $f \in F[x]$, если многочлен $f(x)$ делится на многочлен $(x-c)^k$ и не делится на многочлен $(x-c)^{k+1}$.

Следствие 6.1. *Если F — поле и многочлен $f \in F[x]$ имеет степень n, $n \geq 1$, то в поле F у него найдется не более n корней с учетом их кратностей*.

Неприводимые многочлены степени 2 или 3

Теорема 7 (критерий неприводимости многочленов степени 2 и 3). *Пусть F — поле. Многочлен $f \in F[x]$ степени 2 или 3 неприводим над полем F тогда и только тогда, когда у него нет корней в этом поле.*

Доказательство. Рассмотрим представление

$$f(x) = g(x) \cdot h(x),$$

где $g(x), h(x) \in F[x]$, $\deg(g) \geq 1$, $\deg(h) \geq 1$.
Т.к. степень многочлена $f(x)$ равна 2 или 3, или $\deg(g) = 1$, или $\deg(h) = 1$.
Значит, многочлен $f(x)$ неприводим над полем F тогда и только тогда когда у него нет корней в этом поле.

□

Неприводимые многочлены степени 2 или 3

Пример. Рассмотрим многочлен $f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$:

c	$f(c)$
0	2
1	2
2	1

Многочлен $f(x)$ не имеет корней в поле $\mathbb{Z}_3$, значит, он неприводим над полем $\mathbb{Z}_3$.

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Гл. 1, с. 24–27, 29–31, 33–36, 38, 40–41.

Конец лекции