8. Примарное разложение

До конца лекции все кольца и модули считаются нётеровыми, если явно не оговорено противное.

Теперь мы можем наконец перейти непосредственно к разложению (т.е. к аналогу предложения 6.8). Хотелось бы надеяться, что, как подсказывает аналогия с разложением целых чисел на простые множители, всякий идеал в нётеровом кольце представим в виде пересечения $\mathfrak{p}_1^{r_1} \cap \ldots \cap \mathfrak{p}_n^{r_n}$, где $\mathfrak{p}_i$ — простые идеалы. Жизнь, однако, устроена сложнее.

Мы начнем с того, что определим «строительные блоки», которые будут обобщать простые идеалы из предложения 6.8 и степени простых чисел из «основной теоремы арифметики». Работать мы будем по-прежнему для произвольных модулей, причем нам понадобится некоторая подготовка.

Определение 8.1. Пусть M — конечно порожденный модуль над нётеровым кольцом A и $\mathfrak{p} \subset A$ — простой идеал. Подмодуль $Q \subset M$ называется $\mathfrak{p}$-*примарным*, если $\operatorname{Ass}(M/Q) = \{\mathfrak{p}\}$; он называется *примарным*, если он $\mathfrak{p}$-примарен для некоторого $\mathfrak{p}$.

Предложение 8.2. *Если $Q \subset M$ является $\mathfrak{p}$-примарным подмодулем, то $r(\operatorname{Ann}(M/Q)) = \mathfrak{p}$.*

Доказательство. Если $r(\operatorname{Ann}(E)) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ — минимальное разложение в пересечение простых, то каждый из $\mathfrak{p}_i$ лежит в $\operatorname{Ass}(E)$ ввиду предложения 7.12; поскольку с E ассоциирован ровно один простой идеал, заключаем, что $r = 1$ и $r(\operatorname{Ann}(E)) = \mathfrak{p}_1 = \mathfrak{p}$. $\square$

В частности, идеал $\mathfrak{q} \subset A$ является $\mathfrak{p}$-примарным, если $\operatorname{Ass}_A(A/\mathfrak{q}) = \{\mathfrak{p}\}$. В этом случае имеем $r(\mathfrak{q}) = \mathfrak{p}$.

Пример 8.3. Тривиально проверяется, что идеал в $\mathbb{Z}$ является примарным тогда и только тогда, когда он имеет вид (0) или (p^n), где p — простое число; в этом смысле можно считать, что примарные идеалы — обобщение степеней простых чисел. В других кольцах ситуация может быть сложнее. Например, хотя радикал всякого примарного идеала прост, *неверно*, что идеал примарен, как только его радикал является простым идеалом; неверно даже и то, что всякая степень простого идеала является примарным идеалом. Вот пример. Пусть k — поле и $A = k[X, Y, Z]/(XY - Z^2)$ — кольцо функций на квадратичном конусе. Пусть $\mathfrak{p} \subset A$ — идеал, порожденный $\bar{Y}$ и $\bar{Z}$ (образами Y и Z в кольце A; это идеал, соответствующий лежащей на конусе прямой $\{(t, 0, 0)\}$). Идеал $\mathfrak{p}$, очевидно, прост (фактор по нему изоморфен $k[X]$), но идеал $\mathfrak{p}^2$ примарным не является: в $\operatorname{Ass}_A(A/\mathfrak{p}^2)$ лежит как сам идеал $\mathfrak{p}$ (поскольку $\operatorname{supp}(A/\mathfrak{p}^2) = V(\mathfrak{p})$), так и идеал $\mathfrak{m} = (\bar{X}, \bar{Y}, \bar{Z})$ (являющийся аннулятором элемента $\bar{Y} \bmod \mathfrak{p}^2$).

С другой стороны, не всякий примарный идеал является степенью простого: достаточно посмотреть на идеал $(X^2, Y^3) \subset k[X, Y]$.

Сейчас мы построим разложение произвольного идеала в нётеровом кольце в пересечение примарных идеалов (и аналогичное разложение для модулей). Чтобы не прерывать нить изложения, начнем с двух лемм.

Лемма 8.4. *Если $Q_1, \ldots, Q_n$ — $\mathfrak{p}$-примарные подмодули модуля M, то пересечение $Q_1 \cap \ldots \cap Q_n$ тоже $\mathfrak{p}$-примарно.*

Доказательство. Очевидно,

$$M/(Q_1 \cap \ldots \cap Q_n) \subset M/Q_1 \oplus \ldots \oplus M/Q_n.$$

Из предложения 7.5 следует, что Ass от модуля, стоящего в правой части, есть $\{\mathfrak{p}\}$, а тогда то же предложение показывает, что таков же и Ass от модуля, стоящего в левой части. $\square$

Лемма 8.5. *Пусть подмодуль $Q \subset M$ не является пересечением двух подмодулей, отличных от самого Q. Тогда Q примарен.*

Доказательство. Если модуль Q не примарен, то в M/Q существуют подмодули M_1 и M_2, изоморфные $A/\mathfrak{p}_1$ и $A/\mathfrak{p}_2$, где $\mathfrak{p}_1$ и $\mathfrak{p}_2$ — различные простые идеалы. Пересечение $M_1 \cap M_2$ состоит только из нуля, поскольку аннулятор всякого ненулевого элемента в M_1 совпадает с $\mathfrak{p}_1$, а в M_2 — с $\mathfrak{p}_2$; беря прообразы в M, получаем разложение Q в пересечение двух строго больших модулей. $\square$

Теперь мы можем, наконец, сформулировать и доказать теорему о примарном разложении.

Определение 8.6. Пусть N — собственный подмодуль модуля M. Тогда его *минимальным примарным разложением* называется представление $N = Q_1 \cap \ldots \cap Q_n$, где все подмодули $Q_i \subset M$ примарны и их количество — наименьшее возможное.

Теорема 8.7. *Пусть M — конечно порожденный модуль над нётеровым кольцом и $N \subset M$ — его подмодуль. Тогда:*

(i) *Существует минимальное примарное разложение $N = Q_1 \cap \ldots \cap Q_n$.*

(ii) *Если в этом разложении подмодуль Q_i является $\mathfrak{p}_i$-примарным, то все простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ различны и $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \operatorname{Ass}(M/N)$.*

(iii) *Если $\mathfrak{p} \in \operatorname{Ass}(M/N)$ — изолированный ассоциированный идеал, то $\mathfrak{p}$-примарный подмодуль из минимального примарного разложения модуля N не зависит от выбора этого минимального разложения.*

Доказательство. Не ограничивая общности, можно считать, что $N = 0$, что мы при необходимости и будем предполагать.

Докажем сначала, что всякий собственный подмодуль в M представим в виде конечного пересечения примарных подмодулей. В самом деле, если это не так, то существует максимальный собственный подмодуль $M' \subset M$, не представимый в виде такого пересечения. Поскольку при этом сам M' примарным быть не может, лемма 8.5 показывает, что M' является пересечением двух строго больших подмодулей M_1 и M_2. Ввиду максимальности M' каждый из модулей M_1 и M_2 представим в виде конечного пересечения примарных подмодулей, а значит, таков и $M = M_1 \cap M_2$.

Итак, N является пересечением конечного числа примарных подмодулей; выбирая разложение минимальной длины, получаем минимальное примарное разложение $N = Q_1 \cap \ldots \cap Q_n$. Этим доказано (i).

Если два модуля Q_i и Q_j являются $\mathfrak{p}$-примарными с одним и тем же $\mathfrak{p}$, то $Q_i \cap Q_j$ также $\mathfrak{p}$-примарен; заменяя в разложении пару (Q_i, Q_j) на пересечение $Q_i \cap Q_j$, получаем более короткое примарное разложение в противоречие с его минимальностью. Этим доказано, что все идеалы $\mathfrak{p}_i$ различны.

Далее, из равенства $N = Q_1 \cap \ldots \cap Q_n$ следует, что M/N вкладывается в $M/Q_1 \oplus \ldots \oplus M/Q_n$. Поскольку Ass от правой части, как показывает предложение 7.5, равен $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, из того же предложения следует, что $\mathrm{Ass}(M/N) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Обратно, зафиксируем $j \in [1; n]$ и покажем, что $\mathfrak{p}_j \in \mathrm{Ass}(M/N)$. Будем считать, что $N = 0$. Поскольку $\bigcap_i Q_i = 0$, пересечение $\bigcap_{i \neq j} Q_i$ вкладывается в M/Q_j. Поскольку $\bigcap_{i \neq j} Q_i \neq 0$ и $\mathrm{Ass}(M/Q_j) = \{\mathfrak{p}_j\}$, предложение 7.5 показывает, что $\mathrm{Ass}(\bigcap_{i \neq j} Q_i) = \{\mathfrak{p}_j\}$, откуда в силу того же предложения имеем $\mathfrak{p}_j \in \mathrm{Ass}(M)$. Стало быть, $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \mathrm{Ass}(M)$, чем завершается доказательство утверждения (ii).

Пусть, наконец, $\mathfrak{p}_i \in \mathrm{Ass}(M/N)$ — изолированный ассоциированный простой идеал. Опять будем считать, что $N = 0$. Докажем равенство $Q_i = \mathrm{Ker}\,\varphi$, где $\varphi\colon M \to M_{\mathfrak{p}_i}$ — каноническое отображение (отсюда, очевидно, вытекает утверждение о независимости Q_i от выбора минимального разложения).

Покажем сначала, что $\mathrm{Ker}\,\varphi \subset Q_i$. Заметим, что множество M/Q_i-делителей нуля совпадает с $\mathfrak{p}_i$. Если теперь $\varphi(x) = 0$, то $sx = 0$ для некоторого $s \in A \setminus \mathfrak{p}_i$, так что $x \bmod Q_i = 0$ и $x \in Q_i$.

Покажем теперь, что $Q_i \subset \mathrm{Ker}\,\varphi$. Поскольку $\mathfrak{p}_i \in \mathrm{Ass}(M)$ — изолированный идеал, имеем $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ при $j \neq i$, так что для всякого $j \neq i$ существует элемент $s_j \in \mathfrak{p}_j \setminus \mathfrak{p}_i$. Пусть теперь $x \in Q_i$. Поскольку $\mathfrak{p}_j = r(\mathrm{Ann}(M/Q_j))$, для всякого $j \neq i$ существует такое $m_j > 0$, что $s_j^{m_j} x \in Q_j$. Положим $s = \prod_{j \neq i} s_j^{m_j}$. Тогда $s \notin \mathfrak{p}_i$ и $sx \in Q_j$, как только $j \neq i$. Поскольку, кроме того, $sx \in Q_i$, элемент sx лежит в пересечении *всех* Q_i и тем самым равен нулю. $\square$

Замечание 8.8. Единственность подмодулей Q_i в минимальном примарном разложении, соответствующих *вложенным* ассоциированным идеалам, в теореме не утверждается; более того, если вложенные идеалы присутствуют, то соответствующие им компоненты примарного разложения *никогда* не определены однозначно.

Пример 8.9. Пусть $A = k[x, y]$, где k-поле, и пусть $\mathfrak{a} = (y^2, xy)$ (словами: $\mathfrak{a}$ — множество многочленов f, тождественно равных нулю на оси абсцисс и таких, что $f_y(0, 0) = 0$). Тогда для всякого ненулевого $\lambda \in k$ имеем минимальное примарное разложение $\mathfrak{a} = (y) \cap (y - \lambda x, y^2)$, в котором идеал (y) примарен (и даже прост), а идеал $(y - \lambda x, y^2)$ является (x, y)-примарным и соответствует вложенному ассоциированному идеалу. (Условие $f \in (y)$ означает «f — тождественный нуль на оси абсцисс», а условие $f \in (y - \lambda x, y^2)$ означает, что $f(0, 0) = 0 = f_y(0) - \lambda f_x(0)$.)

Приложение: теорема Крулля

В качестве приложения изложенной теории докажем следующий факт.

Предложение 8.10 (теорема Крулля). *Пусть $\mathfrak{a}$ — собственный идеал в нётеровом кольце A; предположим, что A либо целостно, либо локально. Тогда $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = 0$.*

Доказательство. Начнем с леммы.

Лемма 8.11. *Пусть $\mathfrak{a}$ — простой идеал в нётеровом кольце A, M — конечно порожденный A-модуль и $Q \subset M$ — $\mathfrak{p}$-примарный подмодуль. Если $N \subset M$ — такой подмодуль, что $\mathfrak{a}N \subset Q$, то либо $\mathfrak{a} \subset \mathfrak{p}$, либо $N \subset Q$.*

Доказательство леммы. Множество M/Q-делителей нуля совпадает с $\mathfrak{p}$; если теперь $f \in \mathfrak{a} \setminus \mathfrak{p}$, то из $fN \subset Q$ вытекает, что образ N в M/Q является нулевым, то есть $N \subset Q$. □

Перейдем к доказательству предложения. Положим $I = \bigcap_{n=1}^{\infty} \mathfrak{a}^n$ и покажем, что $I \subset \mathfrak{a}I$. В самом деле, поскольку $\mathfrak{a}I$ является пересечением примарных идеалов, достаточно показать, что $I \subset \mathfrak{q}$ для всякого примарного идеала $\mathfrak{q}$, содержащего $\mathfrak{a}I$. И действительно, пусть $\mathfrak{a}I \subset \mathfrak{q}$, где $\mathfrak{q}$ — $\mathfrak{p}$-примарный идеал. Применяя лемму к случаю $M = A$, $Q = \mathfrak{q}$, $N = I$, получаем, что либо $\mathfrak{a} \subset \mathfrak{p}$, либо $I \subset \mathfrak{q}$. Во втором случае доказывать нечего, а в первом заметим, что $\mathfrak{p} = r(\mathfrak{q})$, откуда $\mathfrak{a}^n \subset \mathfrak{q}$ для некоторого n, так что и подавно $I \subset \mathfrak{q}$.

Итак, $I \subset \mathfrak{a}I$, так что $I = \mathfrak{a}I$. Из леммы Накаямы (предложение 4.3) теперь следует, что $(1 + f)I = 0$ для некоторого $f \in \mathfrak{a}$. Если A целостно, то равенство $I = 0$ отсюда следует с очевидностью, а если A локально, то оно следует из того, что f лежит в максимальном идеале и тем самым $1 + f$ обратимо. □