Лекция 12

Далее переходим к изучению коммутативных ассоциативных колец с единицей. Все кольца далее являются коммутативными ассоциативными и с единицей, не будем писать это для краткости, но будем это предполагать. Так как кольцо коммутативно, понятия левого, правого и двустороннего идеалов совпадают. Будем использовать обозначение $I \triangleleft R$ для идеала I в кольце R. Напомним, что минимальны идеал, содержащи некоторое подмножество S в кольце R имеет вид

$$(S) = \left\{ \sum_{i=1}^{k} r_i s_i \mid r_i \in R, s_i \in S, k \in \mathbb{N} \right\}.$$

Будем называть данный идеал *идеалом, порожденным* S.

Определение 1. Идеал, порожденный одним элементом, называется *главным*.

Пример 1. *Идеал* (n) *в кольце* $\mathbb{Z}$ *состоит из чисел, делящихся на* n.

Лемма 1. *Идеал в кольце содержащий обратимый элемент совпадает со всем кольцом.*

Доказательство. Пусть $I \triangleleft R$ – левый идеал некоторого кольца и пусть $a \in I$ – обратимый элемент. Тогда $a^{-1}a = 1 \in I$. Но тогда для любого $r \in R$ имеем $r = r1 \in I$. □

Предложение 1. *Кольцо* R *не имеет нетривиальных (то есть отличных от* $\{0\}$ *и* R*) идеалов тогда и только тогда, когда это поле.*

Доказательство. Пусть R – поле. Тогда любой ненулевой идеал содержит обратимый элемент, и следовательно, совпадает с R.

Пусть теперь R кольцо без нетривиальных идеалов. Рассмотрим $r \neq 0 \in R$. Тогда можно рассмотреть идеал (r). Так как в этом идеале содержится $r \neq 0$, это ненулевой идеал. Значит, $(r) = R$. Тогда $1 \in (r)$, что означает $1 = xr$. □

Определение 2. Кольцо (коммутативное ассоциативное с единицей) называется *областью целостности* или, что то же самое *целостным кольцом*, если в нем нет делителей нуля.

Определение 3. Идеал I в кольце R называется *простым*, если из того, что $ab \in I$ следует, что $a \in I$ или $b \in I$.

Пример 2. *Идеал* (n) *в кольце* $\mathbb{Z}$ *является простым тогда и только тогда, когда число* n *простое.*

Предложение 2. *Факторкольцо* R/I *не имеет делителей нуля тогда и только тогда, когда* I *– простой идеал.*

Доказательство. Пусть $a + I$ и $b + I$ – ненулевые смежные классы. Это значит, что $a, b \notin I$. Тогда $(a + I)(b + I) = 0$ равносильно $ab \in I$. Но существование таких a и b, что $a, b \notin I$, а $ab \in I$ равносильно тому, что идеал I не простой. □

Определение 4. Идеал I в кольце R называется *максимальным*, если не существует идеала $J \triangleleft R$ такого, что $I \subsetneq J \subsetneq R$.

Лемма 2. *Пусть* $\psi\colon R \to S$ *– гомоморфизм колец. Пусть* J *– идеал в* S*. Тогда полный прообраз* $\psi^{-1}(J)$ *– это идеал в* R*.*

Доказательство. Пусть $a, b \in \psi^{-1}(J)$. Тогда $\psi(a+b) = \psi(a) + \psi(b) \in J$ и $\psi(-a) = -\psi(a) \in J$, то есть $a+b \in \psi^{-1}(J)$ и $-a \in \psi^{-1}(J)$. Кроме того $\psi(ra) = \psi(r)\psi(a) \in J$, $\psi(ar) = \psi(a)\psi(r) \in J$, то есть $ra, ar \in \psi^{-1}(J)$. □

Лемма 3. *Пусть $\psi\colon R \to S$ – сюръективный гомоморфизм колец. И пусть I – идеал в R. Тогда $\psi(I)$ – идеал в S.*

Доказательство. Пусть $a = \psi(x)$, $b = \psi(y)$, где $x, y \in I$. Тогда $x + y \in I$ и $\psi(x+y) = a + b \in \psi(I)$. И $-a = \psi(-x) \in \psi(I)$. Для любого $s \in S$ имеем $s = \psi(r)$ для некоторого $r \in R$. Тогда $sa = \psi(rx) \in \psi(I)$. □

Теорема 1. *Пусть R – коммутативное кольцо с единицей. Факторкольцо R/I – поле тогда и только тогда, когда I – максимальный идеал.*

Доказательство. Рассмотрим канонический гомоморфизм (колец) $\pi_I\colon R \to R/I$, $\operatorname{Ker}\pi_I = I$. Существование собственного идеала J такого, что $I \subsetneq J \subsetneq R$ равносильно существованию промежуточного идеала $\{0\} \subsetneq L \subsetneq R/I$ такого, что $\pi_I^{-1}(L) = J$. Но существование такого L равносильно тому, что R/I – не поле. □

Определение 5. Пусть R – область целостности, не являющаяся полем. Тогда R называется *евклидовым кольцом*, если задана функция (*евклидова норма*)

$$N\colon R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

такая, что

1) $N(ab) \geq N(a)$ для любых $a, b \in R \setminus \{0\}$;

2) для любых $a, b \in R$, $b \neq 0$ возможно "деление с остатком", то есть существуют такие $q, r \in R$, что $a = bq + r$, причем либо $N(r) < N(b)$, либо $r = 0$.

Пример 3. *1)* $R = \mathbb{Z}$, $N(a) = |a|$.

2) $R = F[x]$, $N(f) = \deg f$.

3) **Задача.** *Докажите, что $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ – евклидово кольцо с нормой $N(z) = |z|$.*

4) **Задача.** *Для каких $c \in \mathbb{R}$ кольцо $\mathbb{Z}[ci] = \{a + bci \mid a, b \in \mathbb{Z}\}$ является евклидовым кольцом с нормой $N(z) = |z|$?*

Определение 6. Область целостности R назовем *кольцом главных идеалов*, если любой идеал в нем главный, то есть равен (r) для некоторого $r \in R$.

Пример 4. *Идеал (x, y) в $F[x, y]$ не является главным. Действительно, если $(x, y) = (f)$, то f делит и x и y. Тогда f – константа и $(f) = F[x, y]$.*

Теорема 2. *Евсклидово кольцо является кольцом главных идеалов.*

Доказательство. Пусть R – евклидово кольцо с нормой N. И пусть $I \triangleleft R$. Если $I \neq \{0\}$, рассмотрим ненулевой элемент $a \in I$ с минимальной нормой. Пусть $b \in I$. Тогда $b = aq + r$. Предположим, что $r \neq 0$. Получаем $r \in I$, $N(r) < N(a)$. Противоречие с выбором a. Значит, $r = 0$, то есть $b \in (a)$. Следовательно, $I = (a)$. □

Определение 7. Пусть a и b – два элемента кольца главных идеалов. Рассмотрим $(a, b) = (d)$. Назовем d *наибольшим общим делителем* a и b. (НОД определен с точностью до обратимого множителя.)

Имеем $d \mid a$, $d \mid b$, $d = ua + vb$.

Определение 8. 1) Пусть R – область целостности. Необратимый элемент $r \in R$ называется *неприводимым*, если из $ab = r$ следует, что либо a, либо b обратим.

2) Два элемента $u, v \in R$ называются *ассоциированными*, если $u = cv$, где c – обратимый элемент.

3) Кольцо R называется *факториальным*, если любой элемент раскладывается в произведение неприводимых единственным способом с точностью до порядка и ассоциированности сомножителей.

Лемма 4. *Пусть R – кольцо главных идеалов, p – неприводимый элемент. Допустим, что $p \mid ab$. Тогда либо $p \mid a$, либо $p \mid b$.*

Доказательство. Пусть $s = \text{НОД}(a, p)$. Тогда $s \mid p$. Значит, либо s ассоциирован с p, либо с 1. Если $s = p$, то $p \mid a$. Если же $s = 1$, то существуют $u, v \in R$ такие, что $ua + vp = 1$. Домножим это равенство на b. Получим $uab + vpb = b$. Левая часть делится на p. Значит, и правая часть делится на p. □

Следствие 1. *Пусть R – кольцо главных идеалов, p – неприводимый элемент. Допустим, что $p \mid a_1 a_2 \dots a_k$. Тогда найдется j такой, что $p \mid a_j$.*

Теорема 3. *Кольцо главных идеалов факториально.*

Доказательство. **Существование.** Пусть R – кольцо главных идеалов и $a \in R$. Если a не является неприводимым, то $a = bc$ для некоторых необратимых b и c. Тогда имеем $(a) \subsetneq (b)$ и $(a) \subsetneq (c)$. Если оба множителя неприводимы, то получено разложение. Иначе какой-то из них снова можно разложить, что даст увеличение идеала и т.д. Если разложения так и не будет, получим бесконечно возрастающую цепочку $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \dots$

Рассмотрим $I = \cup(a_i)$. Легко видеть, что I – идеал. Значит, $I = (b)$. Но $b \in \cup(a_i)$, значит, найдется j такой, что $b \in (a_j)$. Тогда $I = (a_j)$. То есть бесконечно возрастающих цепочек не может быть.

Единственность. Пусть $a = p_1 \dots p_k = q_1 \dots q_m$ – два разложения на неприводимые. Тогда $p_1 \mid q_1 \dots q_m$. Значит, существует j такое, что $p_1 \mid q_j$. Так как p_1 и q_j неприводимы, они ассоциированы. Значит, перебрасывая обратимый элемент в другой множитель и меняя нумерацию, можно считать $p_1 = q_1$.

$$p_1 p_2 \dots p_k = p_1 q_2 \dots q_m.$$

Перенесем все в одну часть.

$$p_1(p_2 \dots p_k - q_2 \dots q_m) = 0.$$

Так как $p_1 \neq 0$ и в R нет делителей нуля, получаем $p_2 \dots p_k = q_2 \dots q_m$ и т.д. □