
Лекция №16

---

2 Теория колец

2.7 Делимость в кольцах целостности

Неприводимость и простота

Определение 1. *Пусть D – кольцо целостности. Элементы $a, b \in D$ называются ассоциированными, если $a = u \cdot b$, где $u \in D^*$ – обратимы. Элемент $a \in D$ называется неприводимым, если $a \notin D^*$ и если $a = b \cdot c$, где $b, c \in D \Rightarrow \left[\begin{array}{l} b \in D^* \\ c \in D^* \end{array} \right.$ Элемент $a \in D$ назыется простым, если $a|b \cdot c \Rightarrow \left[\begin{array}{l} a|b \\ a|c \end{array} \right.$*

Теорема 1. *В кольце целостности всякий простой элемент является неприводимым.*

Доказательство. Рассмотрим $a \in D$ – простой. Пусть, например, $a = b \cdot c$.

Покажем, что $\left[\begin{array}{l} b \in D^* \\ c \in D^* \end{array} \right.$. Из определения следует, что $\left[\begin{array}{l} a|b \\ a|c \end{array} \right.$
Пусть $a|b$, тогда $b = a \cdot t = b \cdot (c \cdot t)$, следовательно, $c \cdot t = e \Rightarrow c \in D^*$. □

Кольцо главных идеалов есть кольцо целостности, в котором каждый идеал имеет вид (a).

Теорема 2. *В кольце главных идеалов элемент тогда и только тогда неприводим, когда прост.*

Доказательство. Достаточность доказана в предыдущей теореме. Докажем необходимость.

Пусть D – кольцо главных идеалов, $a \in D$ – неприводим и $a|b \cdot c$. Рассмотрим $I = \{ax + by | x, y \in D\}$ – идеал. Пусть $I = (d)$.

$$a \in I \Rightarrow a = d \cdot r, r \in D \Rightarrow \left[\begin{array}{l} d \in D^* \Rightarrow 1 = ax + by \Rightarrow c = cax + cby \Rightarrow a|c. \\ r \in D^* \Rightarrow b \in I \Rightarrow \exists t \in D \big| b = at \Rightarrow a|b. \end{array} \right.$$

□

Кольцо с единственным разложением на множители

Определение 2. *Кольцо целостности D называется кольцом с единственным разложением на множители, если:*

1. *Каждый ненулевой элемент из D, который не является обратимым, может быть записан в виде произведения неприводимых элементов из D.*
2. *Разложение на неприводимые элементы единственно с точностью до ассоциирования и порядка их следования.*

Лемма 1. *В кольце главных идеалов строго возрастающая цепочка идеалов $I_1 \subset I_2 \subset ...$ должна стабилизироваться, то есть иметь конечную длину.*

Теорема 3. *Всякое кольцо главных идеалов является кольцом с единственным разложением на множители.*

Следствие 1. *Пусть F – поле, тогда $F[X]$ – кольцо с единственным разложением на множители.*

Евклидовы кольца

Определение 3. *Кольцо целостности D называется евклидовым кольцом, если существует функция d, называемая мерой, действующая $\left|d : D \setminus \{0\} \to \mathbb{Z}^{\geq 0}\right.$ и обладающая следующими свойствами:*

1. $d(a) \leq d(ab)$ *для* $\forall a, b \in D \setminus \{0\}$
2. *Если* $a, b(\neq 0) \in D$, *то существуют* $q, r \in D$, *такие, что* $a = bq + r$, *где* $r = 0$ *или* $d(r) < d(b)$.

Сравнение колец $\mathbb{Z}$ и $F[X]$.

Характеристика	$\mathbb{Z}$	$F[X]$
Вид элементов	$a_n 10^n + ... + a_1 10 + a_0$	$a_n X^n + ... + a_1 X + a_0$
Мера d	$d(a) = \lvert a \rvert$	$d(f(X)) = \deg f$
$\mathbb{Z}^*$	a 0 обратим $\Leftrightarrow \lvert a \rvert = 1$	f 0 обратим $\Leftrightarrow \deg f = 0$
Алгоритм деления	$a = bq + r, o \leq r < \lvert b \rvert$	$f(X) = q(X)g(X) + r(X), \left[\begin{array}{l} 0 \leq \deg r < \deg g \\ r(X) = 0 \end{array}\right.$
Кольцо главных идеалов	$\forall \neq 0\ I = (a), \lvert a \rvert \neq 0 - min$	$\forall \neq 0\ I = (f(X)), \deg f - min$

Теорема 4. *Любое евклидово кольцо является кольцом главных идеалов.*

Доказательство. Пусть D – евклидово кольцо, $I(\neq 0) \subset D$ – идеал. Среди всех ненулевых элементов из I рассмотрим такой a, чтобы $d(a)$ было минимальным.

Если $b \in I$, то существуют $q, r \in D$, такие, что $b = aq + r$, где либо $r = 0$, либо $d(r) < d(a)$. Следовательно, $r = b - aq$, откуда $r \in I$.

Так как $d(r) \geq d(a)$, то $r = 0 \Rightarrow b = aq \Rightarrow b \in (a) \Rightarrow I \subset (a) \Rightarrow I = (a)$. □

В общем случае сущетвуют кольца главных идеалов, которые не являются евклидовыми.

Следствие 2. *Любое евклидово кольцо является кольцом с единственным разложением на множители.*

Теорема 5. *Если D – кольцо с единственным разложением на множители, то $D[X]$ также является кольцом с единственным разложением на множители.*