

ЛЕКЦИЯ 1

Все кольца (если явно не сказано другого) предполагаются коммутативными, ассоциативными и с единицей, то есть верно следующее определение.

Определение 1. Множество R называется *кольцом*, если на нём введены две бинарные операции $+: R \times R \rightarrow R$ и $\cdot: R \times R \rightarrow R$ такие, что:

- 1) для любых $a, b, c \in R$ выполнено $a + (b + c) = (a + b) + c$;
- 2) существует элемент $0 \in R$ такой, что для любого $a \in R$ выполняется $0 + a = a$;
- 3) для каждого $a \in R$ найдётся элемент $-a \in R$ такой, что $a + (-a) = 0$;
- 4) для любых $a, b \in R$ выполнено $a + b = b + a$;
- 5) для любых $a, b, c \in R$ выполнено $a(b + c) = ab + ac$;
- 6) для любых $a, b, c \in R$ выполнено $a(bc) = (ab)c$;
- 7) для любых $a, b \in R$ выполнено $ab = ba$;
- 8) существует элемент $1 \in R$ такой, что для любого $a \in R$ выполнено $1a = a$.

Определение 2. Идеал I кольца R называется *простым*, если $I \neq R$ и из $ab \in I$ следует, что хотя бы один из элементов a и b лежит в I .

Упражнение 1. Докажите, что идеал I простой тогда и только тогда, когда факторкольцо R/I – область целостности (т.е. не имеет делителей нуля).

Определение 3. Идеал I кольца R называется *максимальным*, если $I \neq R$ и не существует такого идеала J в R , что $I \subsetneq J \subsetneq R$.

Упражнение 2. Докажите, что идеал I максимальный тогда и только тогда, когда факторкольцо R/I – поле.

Определение 4. Пусть R – область целостности, не являющаяся полем. Тогда R называется *евклидовым кольцом*, если задана функция (евклидова норма) $N: R \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ 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 1. 1) $R = \mathbb{Z}$, $N(a) = |a|$.

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

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

Задача 1. 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 5. Область целостности R назовем *кольцом главных идеалов* (КГИ), если любой идеал в нем главный, то есть равен (r) для некоторого $r \in R$.

Определение 6. Кольцо называется *нётеровым*, если в нём любая нестрогая возрастающая цепочка вложенных друг в друга идеалов стабилизируется. (Или, что то же самое, не существует бесконечных строго возрастающих цепочек идеалов.)

Лемма 1. Следующие условия равносильны:

- 1) Кольцо R нётерово;
- 2) Любой идеал в R конечно порождён.

Доказательство. $1 \Rightarrow 2$. Допустим, что в нётеровом кольце есть не конечно порождённый идеал I . Возьмём любой элемент $a_1 \in I$. Идеал (a_1) не совпадает с I , иначе I порождён одним элементом. Значит, найдётся $a_2 \in I \setminus (a_1)$. Тогда $(a_1) \subsetneq (a_1, a_2)$. Опять I не совпадает с (a_1, a_2) , значит, найдётся элемент $a_3 \in I \setminus (a_1, a_2)$. Получаем $(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3)$. Продолжая выбирать элементы a_i аналогичным образом, получаем бесконечную цепочку строго возрастающих идеалов, что противоречит нётеровости.

$2 \Rightarrow 1$. Пусть R – кольцо, в котором все идеалы конечно порождены. Допустим, что оно не нётерово. Тогда существует бесконечная строго возрастающая цепочка идеалов $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$. Рассмотрим $I = \bigcup_{j=1}^{\infty} I_j$.

Упражнение 4. Подмножество $I \subseteq R$ является идеалом.

Пусть $I = (a_1, \dots, a_k)$. Для каждого j существует число n_j такое, что $a_j \in I_{n_j}$. Пусть $n = \max\{n_j\}$. Тогда $a_1, \dots, a_k \in I_n$. Значит, $I_n = I$. Это противоречит тому, что $I_n \subsetneq I_{n+1}$. $\square$

Определение 7. Пусть R – область целостности. Необратимый ненулевой элемент $r \in R$ называется *неприводимым*, если из $ab = r$ следует, что либо a , либо b обратим.

Определение 8. Два элемента $u, v \in R$ называются *ассоциированными*, если $u = cv$, где c – обратимый элемент.

Определение 9. Кольцо (область целостности) R называется *факториальным*, если любой элемент раскладывается в произведение неприводимых единственным способом с точностью до порядка и ассоциированности сомножителей.

Лемма 2. В любом нётеровом кольце любой ненулевой необратимый элемент раскладывается (хотя бы одним способом) в произведение неприводимых.

Доказательство. Рассмотрим некоторый ненулевой необратимый элемент $r \in R$. Если его нельзя разложить в произведение двух необратимых, то он неприводим и, следовательно, может быть разложен на неприводимые. Пусть его можно разложить в произведение двух необратимых (и, конечно, ненулевых) элементов $r = r_1 r_2$. Если оба элемента r_1 и r_2 неприводимы, то r раскладывается в произведение неприводимых. Если же без ограничения общности $r_1 = r_{11} r_{12}$, то проводим те же рассуждения для новых множителей и т.д. Если этот процесс никогда не закончится, то мы получаем цепочку делящих друг друга элементов $\dots r_{111} \mid r_{11} \mid r_1$. Так как вторые сомножители необратимы, получаем строго возрастающую цепочку идеалов: $(r_1) \subsetneq (r_{11}) \subsetneq (r_{111}) \subsetneq \dots$, что противоречит нётеровости. $\square$

Определение 10. Пусть R КГИ и $a, b \in R$. Найдётся элемент $d \in R$ такой, что $(a, b) = (d)$. Назовём такой элемент D наибольшим общим делителем a и b . НОД определён с точностью до умножения на обратимый элемент.

Легко видеть, что найдутся такие $u, v \in R$, что $\text{НОД}(a, b) = ua + vb$.

Определение 11. Пусть R – область целостности. Элемент $p \in R$ называется *простым*, если из $p \mid ab$ следует, что либо $p \mid a$, либо $p \mid b$.

Лемма 3. В кольце главных идеалов неприводимый элемент является простым.

Доказательство. Пусть $p \in R$ – неприводимый элемент. Допустим, что $p \mid ab$. Надо доказать, что тогда либо $p \mid a$, либо $p \mid b$. Пусть $s = \text{НОД}(a, p)$, то есть $(a, b) = (s)$. 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 . $\square$

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 1. Кольцо главных идеалов факториально.

Доказательство. Существование разложения необратимого ненулевого элемента на неприводимые следует из того, что КГИ является нётеровым и ktvvs 2. Докажем 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. $\square$

1. Модули

Определение 12. R -модуль – это абелева группа (по сложению) M с отображением $R \times M \rightarrow M$, $(r, m) \mapsto rm$, удовлетворяющем для всех $r, s \in R$, $m, n \in M$ аксиомам:

- $r(sm) = (rs)m$;
- $r(m+n) = rm + rn$;
- $(r+s)m = rm + sm$;
- $1m = m$.

Пример 2. Любой идеал $I \triangleleft R$ является модулем над R . В частности, само R является R -модулем. Также факторкольцо R/I является модулем над R .

Пример 3. Векторное пространство – модуль над полем.

Определение 13. Подмодуль N в модуле M – это подгруппа по сложению, замкнутая относительно операции умножения на R . Легко видеть, что подмодуль сам по себе является модулем над R .

Пример 4. Подмодуль в R -модуле R – это идеал в R .

Определение 14. Аннулятором R -модуля M называется следующее подмножество в R :

$$\text{ann } M = \{r \in R \mid rm = 0 \text{ для всех } m \in M\}.$$

Легко видеть, что аннулятор – идеал в R .

Пример 5. $\text{ann } R/I = I$.

Определение 15. Пусть M и N – подмодули в R -модуле P . Обозначим

$$(M : N) = \{f \in R \mid fN \subseteq M\}.$$

Будем говорить, что $(M : N)$ – *частное* двух подмодулей.

Упражнение 5. Докажите, что $(M : N)$ – идеал в R .

Введём аналогичное определение.

Определение 16. Пусть M – подмодуль в R -модуле P и I – идеал в R . Обозначим

$$(M :_P I) = \{p \in P \mid Ip \subseteq M\}.$$

Назовём $(M : N)$ – *частное* подмодуля и идеала. Если модуль P восстанавливается из контекста, будем писать $(M : I)$.

Упражнение 6. Докажите, что $(M :_P I)$ – подмодуль в P .

Задача 2. Приведите пример, когда $(M :_P I)$ зависит не только от M и I , но и от P .

Определение 17. Скажем, что $r \in R$ – *делитель нуля* на M , если

$$(\{0\} :_M (r)) \neq \{0\}.$$