

ЛЕКЦИЯ 8

Лемма 1 (Цорна (эквивалентна аксиоме выбора)). *Если в частично упорядоченном множестве $\mathcal{M}$ каждая цепь (линейно упорядоченное подмножество) имеет верхнюю грань, то существует максимальный элемент в $\mathcal{M}$.*

Ясно, что эта лемма имеет эквивалентную формулировку.

Лемма 2. *Если в частично упорядоченном множестве $\mathcal{M}$ каждая цепь имеет нижнюю грань, то существует минимальный элемент в $\mathcal{M}$.*

Выведем из леммы Цорна то, что существует минимальный из простых идеалов, содержащих данный идеал.

Лемма 3. *Пусть $I \triangleleft R$ — собственный идеал, и $\mathcal{P}$ — множество всех простых идеалов, содержащих I . Тогда то $\mathcal{P}$ содержит минимальный (по включению) элемент.*

Доказательство. Рассмотрим множество $\mathcal{P}$ всех простых идеалов, содержащих I . Это множество непусто (поскольку любой идеал содержится в некотором простом максимальном, а следовательно, простом идеале). Возьмём произвольную цепь $\{P_\alpha\}$ в $\mathcal{P}$. Тогда $P = \bigcap_\alpha P_\alpha$ — идеал (пересечение цепи идеалов), и он простой: если $a, b \notin P$, то $\exists \alpha, \beta$ такие, что $a \notin P_\alpha, b \notin P_\beta$. Без ограничения общности $P_\alpha \subseteq P_\beta$, тогда $a, b \notin P_\alpha$, значит, $ab \notin P_\alpha \Rightarrow ab \notin P$. Значит, P — простой идеал, содержащий I , и является нижней гранью цепи. По лемме Цорна, в $\mathcal{P}$ есть минимальный элемент, который и будет минимальным простым идеалом над I . $\square$

Теорема 1. *Пусть R — нетерово кольцо, M — конечно порождённый R -модуль, $P \triangleleft R$ — простой идеал. Тогда следующие утверждения эквивалентны:*

- (1) M — P -копримарный модуль (то есть $\text{Ass}_R M = \{P\}$).
- (2) P — минимальный среди простых идеалов, содержащих $\text{ann}(M)$, и любой элемент вне P не является делителем нуля на M .
- (3) Существует $k \in \mathbb{N}$ такое, что $P^k \subseteq \text{ann}(M)$, и любой элемент вне P не является делителем нуля на M .

Доказательство. (1) $\Rightarrow$ (2). Пусть $\text{Ass}_R M = \{P\}$. Тогда P — единственный ассоциированный простой идеал. По теореме 1(a) предыдущей лекции $P \supseteq \text{ann}(M)$. С другой стороны по теореме 1(d) предыдущей лекции $\text{Ass}_R M$ содержит все минимальные среди простых идеалов, содержащих $\text{ann}(M)$. Если Q — некоторый минимальный среди простых идеалов, содержащих $\text{ann}(M)$ (а такой существует, как мы доказали), то $Q \in \text{Ass}_R M = \{P\}$. Значит, $Q = P$.

Так как по теореме 1(b) предыдущей лекции все элементы вне P не являются делителями нуля на M , получаем (2).

(2) $\Rightarrow$ (3). Пусть $I = \text{ann}(M)$. Тогда:

$$\sqrt{I} = \bigcap_{\substack{P \supseteq I \\ P \text{ простой}}} P.$$

Из (2) следует, что P — минимальный среди простых идеалов, содержащих $\text{ann}(M)$. Докажем, что P — единственный минимальный простой идеал, содержащий $\text{ann}(M)$. Действительно, пусть Q — другой минимальный простой

идеал, содержащий $\text{ann}(M)$. Тогда $Q \in \text{Ass}_R M$ (по теореме предыдущей лекции все минимальные простые идеалы над $\text{ann}(M)$ принадлежат $\text{Ass}_R M$). Но по условию, любой элемент вне P не является делителем нуля на M , значит, $Q \subseteq P$ (иначе элементы из $Q \setminus P$ были бы делителями нуля). Так как P минимальный, $Q = P$, то есть P — единственный минимальный простой идеал, содержащий $\text{ann}(M)$.

Таким образом:

$$\sqrt{\text{ann}(M)} = \bigcap_{\substack{\hat{P} \supseteq \text{ann}(M) \\ \hat{P} \text{ простой}}} \hat{P} = P,$$

поскольку P — единственный минимальный простой идеал, содержащий $\text{ann}(M)$, а значит, он лежит в каждом простом идеале, содержащем $\text{ann}(M)$.

Кроме того, поскольку R — нетерово кольцо, идеал P конечно порождён. Пусть $P = (f_1, \dots, f_m)$. Для каждого i существует k_i такие, что $f_i^{k_i} \in \text{ann}(M)$. Положим $k = \sum k_i$. Тогда $P^k \subseteq \text{ann}(M)$.

(3) $\Rightarrow$ (1). Поскольку P — идеал, выполнено $0 \in P$. Все элементы вне P не являются делителями нуля на M , следовательно, если $r \in R \setminus P$, то

$$\forall m \in M, rm = 0 \Rightarrow m = 0.$$

Отсюда следует, что $P \supseteq \text{ann}(M)$. Действительно, если $r \in \text{ann}(M)$, то $rm = 0$ для всех $m \in M$, значит, r — делитель нуля, и по условию $r \in P$.

Так как $P^k \subseteq \text{ann}(M)$, то

$$P \subseteq \sqrt{\text{ann}(M)} = \bigcap_{\substack{Q \supseteq \text{ann}(M) \\ Q \text{ простой}}} Q.$$

Получаем, что все простые идеалы Q , содержащие $\text{ann}(M)$, содержат P . Следовательно,

$$P = \bigcap_{\substack{Q \supseteq \text{ann}(M) \\ Q \text{ простой}}} Q,$$

так как P сам является одним из них, и пересечение не может быть больше, чем P .

Следовательно, P — единственный минимальный простой идеал, содержащий $\text{ann}(M)$. По теореме предыдущей лекции (d), это означает, что $P \in \text{Ass}_R M$.

Теперь покажем, что других ассоциированных идеалов нет. Пусть $Q \in \text{Ass}_R M$. Тогда $Q = \text{ann}(m^*)$ для некоторого $m^* \in M$, $m^* \neq 0$. Так как $Q \supseteq \text{ann}(M)$, и P — единственный минимальный такой идеал, то $Q \supseteq P$. Но включение $Q \supseteq P$ строгое, то существует элемент $r \in Q \setminus P$, который аннулирует m^* , то есть был r является делителем нуля — противоречие с условием (элементы вне P не являются делителями нуля). Значит, $Q = P$.

Таким образом, $\text{Ass}_R M = \{P\}$. $\square$

Теорема 2. Пусть R — нетерово кольцо, M — конечно порождённый R -модуль, $M' \subseteq M$ — подмодуль. Тогда:

- (a) $\text{Ass}_R(M/M') \subseteq \{P_1, \dots, P_n\}$, где $M' = \bigcap_{i=1}^t M_i$, и каждый M_i — P_i -примарный подмодуль. (Такое представление в виде пересечения примарных называется примарным разложением).

- (b) Если это пересечение несократимо (то есть ни один из M_i нельзя убрать без изменения результата), то $\text{Ass}_R(M/M') = \{P_1, \dots, P_n\}$.
- (c) Если пересечение по количеству минимально (т.е. число слагаемых наименьшее возможное), то P_i не повторяются.
- (d) Пусть $U \subseteq R$ — мультипликативно замкнуто, $P_1, \dots, P_t$ — те простые идеалы, которые не пересекаются с U . Тогда:

$$M'[U^{-1}] = \bigcap_{i=1}^t M_i[U^{-1}].$$

Докажем эту теорему в следующий раз, а пока воспользуемся ей.

Пример 1. Пусть R — нетерово целостное кольцо, $f \in R$, и $f = u \cdot \prod_{i=1}^n p_i^{a_i}$, где u — обратимый элемент, p_i — простые элементы. Тогда:

$$(f) = \bigcap_{i=1}^n (p_i^{a_i})$$

есть примарное разложение идеала (f) . Покажем это.

Покажем, что каждый идеал $(p_i^{a_i})$ является P_i -примарным, где $P_i = (p_i)$. Рассмотрим модуль $R/(p_i^{a_i})$. Имеем $\text{ann}(R/(p_i^{a_i})) = \text{ann}(1 + (p_i^{a_i})) = (p_i^{a_i})$. Применим теорему 1 к $P = (p_i)$. Получаем, что удовлетворяется условие (3), а значит, выполнено условие (1), то есть модуль $R/(p_i^{a_i})$ является (p_i) -копримарным.

Теперь нужно показать, что

$$(f) = \bigcap_{i=1}^n (p_i^{a_i}).$$

Для этого нам понадобится следующая лемма.

Лемма 4. Пусть $g \notin P$, где $P = (p)$ — простой идеал. Тогда:

$$(g) \cap (p^\alpha) = (gp^\alpha),$$

Доказательство. $\supseteq$: очевидно, $(gp^\alpha) \subseteq (g) \cap (p^\alpha)$.

$\subseteq$: пусть $h \in (g) \cap (p^\alpha)$. Тогда $h = gr_1 = p^k r_2$ для некоторых $r_1, r_2 \in R$. Тогда из равенства $gr_1 = p^\alpha r_2$ следует, что $p \mid gr_1$, и так как $p \nmid g$, то $p \mid r_1$. Значит, $r_1 = ps$ для некоторого $s \in R$, и тогда $h = gr_1 = gps = p^\alpha r_2$. Поскольку R — область целостности, получаем $gs = p^{\alpha-1} r_2$. Действуя аналогично, получим, что $r_1 = p$, а значит, $h = gr_1 = gp^\alpha \in (gp^\alpha)$. Следовательно, $(g) \cap (p^\alpha) \subseteq (gp^\alpha)$.

Итак, $(g) \cap (p^\alpha) = (gp^\alpha)$. $\square$

Вернёмся к нашему примеру. То, что $f \in \bigcap_i (p_i^{a_i})$ очевидно.

Рассмотрим пересечение двух примарных идеалов: $(p_1^{a_1}) \cap (p_2^{a_2})$. Пусть $g = p_1^{a_1}$, $h = p_2^{a_2}$. Тогда:

$$(p_1^{a_1}) \cap (p_2^{a_2}) = (g) \cap (h).$$

Если $P_1 = (p_1)$, $P_2 = (p_2)$ — различные простые идеалы, то по лемме выше:

$$(g) \cap (h) = (gh) = (p_1^{a_1} p_2^{a_2}),$$

поскольку $g \notin P_2$, $h \notin P_1$. Далее, по индукции: если $(p_1^{a_1}) \cap \dots \cap (p_k^{a_k}) = (p_1^{a_1} \dots p_k^{a_k})$, то добавление $(p_{k+1}^{a_{k+1}})$ даёт:

$$(p_1^{a_1} \dots p_k^{a_k}) \cap (p_{k+1}^{a_{k+1}}) = (p_1^{a_1} \dots p_{k+1}^{a_{k+1}}),$$

так как p_{k+1} не делит произведение $p_1^{a_1} \cdots p_k^{a_k}$ (в целостном кольце). Следовательно, $\bigcap_i (p_i^{a_i}) = (f)$, где $f = u \cdot \prod_i p_i^{a_i}$.

Теорема 3. R — факториально (любой элемент однозначно разложим на неприводимые) $\iff$ любой простой идеал, минимальный над главным, является главным.

Доказательство. $\Rightarrow$ Пусть (f) — главный идеал. Поскольку R факториально, имеем

$$f = u \prod_{i=1}^n p_i^{e_i},$$

где u — обратимый элемент, а p_i — неприводимые. В факториальном кольце неприводимые элементы являются простыми (действительно, если q — неприводим и $q \mid ab$, то из единственности разложения следует, что q делит a или b).

Тогда по теореме 2

$$\text{Ass}(R/(f)) = \{(p_1), \dots, (p_n)\}.$$

Имеем $\text{ann}(R/(f)) = (f)$. Пусть Q — простой идеал, минимальный над (f) . Тогда $Q \in \text{Ass}(R/(f))$, откуда $Q = (p_j)$ для некоторого j . Следовательно, Q — главный.

$\Leftarrow$ Сначала докажем существование разложения на неприводимые. Пусть $f \in R$ не является неприводимым, то есть $f = ab$ с $a, b \notin R^\times$. Тогда $(f) \subsetneq (a)$. Если a также не неприводим, повторяем процесс. Получаем возрастающую цепочку главных идеалов

$$(f) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$$

Кольцо R нётерово, поэтому эта цепочка обрывается. Следовательно, любой элемент допускает разложение на неприводимые.

Теперь докажем единственность разложения. Пусть

$$p_1 \cdots p_k = q_1 \cdots q_m,$$

где все p_i, q_j — неприводимые. По условию любой неприводимый элемент порождает простой идеал: действительно, пусть h — неприводим, тогда (h) содержится в некотором простом идеале P , минимальном над (h) . По предположению P главный, то есть $P = (p)$ для некоторого p . Тогда $h \in (p)$, откуда $h = ps$. Поскольку h неприводим, один из множителей обратим; p не обратим (иначе $P = R$), значит, s обратим, и $h \sim p$. Следовательно, h ассоциирован с простым элементом p , а значит, сам h прост.

Таким образом, все p_i, q_j — простые элементы. Тогда из $p_1 \mid q_1 \cdots q_m$ следует, что $p_1 \mid q_j$ для некоторого j . Без ограничения общности $j = 1$, и тогда $p_1 \sim q_1$. Сокращая обе части на p_1 , получаем

$$p_2 \cdots p_k = u q_2 \cdots q_m$$

для некоторого обратимого u . Продолжая индукцией, получаем $k = m$ и $p_i \sim q_{\sigma(i)}$ для некоторой перестановки σ . Следовательно, разложение единственно с точностью до ассоциированности и порядка множителей.

Итак, R факториально. $\square$