Коммутативная алгебра.

1 Идеалы

Все кольца будут коммутативными ($1 \neq 0$). R по умолчанию кольцо. Идеал считаем отличным от всего кольца.

Определение 1.1. Идеал называется *максимальным*, если он не содержится ни в каком другом идеале.

Напоминание. Идеал m в кольце R максимальный, если и только если R/m — поле.

Лемма Цорна. Если в частично упорядоченном множестве M для всякого линейного упорядоченного подмножества существует верхняя грань, то в M существует максимальный элемент.

Теорема 1.1. Каждый идеал содержится в каком-то максимальном.

Доказательство. Рассмотрим какую-то цепочку вложенных идеалов, там есть верхняя грань. Тогда по лемме Цорна есть максимальный элемент. □

Задача 1.1. Пусть I, J — идеалы. Докажите, что $I \cup J$ — идеал тогда и только тогда, когда один из этих идеалов вкладывается в другой.

Доказательство. Предположим противное, тогда существует элемент $i \in I$, $i \notin J$ и такой элемент $j \in J$, $j \notin I$. Тогда $i + j \notin I \cup J$.

□

Напоминание. Для любого необратимого элемента существует содержащий его идеал.

Определение 1.2. Кольцо называется *локальным (полулокальным)*, если в нем ровно один (конечно) максимальный идеал.

Предложение 1.1. Пусть $\mathfrak{m} \subset R$ — идеал. Если любое $x \in R \backslash \mathfrak{m}$ обратимо, тогда кольцо локально, а $\mathfrak{m}$ — максимальный.

Доказательство. Пусть I — какой-то другой идеал. Он не содержит обратимых элементов, следовательно, содержится в $\mathfrak{m}$, то есть $\mathfrak{m}$ — максимальный и единственный среди максимальных. □

Предложение 1.2. Пусть $\mathfrak{m}$ — такой максимальный идеал, что любой элемент из множества $1 + \mathfrak{m}$ обратим, тогда $(R, \mathfrak{m})$ — локальное.

Доказательство. Докажем, что выполнено условие предыдущего предложения.

Пусть $x \in R \backslash \mathfrak{m}$, тогда сущетвует такие $t \in \mathfrak{m}$ и $y \in R$, что $xy + t = 1$ (потому что $(\mathfrak{m}, x) = R$). Таким образом, xy обратимо, а значит, x — тоже.

□

Определение 1.3. Идеал $\mathfrak{p}$ называется *простым*, если для любого $ab \in \mathfrak{p}$ или $a \in \mathfrak{p}$, или $b \in \mathfrak{p}$.

Напоминание. Идеал прост, если и только если $R \backslash \mathfrak{p}$ — область целостности.

Следствие 1.1. Любой максимальный идеал является простым.

Замечание 1.1. Но существуют простые идеалы, не являющиеся максимальными. Например, $\langle x \rangle \in \Bbbk[x, y]$ прост, но не максимален.

2 Радикалы

Определение 2.1. *Радикалом* идеала I называется $\sqrt{I} = \left\{x \in R \;\middle|\; x^n \in I\right\}$.

Замечание 2.1. Это, кстати, тоже идеал.

Определение 2.2. Подмножество $S \subset R$ называется *мультипликативным*, если выполнены следующие свойства:

(1) если $x, y \in S$, то $xy \in S$;

(2) $1 \in S$.

Теорема 2.1. Пусть S — мультипликативно, I — идеал. $I \cap S = \varnothing$. Тогда существует такой простой идеал P, что $I \subset P$ и $S \cap P = \varnothing$.

Доказательство. По лемме Цорна в множестве идеалов, содержащих I и не пересекающихся с S, есть максимальный элемент P.

Докажем, что P прост. Действтельно, пусть так случилось, что $x, y \notin P$.

Тогда $(P + xR) \cap S \neq \varnothing$ и $(P + yR) \cap S \neq \varnothing$ в силу максимальности P. Тогда по мультипликативности $(P + xR)(P + yR) \cap S \neq \varnothing$. Но отсюда следует, что $(P + xyR) \cap S \neq \varnothing$, значит $xy \notin P$ тоже.

$\square$

Теорема 2.2. $\sqrt{I} = \bigcap\limits_{I \subset \mathfrak{p}} \mathfrak{p}$, где $\mathfrak{p}$ — простой.

Доказательство. Пусть $I \subset \mathfrak{p}$, тогда $x^n \in I \subset \mathfrak{p}$, тогда $x \in \mathfrak{p}$. То есть все элементы $\sqrt{I}$ содержатся в правой части.

Осталось доказать, что справа нет ничего лишнего. Пусть элемент $x \notin \sqrt{I}$. Тогда мультипликативное множество $S = \left\{1, x, x^2, \ldots,\right\}$ не пересекается с I и по предыдущей теореме существует идеал $\mathfrak{p}$, разделяющий их.

$\square$

Определение 2.3. *Нильрадикалом* называется $nil(R) = \sqrt{0}$ — множество всех *нильпотентных* элементов.

Замечание 2.2. В силу теоремы 2.2 $nil(R) = \bigcap\limits_{\mathfrak{p}} \mathfrak{p}$, где $\mathfrak{p}$ — простой.

Определение 2.4. Если $nil(R) = 0$, то R называется *редуцированным*, а взятие фактора $R_{red} = R\backslash nil(R)$ — *редукцией.*

Определение 2.5. *Радикалом Джекобсона* называется $J(R) = rad(R) = \bigcap\limits_{\mathfrak{m}} \mathfrak{m}$, где $\mathfrak{m}$ — максимальный идеал.

Теорема 2.3. $x \in J(R)$ тогда и только тогда, когда $1-xy$ обратим для любого $y \in R$.

Доказательство. Пусть $x \in rad(R)$ и $1 - xy$ необратим. Тогда $(1 - xy)$ — идеал, содержащийся в некотором максимальном $\mathfrak{m}$. Но тогда $1 \in \mathfrak{m}$.

Обратно, предположим, такое $x \notin rad(R)$. Тогда существует такой максимальный идеал $\mathfrak{m}$, что $x \notin \mathfrak{m}$. Тогда $\mathfrak{m} + xR = R$ и $1 = u + xy$ (для некоторых $u \in \mathfrak{m}, y \in R$). Тогда $1 - xy = u \in m$ — необратимый, что и требовалось.

□

3 Операции над идеалами

Задача 3.1. Если $I + J = (1)$, то $IJ = I \cap J$.

Доказательство. Очевидно, что $IJ \subset I \cap J$. С другой стороны,

$$(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ.$$

Первое равенство верно в силу дистрибутивности

$$(a + b)c = ac + bc.$$

□

Определение 3.1. Идеалы I, J называются *взаимно простыми*, если $I + J = (1)$.

Китайская теорема об остатках. Пусть $I_1, I_2, \dots, I_n$ — идеалы и гомоморфизм $\varphi : R \to \prod R\backslash I_i$. Тогда

(1) Если $I_i + I_j = (1)$, то $\bigcap I_i = \prod I_i$;

(2) φ сюръективно тогда и только тогда, когда $I_i + I_j = (1)$;

(2) φ инъективно тогда и только тогда, когда $\bigcap I_i = (0)$.

Prime Avoidance. Пусть $I \subset R$ содержится в $\bigcup\limits_{i=1}^{n} p_i$, где p_i — идеалы, последние $(n - 2)$ из которых просты. Тогда $I \subset p_i$ для какого-то i.

Доказательство. Будем доказывать по индукции по n.

- $n = 1$. Тут и доказывать нечего.

- Выберем $x_i \in p_i \cap I$ и $x_i \notin \bigcup\limits_{j \neq i} p_j$ (иначе побеждаем по предположению индукции).

  Теперь случай для $n = 2$ тоже стал тривиальным: $x_1 + x_2 \in I$ (противоречие с выбором x_i).

  Пусть $n \geqslant 3$ и $x = x_1 x_2 \dots x_{n-1} + x_n \in I$, но $x \notin p_n$ (из простоты p_n) и $x \notin p_j$ (в силу выбора x_n).

□

Предложение 3.1. **(1)** Пусть $I_1, \dots, I_n$ — идеалы, p — такой простой идеал, что $\bigcap I_i \subset p$ тогда $I_i \subset p$ для некоторого i.

(2) Если $\bigcap I_i = p$, то $I_i = p$ для некоторого i.

Доказательство. **(1)** Предположим противное, тогда для любого i существует $x_i \notin p$ и $x_i \in I_i$. Тогда $x_1 x_2 \dots x_n \notin p$.

(2) Если это не так, то и первое равенство не верно.

□

Определение 3.2. *Частным* идеалов I, J называется множество

$$(I : J) = \left\{ x \in R \;\middle|\; xJ \subset I \right\}.$$

Нетрудно заметить, что это тоже идеал.

Задача 3.2. **(1)** $I \subset (I : J)$;

(2) $(I : J)J \subset J$;

(3) $((I : K) : K) = (I : JK) = ((I : K) : J)$;

(4) $(\bigcap I_i : J) = \bigcap (I_i : J)$;

(5) $(I : \sum J_i) = \bigcap (I : J_i)$.

Пусть $f : R \to S$ — гомоморфизм колец. Пусть $J \subset S$ — идеал.

Определение 3.3. *Сужением* идеала J называется $J^c = f^{-1}(J)$ — тоже идеал.

Замечание 3.1. В другую сторону не работает: $f(I)$ в общем случае — не идеал (например, вложение $\mathbb{Z}$ в $\mathbb{Q}$).

Определение 3.4. *Расширением идеала* I называется $I^e = \left\{ \sum y_i f(x_i) \;\middle|\; x_i \in I, y_i \in S \right\}$ — тоже идеал (в определении буквально написано, что это идеал, натянутый на образ $f(I)$).

Задача 3.3. **(1)** $I \subset I^{ec}$, $J \supset J^{ce}$;

(2) $I^e = I^{ece}$, $J^c = J^{cec}$;

(3) Пусть C — множество идеалов в R, которые являются сужениями, а E — множество идеалов в S, которые являются расширениями. Тогда

$$C = \left\{ I \in R \;\middle|\; I^{ec} = I \right\},\ E = \left\{ J \in S \;\middle|\; J^{ce} = J \right\}$$

Кроме того, отображение $I \mapsto I^e$ является биекцией $C \to E$ с обратным отображением $J \mapsto J^c$.

4 Модули

Определение 4.1. Пусть M — это $R-$модуль. *Аннулятором* M называется $Ann(M) = \{x \in R \mid xM = 0\} = (0 : M)$.

Определение 4.2. *Радикалом* модуля M называется $rad(M) = \bigcap\limits_{Ann(M) \subset m} m$, где m — максимальный идеал.

Замечание 4.1. Ясно, что **(1)** $rad(M)/Ann(M) \simeq rad(R/Ann(M))$.

(2) Если N — подмодуль M, то $Ann(M) \subset Ann(N)$ и $rad(M \subset rad(N))$.

(3) $Ann(M) \subset Ann(M/N)$ и $rad(M) \subset rad(M/N)$.

Определение 4.3. M называется *(полу)локальным,* если $R/Ann(M)$ (полу) локально.

Определение 4.4. Модуль называется *строгим*, если у него нулевой аннулятор.

Предложение 4.1. Пусть $x \in rad(M)$, $m \in M$. Если $(1 + x)m = 0$, то $m = 0$

Доказательство. Рассмотрим идеал $I = (AnnM, 1 + x)$. Если $I = R$, то для некоторых $n \in AnnM$, $y \in R$ выполнено $n + (1 + x)y = 1$. Тогда

$$m = 1 \cdot m = nm + y(1 + x)m = 0,$$

что и требовалось.

В противном случае I содержится в некотором максимальном идеале $\mathfrak{m}$. По условию $x \in \mathfrak{m}$, а по построению $1 + x \in \mathfrak{m}$, то есть $\mathfrak{m} = R$, противоречие. □

Напоминание. Модуль M конечно порожден тогда и только тогда, когда $M \simeq R^n/N$, $N \subset R^n$ — подмодуль.

Пусть $A \in Mat_{n\times n}(R)$, $P_A(t)$ — характеристический многочлен.

Теорема Гамильтона-Кэли. Пусть M — модуль, порожденный $m_1, \dots, m_n$. Отображение $\varphi \in End(M)$ таково, что $\varphi(m_i) = \sum\limits_{j=1}^{n} A_i^j m_j$. Тогда $P_A(\varphi) = 0$.

Доказательство. Напишем тождество:

$$(tE - A)(tE - A)^* = P_A(t)E,$$

звездочкой обозначается сопряженная матрица (та, которая из миноров состоит). Подставим $t = A$, получим то, что хотелось. □

Следствие 4.1. Пусть M — конечно порожденный модуль, I — идеал. Тогда $M = IM$ тогда и только тогда, когда существует такое $a \in I$, что $(1+a)M = 0$.

Доказательство. Пусть $M = IM$. Тогда существует матрица A, выражающая образующие друг через друга с коэффициентами из I. Пусть $P_A(t) = t^n + c_{n-1}t^{n-1} + \ldots + c_0$. Положим $a = c_0 + \ldots + c_{n-1}$. Тогда $(1+a)M = P_A(Id)M = 0$ (последнее верно по теореме Гамильтона-Кэли).

Обратно, если $(1+a)M = 0$, то $m = -am$. То есть $M \subset MI$.

□

Следствие 4.2. M — конечно порожденнный модуль, $\varphi \in End(M)$. Если φ сюръективное, то это изоморфизм.

Доказательство. Рассмотрим кольцо $P = R[x]$, пусть x действует на M как φ. Таким образом, M — P – модуль. Применим предыдущее следствие к $I = (x) \subset P$. Из условия следует, что $M = IM$. Тогда существует такое $x \cdot g(x) = a \in I$, что $(1+a)M = 0$. Таким образом, $Id + \varphi g(\varphi) = 0$. Обратное отображение существует (это в точности $-g(\varphi)$).

□

Следствие 4.3. Пусть R^n — свободный модуль, тогда любые его n образующих $v_1, \ldots, v_n$ — свободный базис.

Доказательство. Рассмотрим сюръекцию, переводящую свободные образующие e_i в данные v_i. По следствию 4.2 эта сюръекция — изоморфизм. Но тогда никаких соотношений на образующие нет(иначе было бы ядро). □

Следствие 4.4. Пусть m, n — натуральные. Тогда $R^n \simeq R^m$ только тогда, когда $n = m$.

Доказательство. Пусть без ограничения общности $m \leqslant n$. Дополним m образующих в R^m $n-m$ нулями и посмотрим на образ получившейся системы при изоморфизме. Получилась снова система образующих, тогда по следствию 4.3 не может быть нулей. □

Лемма Накаямы. Пусть M — конечно порожденный R – модуль, $I \subset rad(M)$ — некоторый идеал. Если $IM = M$, то $M = 0$.

Доказательство. По следствию 4.1 существует такое $a \in I$, $(1+a)M = 0$. Тогда по предложению 4.1 $M = 0$.

□

Предложение 4.2. $N \subset M$, $I \in rad(M)$.

(1) Если M/N — конечнопорожденный и $N + IM = M$, тогда $N = M$.

(2) Если M — конечнопорожденный, то $m_1, \ldots m_n$ порождают M тогда и только тогда, когда $m'_1, \ldots, m'_n$ порождают M/IM (штрихи тут обозначают как класс эквивалентности при факторизации, так и некоторых представителей класса).

Доказательство. **(1)** $I(M/N) = (M/N)$, отсюда по лемме Накаямы $(N/M) = 0$.

(2) Доказательство прямого утверждения очевидно, докажем обратное. Пусть N — подмодуль, порожденный $m'_1, \ldots, m'_n$. Поскольку M — конечнопорожденный, M/N — тоже. Тогда $N + IM = M$ и по предыдущему утверждению $N = M$. □

5 Произведения и прямые суммы модулей.

Пусть $\{M_\lambda\}_{\lambda \in \Lambda}$ — семейство R-модулей.

Определение 5.1. *Произведением* называется множество

$$\prod_{\lambda \in \Lambda} M_\lambda = \big\{(m_\lambda) \;\big|\; m_\lambda \in M_\lambda\big\}.$$

Замечание 5.1. $\mathrm{Hom}(R^{\oplus \Lambda}, M) = \prod\limits_{\lambda \in \Lambda} M.$

Определение 5.2. *Прямой суммой* называется множество

$$\bigoplus_{\lambda \in \Lambda} M_\lambda = \big\{(m_\lambda) \;\big|\; m_\lambda \in M_\lambda, \text{ где лишь конечное число} m_\lambda \text{ отлично от нуля}\big\}.$$

Определение 5.3. *Каноническая проекция* $\pi_k : \prod M_\lambda \to M_k$ определяется естественным образом.

Определение 5.4. *Каноническое вложение* $i_k : M_k \to \bigoplus M_\lambda$ тоже определяется естественным образом.

6 Точные последовательности

Тут мы обычно считаем модули конечно порожденными.

Определение 6.1. Последовательность $R-$модулей и гомоморфизмов

$$\ldots M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \ldots$$

называется *точной,* если $\mathrm{im}(f_i) = \ker(f_{i+1})$.

Пример 6.1. (1) $0 \to M \xrightarrow{g} M'$ точна тогда и только тогда, когда g инъективен.

(2) $M \xrightarrow{f} M' \to 0$ точна тогда и только тогда, когда f сюръективен.

(3) $0 \to M' \xrightarrow{g} M \xrightarrow{f} M'' \to 0$ точна тогда и только тогда, когда g инъективен, f сюръективен и $\mathrm{im}(g) = \ker(f)$. Такая последовательность называется *короткой точной последовательностью.*

Замечание 6.1. Пусть дано семейство $0 \to M'_\lambda \xrightarrow{g} M_\lambda \xrightarrow{f} M''_\lambda \to 0$ коротких точных последовательностей. Тогда

$$0 \to \bigoplus_{\lambda \in \Lambda} M'_\lambda \xrightarrow{g} \bigoplus_{\lambda \in \Lambda} M_\lambda \xrightarrow{f} \bigoplus_{\lambda \in \Lambda} M''_\lambda \to 0$$

и

$$0 \to \prod_{\lambda \in \Lambda} M'_\lambda \xrightarrow{g} \prod_{\lambda \in \Lambda} M_\lambda \xrightarrow{f} \prod_{\lambda \in \Lambda} M''_\lambda \to 0$$

— тоже точные.

Определение 6.2. Короткая точная последовательность

$$0 \to M' \xrightarrow{g} M \xrightarrow{f} M'' \to 0$$

называется *расщепленной*, если существует изоморфизм $\varphi : M \xrightarrow{\simeq} M' \oplus M''$, для которого $\varphi g = i_{M'}$, $f = \pi_{M''}\varphi$.

Предложение 6.1. Пусть дана точная последовательность $M' \xrightarrow{g} M \xrightarrow{f} M''$. Следующие утверждения эквивалентны:

(1) Её дополнение до короткой точной — расщепленная.

(2) Существует такое $\rho : M \to M'$, что $\rho g = \mathrm{id}_{M'}$ (*ретракция*) и f — сюръекция.

(3) Существует такое $\sigma : M'' \to M$, что $f\sigma = \mathrm{id}_{M''}$ (*сечение*) и g — инъекция.

Доказательство. (1) $\Rightarrow$ (2) В качестве такого ρ подойдет $\rho = \pi_{M'}\varphi$, сюръективность f в силу точности последовательности.

(2) $\Rightarrow$ (3) g — инъективно (если $g(m) = 0$, то $\mathrm{id}(m) = 0$). Ясно, что $M/\ker(f) \simeq M''$. Тогда можно выбрать подмодуль $N \subset M$, для которого $f : N \xrightarrow{\simeq} M''$. Пусть тогда σ отправляет элементы M'' в их представителей в N.

(3) $\Rightarrow$ (1) В силу предыдущих обозначений $M \simeq (M/N) \oplus N$, причем $\sigma : M'' \xrightarrow{\simeq} N$ и $g : M' \xrightarrow{\simeq} (M/N)$. Если два изоморфизма склеить, получится искомый φ.

$\square$

Предложение 6.2. Последовательность $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ точна тогда и только тогда, когда точна $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{\beta}} \mathrm{Hom}(M, N) \xrightarrow{\bar{\alpha}} \mathrm{Hom}(M', N)$, где $\bar{\alpha}(f) = f\alpha$, $\bar{\beta}(f) = f\beta$.

Доказательство. Из первого второе следует очевидно.

Теперь, $\bar{\beta}$ инъективно, $\mathrm{im}(\bar{\beta}) = \ker(\bar{\alpha})$. Тогда β сюрьективно. Теперь нужно показать, что $\ker\beta = \mathrm{im}\alpha$. Положим $N = M''$, рассмотрим $f = \mathrm{id}_{M''} \in \mathrm{Hom}(M'', M'')$. По условию $0 = \overline{\alpha}(\overline{\beta}(f)) = \overline{\alpha}(\beta) = \beta\alpha$. Таким образом, $\mathrm{im}(\alpha) \in \ker(\beta)$.

Положим теперь $N = M/\mathrm{im}(\alpha)$, $\varphi \in \mathrm{Hom}(M, N)$ — отображение факторизации. Поскольку $\overline{\alpha}(\varphi) = 0$, то существует такое $\psi \in \mathrm{Hom}(M'', N)$, что $\varphi = \overline{\beta}(\psi) = \psi\beta$. То есть в образе ничего лишнего нет.

□

Предложение 6.3. Последовательность $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ точна тогда и только тогда, когда точна $0 \to Hom(N.M') \xrightarrow{\bar{\alpha}} Hom(N, M) \xrightarrow{\bar{\beta}} Hom(N, M'')$.

Доказательство. Аналогично доказательству предложения 6.2 здесь будет игра в подбирание N и гомоморфизма. □

Определение 6.3. *Представлением (конечным)* модуля называется точная последовательность $F_1 \to F_0 \to M \to 0$, где F_1, F_0 свободные (конечного ранга).

Предложение 6.4. Пусть R — кольцо, R — модуль, $\{m_\lambda\}_{\lambda\in\Lambda}$ — семейство образующих. Тогда существует короткая точная последовательность

$$0 \to K \to R^{\oplus\Lambda} \xrightarrow{\alpha} M \to 0,$$

где $\alpha(r_\lambda) = m_\lambda$, $K = \ker K$. Эта последовательность определяет представление

$$R^{\oplus\Sigma} \to R^{\oplus\Lambda} \xrightarrow{\alpha} M \to 0.$$

Доказательство. Построенная последовательность точна по жизни. Нужно лишь отметить, что Σ — множество индексов образующих ядра K. □

Определение 6.4. Модуль P называется *проективным* если для любого эпиморфизма $f : N \to M$ и любого гомоморфизма $g : P \to M$ существует такое $h : P \to N$, что $g = fh$ или диаграмма коммутативна:

$$\begin{tikzcd} P \arrow[r, dashed, "\exists h"] \arrow[dr, "g"'] & N \arrow[d, two heads, "f"] \\ & M \end{tikzcd}.$$

Теорема 6.1. Следующие утверждения эквивалентны:
(1) P — проективный R – модуль;
(2) любая точная последовательность $0 \to K \to M \to P \to 0$ расщепленная;
(3) существует такой модуль K, что $K \oplus P$ — свободный;

(4) для каждой точной последовательности $N' \to N \to N''$ последовательность $Hom(P, N') \to Hom(P, N) \to Hom(P, N'')$;

(5) любое сюрьективное отображение $N \xrightarrow{\beta} N'' \to 0$ индуцирует сюрьекцию $Hom(P, N) \xrightarrow{\overline{\beta}} Hom(P, N'') \to 0$.

Доказательство. (1) $\Rightarrow$ (2) Рассмотрим произвольную точную последовательность

$$0 \to K \xrightarrow{g} M \xrightarrow{f} P \to 0.$$

Для сюръекции f существует сечение $h : P \to M$, которое делает диаграмму коммутативной:

$$\begin{tikzcd} P \arrow[r, "h"] \arrow[dr, "id"'] & M \arrow[d, two heads, "f"] \\ & P \end{tikzcd} .$$

Тогда по предложению 6.1 последовательность действительно расщепленная.

(2) $\Rightarrow$ (3) Рассмотрим K и $M = R^{\oplus\lambda}$ из предложения 6.4 (такой M свободен).

(3) $\Rightarrow$ (4) Продублируем данную точную поледовательность для всех $\lambda \in \Lambda$:

$$N'_\lambda \to N_\lambda \to N''_\lambda.$$

В силу замечания 6.1 есть точная последовательность:

$$\prod_{\lambda\in\Lambda} N'_\lambda \to \prod_{\lambda\in\Lambda} N_\lambda \to \prod_{\lambda\in\Lambda} N''_\lambda.$$

А по замечанию 5.1 есть точная последовательность:

$$\mathrm{Hom}(R^{\otimes\Lambda}, N'_\lambda) \to \mathrm{Hom}(R^{\otimes\Lambda}, N_\lambda) \to \mathrm{Hom}(R^{\otimes\Lambda}, N''_\lambda).$$

Поскольку $K \oplus P = R^{\otimes\Lambda}$, последнюю точную последовательность пожно расщепить на две, одна из которых икомая.

(4) $\Rightarrow$ (5) Достаточно положить $N' = \ker\beta$.

(5) $\Rightarrow$ (1) Следствие того, что диаграмма коммутативна

$$\begin{tikzcd} P \arrow[r, "\overline{\beta}(g)"] \arrow[dr, "g"'] & N \arrow[d, two heads, "\beta"] \\ & N'' \end{tikzcd} .$$

$\square$

Лемма Шаунеля. Предположим, что M — R – модуль и есть две точные последовательности

$$0 \to K_1 \xrightarrow{i_1} P_1 \xrightarrow{\alpha_1} M \to 0,$$

$$0 \to K_2 \xrightarrow{i_2} P_2 \xrightarrow{\alpha_2} M \to 0.$$

Модули P_1, P_2 — проективны. Тогда существуют такие вертикальные стрелки, что диаграмма коммутативна:

$$\begin{tikzcd}
0 \arrow[r] & K_1 \oplus P_2 \arrow[r, "i_1 \otimes id_{P_2}"] \arrow[d, "\beta", "\simeq"'] & P_1 \oplus P_2 \arrow[r, "{(\alpha_1, 0)}"] \arrow[d, "\gamma", "\simeq"'] & M \arrow[r] \arrow[d, "id_M", "\simeq"'] & 0 \\
0 \arrow[r] & K_2 \oplus P_1 \arrow[r, "i_1 \otimes id_{P_1}"] & P_2 \oplus P_1 \arrow[r, "{(\alpha_2, 0)}"] & M \arrow[r] & 0
\end{tikzcd}$$

Тогда $K_1 \oplus P_2 = K_2 \oplus P_1$.

Доказательство. Построим коммутативную диаграмму

$$\begin{tikzcd}
0 \arrow[r] & K_1 \oplus P_2 \arrow[r, "i_1 \otimes id_{P_2}"] & P_1 \oplus P_2 \arrow[r, "{(\alpha_1, 0)}"] & M \arrow[r] & 0 \\
0 \arrow[r] & L \arrow[r] \arrow[u, "\lambda"', "\simeq"] & P_1 \oplus P_2 \arrow[r, "{(\alpha_1, \alpha_2)}"] \arrow[u, "\theta"', "\simeq"] & M \arrow[r] \arrow[u, "id"', "\simeq"] & 0
\end{tikzcd}$$

где $L = \ker(\alpha_1, \alpha_2)$, $\theta = \begin{pmatrix} 1 & \pi \\ 0 & 1 \end{pmatrix}$ (здесь π — такой гомоморфизм, который существует по проективности, то есть $\alpha_1 \pi = \alpha_2$). Изоморфизм λ индуцируется изоморфизмом θ. Чтобы завершить доказательство леммы, нужно нарисовать еще одну точно такую же диаграмму.

$\square$

Определение 6.5. Модуль называется *плоским,* если тензорное умножение на него точно.

Замечание 6.2. Это значит, что любая точная последовательность при тензорном домножении на него остается точной. Достаточно проверять только для коротких.

Лемма о змейке. Пусть дана коммутативная диаграмма, строчки которой — цепные комплексы $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ соответственно, а столбцы, кроме, возможно, первого (на картинке он скорее (-1)-ый), — короткие точные последовательности.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \dots & \\
0 \arrow[r] & \tilde{A} \arrow[r, "\alpha"] \arrow[d, "h"] & A_0 \arrow[r, "\alpha_0"] \arrow[d, "h_0"] & A_1 \arrow[r, "\alpha_1"] \arrow[d, "h_1"] & \dots \arrow[r] & {} \\
0 \arrow[r] & \tilde{B} \arrow[r, "\beta"] \arrow[d, "l"] & B_0 \arrow[r, "\beta_0"] \arrow[d, "l_0"] & B_1 \arrow[r, "\beta_1"] \arrow[d, "l_1"] & \dots \arrow[r] & {} \\
0 \arrow[r] & \tilde{C} \arrow[r, "\gamma"] \arrow[d] & C_0 \arrow[r, "\gamma_0"] \arrow[d] & C_1 \arrow[r, "\gamma_1"] \arrow[d] & \dots \arrow[r] & {} \\
 & 0 & 0 & 0 & \dots &
\end{tikzcd}$$

Тогда существуют такие граничные гомоморфизмы, что длинная последовательность

$$0 \to H_0(\mathcal{A}) \xrightarrow{\hat{h}_0} H_0(\mathcal{B}) \xrightarrow{\hat{l}_0} H_0(\mathcal{C}) \xrightarrow{\hat{\delta}_0} H_1(\mathcal{A}) \xrightarrow{\widehat{h_1}} H_1(\mathcal{B}) \xrightarrow{\hat{l}_1} H_1(\mathcal{C}) \xrightarrow{\hat{\delta}_1} H_2(\mathcal{A}) \to$$

— точна.

Доказательство. Достаточно описать построение всех гомоморфизмов. Точность — упражнение, которое рано или поздно должен сделать каждый. *Хотя и гомоморфизмы проще самому придумать, чем прочитать.*

(1) Построим $\hat{h}_k$. Хотелось бы, чтобы это было просто ограничение h_k. Для этого достаточно проверить, что образ переходит в образ, а ядро — в ядро. Первое (как и второе) очевидно: если у элемента есть прообраз, то в силу коммутативности можно обойти квадратик в другую сторону.

(2) $\hat{l}_k$ получается аналогично ограничением l_k.

(3) Построим $\hat{\delta}_k : H^k(\mathcal{C}) \to H^{k+1}(\mathcal{A})$. Тут нужно пройти по трем самым естественным уже нарисованным стрелочкам. Выберем $c \in Z^k(\mathcal{C})$. Отображение l_k сюръективно из точности, следовательно, существует такое $b \in B_k$, что $l_k(b) = c$. Поскольку строчки — цепные комплексы, то $\gamma_k(c) = 0$. $\beta_k(b) \in B_{k+1}$, поэтому из коммутативности диаграммы и точности столбика следует, что $\beta_k(b) \in \ker(l_{k+1}) = im(h(k+1))$. Кроме того, h_{k+1} — инъективно, поэтому существует и единственное такое $a \in A_{k+1}$, что $h_{k+1}(a) = \beta_k(b)$. Определим $\hat{\delta}_k[c] = [a]$. Мы помним, что была свобода в красных буквах.

Мы почти все сделали. Осталось доказать несколько вещей:

(a) $a \in Z^{k+1}(\mathcal{A})$. Действительно, $\beta_{k+1}(\beta_k(b)) = 0$ по определению комплекса. Тогда из коммутативности $h_{k+2}(\alpha_{k+1}(a)) = 0$, но h_{k+2} инъективно, поэтому $\alpha_{k+1}(a) = 0$.

(b) Класс $[a]$ не зависит от выбора прообраза b. Для этого достаточно доказать, что если $b' \in ker(l_k) = im(h_k)$, то $a' \in im(\alpha_k)$. Действительно, тогда найдется такое a^*, что $h_k(a^*) = b'$. Но тогда $a' = \alpha_k(a^*)$, что и требовалось.

(c) Класс $[a]$ не зависит от выбора представителя . Для этого достаточно показать, что если $c' \in im(\gamma_{k-1})$, то соотетствующий ему прообраз $b^* \in im(\beta_{k-1})$. Действительно, существует такое $c^* \in C_{k-1}$, что $\gamma_{k-1}(c^*)$. В силу точности у c^* существует прообраз $b'' \in B_{k-1}$. Уже по доказанному в пункте **(b)** класс $[a]$ не зависит от выбора прообраза во второй строке, значит, можно считать, что $l_k(b^*) = c'$.

Замечание, которое нужно увидеть перед тем, как посмотреть на диаграмму. Формально она ни в коем случае не коммутативна. Смотреть на нее надо слоями (каждый из которых по-честному коммутативен): **черный слой** — доказательство пункта **(a)** и построение, **зеленый слой** — доказательство **(b)**, **синий слой** — доказательство **(c)**.

$$\begin{tikzcd}
 & a^* \arrow[r, "\alpha_k"] \arrow[d, "h_k"] & a+\alpha_k(a^*) \arrow[r, "\alpha_{k+1}"] \arrow[d, "h_{k+1}"] & \alpha_{k+1}(a) = 0 \arrow[d, "h_{k+2}"] \\
b'' \arrow[r, "\beta_{k-1}"] \arrow[d, "l_{k-1}"] & b^*+b+b' \arrow[r, "\beta_k"] \arrow[d, "l_k"] & \beta_k(b) = h_{k+1}(a) \arrow[r, "\beta_{k+1}"] \arrow[d, "l_{k+1}"] & 0 \\
c^* \arrow[r, "\gamma_{k-1}"] & c'+c = l_k(b) \arrow[r, "\gamma_k"] & 0 &
\end{tikzcd}$$

□

7 Алгебры

Пусть R, S — два кольца, $f : R \to S$ — гомоморфизм, M — S – модуль. Тогда про M можно мыслить как про R – модуль: $(r, m) \mapsto f(r)m$. Это называется *ограничением скаляров.*

Пусть M — R – модуль, *расширением скаляров* называется S – модуль $S \oplus M$: $(s_1, s_2 \oplus m) = s_1 s_2 \oplus m$.

Определение 7.1. *Алгеброй* над коммутативным кольцом с 1 называется такой R– модуль $\mathcal{A}$ с умножением: $A \oplus A \to A$, которое ассоциативно; и единичным элементом $1_{\mathcal{A}}$.

Определение 7.2. Алгебра называется *конечной*, если она конечнопорожденный свободный модуль.

Определение 7.3. Алгебра называется *алгеброй конечного типа*, если $\mathcal{A} \simeq R[x_1, \ldots, x_n]/I$, I — произвольный идеал.

Определение 7.4. Пусть $\mathcal{A}_1, \mathcal{A}_2$ — две $R-$ алгебры. Их тензорное произведение определено естественным образом.

8 Нётеровость

Замечание 8.1. В чуме следующие два утверждения эквивалентны:

(1) любая возрастающая последовательность стабилизируется;

(2) в любом подмножестве есть максимальный элемент.

Определение 8.1. Пусть внутри модуля M дана нестрого возрастающая цепь подмодулей $M_0 \subset M_1 \subset \ldots$. Если любая такая цепь стабилизируется, то такой модуль называется *нётеровым.*

Замечание 8.2. В силу замечания 8.1 модуль называется *нётеровым*, если выполнено любое из эквивалентных условий: **(1)** Любое множество подмодулей имеет максимальный элемент. **(2)** Любая возрастающая цепочка идеалов стабилизируется. **(3)** Любой идеал конечно порожден.

Предложение 8.1. В нётеровом кольце любой идеал содержит некоторую степень своего радикала.

Доказательство. Пусть $I \subset R$ — идеал, $e_1, \ldots, e_n$ — образующие $\sqrt{I}$. Пусть $e_i^{d_i} \in I$. Тогда $(\sqrt{I})^{\sum d_i} \subset I$. □

Следствие 8.1. В нётеровом кольце нильрадикал нильпотентен.

Предложение 8.2. Предположим, последовательность $0 \to M' \to M \to M'' \to 0$ точна. Тогда M нётеров тогда и только тогда, когда M', M'' нётеровы.

Доказательство. Достаточно рассмотреть цепочку в M и её образ и прообраз при гомоморфизмах. Если крайние последовательности стабилизируются, то центральный тоже.

□

Определение 8.2. Кольцо называется *нётеровым*, если оно нётерово как модуль над самим собой.

Следствие 8.2. Конечнопорожденный модуль над нётеровым кольцом сам нётеров.

Доказательство. Напишем точную последовательность

$$0 \to K \to M \to R^n \to 0.$$

Тогда M — нетеров по предложению 8.2. □

Теорема 8.1. Если любой простой идеал конечно порожден, то R — нётерово.

Доказательство. Пусть P — семейство не конечнопорожденных идеалов. По лемме Цорна существует максимальный элемент $I \in P$ (для любой цепочки можем рассмотреть объединение, оно не конечнопорождено, поскольку каждый элемент цепочки не конечнопорожден). I не прост. Значит, существуют такие $a, b \notin I$: $ab \in I$. Идеал $\langle I, a\rangle$ конечнопорожден (больше максимального в P), $(x_i + \omega_i a)$ — его порождающие, $x_i \in I$. Таким образом, $\langle a, x_1, x_2, \dots, x_n\rangle = \langle I, a\rangle$.

Пусть $z \in I$. Тогда $z = \sum b_i x_i + xa$. Значит, $xa \in I$ и $x \in (I : (a)) \supset I + Rb \supset I$. Таким образом, $(I : a) = \langle u_1, \dots, u_m\rangle$. Следовательно, модуль $I = \langle x_1, \dots, x_n, u_1, \dots, u_m\rangle$.

□

Теорема Гильберта о базисе. R — нётерово кольцо, тогда $R[x]$ — тоже.

Доказательство. Пусть I — не конечнопорожденный идеал. Рассмотрим ненулевой многочлен минимальной степени $f_i \in I/I_i$, $I_1 = \{0\}$, $I_k = \langle f_1, \dots, f_{k-1}\rangle$. Посмотрим на старшие коэффициенты этих многочленов. Они содержатся в конечнопорожденном идеале в R. Тогда начиная с какого-то индекса они выражаются через первые k. Таким образом, f_{k+1} многочлен можно уменьшить.

□

9 Артиновость

Определение 9.1. Модуль называется *артиновым*, если в нем любая убывающая цепочка подмодулей стабилизируется.

Замечание 9.1. Для артиновых модулей верен аналог предолжения 8.2.

Предложение 9.1. Любой простой идеал в артиновом кольце максимален.

Доказательство. Пусть $\mathfrak{p} \subset R$ — простой, тогда $A = R/\mathfrak{p}$ — артинова область целостности. Рассмотрим $x \in A$, покажем, что он обратим.

В силу артиновости для некоторого n $(x^n) = (x^{n+1})$. Тогда для некоторого $y \in R$ $x^n = x^{n+1}y$, это и есть обратный элемент.

□

Следствие 9.1. $nil(R) = J(R)$. Более того, этот идеал нильпотентен.

Доказательство. Первое утверждение следует из совпадения максимальных и простых идеалов.

Для доказательства второго утверждения рассмотрим цепочку $(nil(R))^i$, она стабилизируется:

$$\mathfrak{a} = (nil(R))^k = (nil(R))^{k+1} = \dots$$

Рассмотрим множество Σ, состоящее из тех идеалов $\mathfrak{b}$, для которых $\mathfrak{ab} \neq 0$. Оно непусто, потому что сам $\mathfrak{a}$ там лежит. Значит, можно выбрать минимальный элемен, он обязательно имеет вид $(x) \subset R$. Поскольку

$$(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0,$$

то $(x\mathfrak{a}) = (x)$(в силу минимальности). Следовательно, для некоторого $a \in \mathfrak{a}$ выполнено $x = ax$. Тогда

$$x = ax = a^2x = a^3x = \dots = 0.$$

$\square$

Предложение 9.2. Максимальных идеалов в артиновом кольце конечно.

Доказательство. Рассмотрим множество всевозможных конечных пересечений максимальных идеалов, там есть минимум $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_k$. Тогда для любого максимального идеала $\mathfrak{m}$ выполнено

$$\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_k \subset \mathfrak{m}.$$

По предложению 3.1 $\mathfrak{m} = \mathfrak{m}_\mathfrak{j}$ для некоторого j. $\square$

10 Длина модуля

Определение 10.1. Модуль называется *простым*, если он не имеет собственных подмодулей.

Определение 10.2. *Композиционным рядом* модуля M называется конечная последовательность подмодулей $0 = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_{n-1} \subsetneq M_n = M$, где M_i/M_{i-1} — простой модуль.

Определение 10.3. *Длиной* модуля $\ell(M)$, имеющего композиционный ряд, называется минимальная из длин композиционных рядов n.

Лемма 10.1. Если модуль M представим в виде композиционного ряда, то любой его собственный подмодуль N имеет меньшую длину:

$$\ell(N) < \ell(M).$$

Доказательство. Пусть $N_i = M_i \cap N$.

$$N_i/N_{i-1} = (M_i \cap N)/(M_{i-1} \cap N) \subset M_i/M_{i-1}.$$

В силу простоты длина N_i/N_{i-1} не превосходит 1. Предположим, $N_i/N_{i-1} = M_i/M_{i-1}$ при всех i. Тогда $N = M$, противоречие.

□

Теорема 10.1. Если M представимо в виде композиционного ряда длины n, то любой композиционный ряд имеет длину n. В таком случае $n = \ell(M)$ — *длина модуля.*

Доказательство. Докажем индукцией по длине $\ell(M)$, что $\ell(M) \geqslant k$, где $N_0 \subset \ldots \subset N_k$ — какая-то другая композиционная серия. Для N_{k-1} выполнено предположение индукции. Кроме того, по лемме $\ell(N_{k-1}) \leqslant \ell(M) - 1$. Таким образом заключаем, что $\ell(M) - 1 \leqslant k - 1$. □

Теорема 10.2. M — модуль конечной длины тогда и только тогда, когда он нётеров и артинов.

Доказательство. Если модуль имеет конечную длину, то у всех его подмодулей длина меньше, они артиновы и нётеровы по предположению индукции. Тогда сам модуль тоже артинов и нётеров.

Предположим, модуль M артинов и нётеров, построим явно для него композиционную серию. Пусть $M_0 = 0$, определим M_i как минимальное содержащее M_{i-1} (существует по артиновости). Эта цепочка законится в силу нётеровости □

Определение 10.4. Простой идеал $\mathfrak{p} \subset R$ называется *ассоциированным простым* модуля M, если для некоторого $m \in M$

$$\mathfrak{p} = Ann(m) := \left\{x \in R \,\middle|\, xm = 0\right\}.$$

Обозначение 10.1. Множество ассоциированных простых обозначается $Ass(M)$.

Лемма 10.2. Если $Ann(m) = \mathfrak{p}$, то $Ann(xm) = \mathfrak{p}$ в случае, когда $x \notin \mathfrak{p}$, и $Ann(xm) = R$ в случае, когда $x \in R$.

Доказательство. Если $x \notin \mathfrak{p}$ и $xym = 0$. Из то из того, что $xy \in \mathfrak{p}$, в силу простоты следует, что $y \in \mathfrak{p}$.

Если $x \in \mathfrak{p}$, то $xm = 0$. □

Лемма 10.3. Для нётерового модуля не существует бесконечно убывающей по включению цепочки ассоциированных простых.

Доказательство. Пусть нашлась такая цепочка $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots$ и $Ann(m_i) = \mathfrak{p}_i$. В силу нётеровости цепочка подмодулей $M_i = (m_1, \ldots, m_i)$ стабилизируется. Тогда для некоторого k

$$m_{k+1} = a_1 m_1 + \ldots + a_k m_k.$$

Домножим это равенство на некоторый $x \in \mathfrak{p}_k \backslash \mathfrak{p}_{k+1}$, справа получился ноль, а слева — не ноль. Противоречие. □

Лемма 10.4. Пусть $\mathfrak{m}_0 \cdot \ldots \cdot \mathfrak{m}_k = 0$ — произведение максимальных идеалов в R. Тогда нётеровость этого кольца равносильна его артиновости.

Доказательство. Рассмотрим $V_i = \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_i / \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_{i-1}$ — векторные пространства над $R/\mathfrak{m}_i$. Для векторных пространств артиновость и нетеровость равносильны, а в силу предложения 8.2 и замечания 9.1 получаем требуемое.

□

Точность длины. Пусть $N \subset M$ — подмодуль модуля конечной длины M. Тогда

$$\ell(N) + \ell(M/N) = \ell(M).$$

Доказательство. Заметим, что N — тоже артинов и нётеров, следовательно по теореме 10.2 имеет конечную длину. Кроме того, в силу нётеровости и артиновости любую цепочку можно продолжить до композиционного ряда. Продолжим композиционный ряд для N до композиционного ряда для M. □

11 Локализация колец.

Определение 11.1. Назовем элементы $(r_1, s_1), (r_2, s_2) \in R \times S$, где S — мультипликативное подмножество R, *эквивалентными*, если существует такое $u \in S$, что $r_1 s_2 u = r_2 s_1 u$.

Замечание 11.1. Это честное отношение эквивалентности, не очевидна только транзитивность. Пусть еще есть пара (r_3, s_3) и $r_2 s_3 v = r_3 s_2 v$. Тогда $r_1 s_3 s_2 u v = r_2 s_1 u s_3 v = r_3 s_2 s_1 u$.

Определение 11.2. Кольцо $S^{-1}R$ определим как множество классов эквивалентности. Умножение и сложение там хорошо определены. Это называется *локализацией.*

Замечание 11.2. Это корректное определение, которое удовлетворяет аксиомам. Достаточно проверить независимость от выбора представителей.

Пусть $\varphi_S : R \to S^{-1}R$ — такое отображение колец, что $\varphi_S(x) = \dfrac{x}{1}$. Это отображение отправляет S в обратимые элементы.

Определение 11.3. Пусть S_0 — подмножество R, элементы которого — это в точности не делители нуля. *Полным кольцом частных* $S_0^{-1}R$ называется локализация по этому множеству.

В этом случае отображение φ_{S_0} — инъективно, поскольку если $\varphi_{S_0}(x) = 0$, то существует такой $s \in S_0$, что $xs = 0$, но s — не делитель нуля, значит, $x = 0$. Таким образом, если R — область целостности, то можно рассматривать R как подкольцо $S^{-1}R$.

Если $S \subset S_0$ — мультипликативное, то $R \subset S^{-1}R \subset S_0^{-1}R$, где первое включение осуществляется вложением φ_S, а второе — честное включение множеств *(оно верно в данном случае, но вообще для любых двух мультипликативных вложенных множеств — не всегда)*.

В случае, когда R — область целостности, $S_0 = R\backslash\{0\}$, а $S_0^{-1}R = Frac(R)$ — поле частных.

Универсальное свойство. Пусть R — кольцо, S — мультипликативное подмножество, $\psi : R \to R'$ — отображение колец, тогда $\psi(S) \subset R'^{\times}$ тогда и только тогда, когда существует такое ρ, что диаграмма коммутативна (то есть $\rho \circ \varphi_S = \psi$).

$$\begin{tikzcd} R \arrow[r, "\varphi_S"] \arrow[dr, "\psi"'] & S^{-1}R \arrow[d, "\rho"] \\ & R' \end{tikzcd}$$

В этом случае ρ — единственно, $\ker(\rho) = \ker(\psi)S^{-1}R$.

Доказательство. Предположим, что такое ρ существует, $s \in S$. Тогда $\psi(s) = \rho\left(\dfrac{s}{1}\right)$. Но $\dfrac{s}{1}$ — обратимо, значит $\psi(s)$ — тоже. Таким образом, $\psi(S) \subset R'^{\times}$.

Пусть теперь выполнено второе: $\psi(S) \subset R'^{\times}$. Поскольку $\psi_S(x) = \dfrac{x}{1}$, то если ρ существует, то $\rho\left(\dfrac{x}{1}\right) = \psi(x)$ из коммутативности диаграммы. Кроме того, $\rho(1) = \rho\left(\dfrac{s}{1}\right) \cdot \rho\left(\dfrac{1}{s}\right) = 1$, то есть $\rho\left(\dfrac{1}{s}\right) = \psi^{-1}(s)$. Таким образом, если ρ существует, то он определен так $\rho\left(\dfrac{x}{s}\right) = \dfrac{\psi(x)}{\psi(s)}$. Это определение корректно в силу предположения: пусть $(x,s) \sim (y,t)$ (то есть существует такое $u \in S$, что $xtu = ysu$). Тогда $\psi(xtu) = \psi(ysu)$, значит, $\psi(xt) = \psi(ys)$ (поскольку $\psi(u)$ — обратим). Таким образом, $\rho\left(\dfrac{x}{s}\right) = \dfrac{\psi(s)}{\psi(s)} = \dfrac{\psi(y)}{\psi(t)} = \rho\left(\dfrac{y}{t}\right)$.

Осталось доказать, что $\ker(\rho) = \ker(\psi)S^{-1}R$. А это очевидно из формулы для ρ.

$\square$

Следствие 11.1. ψ_S — изоморфизм тогда и только тогда, когда S состоит из единиц (обратимых элементов).

Доказательство. Предположим, ψ_S — изоморфизм. Как мы знаем, $\psi_S(S)$ состоит из обратимых элементов. Тогда и S — тоже.

Теперь пусть S состоит из обратимых элеменов. Применим тогда универсальное свойство для $R' = R$ и $\psi = id_R$. Нужное ρ существует и инъективно (потому что $\ker(\rho) = \ker(\psi)S^{-1}R = 0$), тогда ψ_S — сюрьективно, но оно же и инъективно, поскольку в S нет делителей нуля.

$\square$

Задача 11.1. Пусть R' и R'' — кольца. Определим $R = R' \times R''$ и $S = \{(1,1),(1,0)\}$. Докажите, что $R' = S^{-1}R$.

Доказательство. Нетрудно проверить, что $\dfrac{(x,y)}{(1,1)} \sim \dfrac{(x,z)}{(1,0)}$ при всех $x, y, z \in R'$. Таким образом, эквивалентны те и только те элементы $\dfrac{(x,y)}{s}$, у которых одинаковая первая координата числителя. То есть получается биекция с R', которая является изоморфизмом, потому что локализация обладает структурой кольца.

$\square$

Определение 11.4. Пусть R — кольцо, $f \in R$. Положим $S_f = \left\{f^n \;\middle|\; n \geqslant 0\right\}$, это мультипликативное множество. Назовем кольцо $S_f^{-1}R = R_f$ — локализацией R по f. Обозначим $\psi_{S_f} = \psi_f$.

Предложение 11.1. $R_f = R[x]/\left\langle 1 - fx\right\rangle$.

Доказательство. Пусть $R' = R[x]/\left\langle 1 - fx\right\rangle$, $\psi : R \to R'$ — каноническое вложение. Проверим, что универсальное свойство применимо. Действительно, пусть $\psi(f)x - 1 = 0$, то есть $\psi(f) \in R'^{\times}$. Тогда существует и единственно $\rho : R_f \to R'$, покажем, что ρ — изоморфизм.

Проверим инъективность. Это очевидно, поскольку $\ker\psi = 0$.

Проверим сюрьективность. Очевидно, что $\rho(f) = x$ (по определению ρ в доказательстве универсального свойства), то есть любой многочлен можно получить.

$\square$

Предложение 11.2. Пусть $\mathfrak{a} \subset R$ — идеал. Тогда

(1) $\mathfrak{a}S^{-1}R = \left\{(a,s) \in R \times S \;\middle|\; a \in \mathfrak{a}, s \in S\right\}$;

(2) $\mathfrak{a} \cap S \neq \varnothing$ равносильно $\mathfrak{a}S^{-1}R = S^{-1}R$ равносильно $\psi_S^{-1}(\mathfrak{a}S^{-1}R) = R$.

Доказательство. **(1)** Это очевидно.

(2) Пусть $a \in \mathfrak{a} \cap S$. Тогда $\dfrac{x}{s} = \dfrac{ax}{as} \in \mathfrak{a}S^{-1}R$ и из первого следует второе. Из второго третье чледует очевидно, потому что у любого x прообраз в $S^{-1}R = \mathfrak{a}S^{-1}R$. Покажем, что из третьего следует первое. Действительно, $\dfrac{1}{1} \in \mathfrak{a}S^{-1}R$. Это значит, что для некоторого $a \in \mathfrak{a}$, $s \in S$ существует такое $u \in S$, что $au = su$. Этот элемент принадлежит одновременно $\mathfrak{a}$ и S.

$\square$

Определение 11.5. Пусть R — кольцо, S — мультипликативное подмножество, $\mathfrak{a} \subset R$ — какое-то подмножество. *Насыщением* $\mathfrak{a}$ относительно S называется множество

$$\mathfrak{a}^S = \big\{a \in R \;\big|\; \text{существует такое } s \in S, \text{ что } as \in \mathfrak{a}\big\}.$$

В случае, когда $\mathfrak{a}^S = \mathfrak{a}$, множество $\mathfrak{a}$ называется *насыщенным.*

Предложение 11.3. (1) $\ker(\varphi_S) = \langle 0 \rangle^S$.

(2) $\mathfrak{a} \subset \mathfrak{a}^S$.

(3) В случае, когда $\mathfrak{a}$ — идеал, $\mathfrak{a}^S$ — тоже идеал.

Доказательство. **(1)** Нетрудно заметить, что $x \in \ker(\varphi_S)$ тогда и только тогда, когда $xs = 0$ для некотрого $s \in S$, а это равносильно равенству.

(2) Это так, просто потому что $1 \in S$.

(3) Чтобы доказать, что $\mathfrak{a}^S$ — идеал, нужно показать, что это множество замкнуто относительно сложения и относительно умножения на что угодно. Пусть $a, b \in \mathfrak{a}^S$, то есть для некоторых $s, t \in S$ выполнено $as, bt \in \mathfrak{a}$. Но тогда $ast, bst \in \mathfrak{a}$, значит, $(a + b)st \in \mathfrak{a}$, следовательно, $(a + b) \in \mathfrak{a}^S$. А про умножение совсем очевидно.

$\square$

Предложение 11.4. Пусть R — кольцо, S — мультипликативное подмножество.

(1) Предположим, $\mathfrak{b}$ — идеал в $S^{-1}R$. Тогда $\varphi_S^{-1}(\mathfrak{b})$ — насыщенный идеал и $\mathfrak{b} = (\varphi_S^{-1}(\mathfrak{b}))S^{-1}R$.

(2) Пусть $\mathfrak{a}$ — идеал в R. Тогда $\mathfrak{a}S^{-1}R = \mathfrak{a}^S S^{-1}R$ и $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = \mathfrak{a}^S$.

(3) Пусть $\mathfrak{p}$ — простой идеал в R и $\mathfrak{p} \cap S = \varnothing$. Тогда $\mathfrak{p}^S = \mathfrak{p}$ и $\mathfrak{p}S^{-1}R$ — простой идеал в $S^{-1}R$.

Доказательство. **(1)** Очевидно, что $\varphi_S^{-1}(\mathfrak{b})$ — идеал. Докажем, что он насыщенный. Пусть $x \in (\varphi_S^{-1})^S$, тогда для некоторого $s \in S$ выполнено $xs \in \varphi_S^{-1}$. Это значит, что $\dfrac{xs}{1} \in \mathfrak{b}$. Но тогда $\dfrac{xs}{1} \cdot \dfrac{1}{s} = \dfrac{x}{1} \in \mathfrak{b}$. Что и требовалось. Аналогично доказывается и второе утверждение: $\frac{x}{s} \in \mathfrak{b}$ тогда и только тогда, когда $\frac{x}{1} \in \mathfrak{b}$, а это равносильно тому, что прообраз состоит из всех числителей $\mathfrak{b}$.

(2) Для доказательства первого утверждения достаточно проверить включение
$\mathfrak{a}^S S^{-1}R \subset \mathfrak{a}S^{-1}R$. Пусть $a \in \mathfrak{a}^S$. Тогда для некоторого $s \in S$ выполнено $as \in \mathfrak{a}$. Нужно доказать, что $\frac{a}{u} \in \mathfrak{a}S^{-1}R$ для любого $u \in S$. Ну а это так, потому что $\frac{as}{us} \in \mathfrak{a}S^{-1}R$. Докажем второе: прообраз — насыщенный идеал, содержащий $\mathfrak{a}$, то есть как минимум $\mathfrak{a}^S$. А больше ничего нет, потому что если $\frac{x}{1} = \frac{a}{s} \in \mathfrak{a}S^{-1}R$ (тут $a \in \mathfrak{a}$), то $xsu = au$ для некоторого $u \in S$, это значит, что $x \in \mathfrak{a}^S$.

(3) Пусть $x \in \mathfrak{p}^S$. Тогда для некоторого $s \in S$ верно, что $xs \in \mathfrak{p}$. По условию $\mathfrak{p}$ — простой и $s \notin \mathfrak{p}$, значит, $x \in \mathfrak{p}$. Далее, по одному из предыдущих замечаний, все числители $\mathfrak{p}S^{-1}R$ принадлежат $\mathfrak{p}$, то есть если перемножить две дроби с числителями не из $\mathfrak{p}$, то получится число не из $\mathfrak{p}S^{-1}R$, что и требовалось.

$\square$

Следствие 11.2. Насыщенные идеалы в R находятся в биекции с идеалами в $S^{-1}R$, причем простые — с простыми.

Определение 11.6. Пусть $\mathfrak{p}$ — простой, тогда $S_\mathfrak{p} = R \backslash \mathfrak{p}$ — мультипликативное и $S_\mathfrak{p}^{-1}R = R_\mathfrak{p}$ называется *локализацией* R по $\mathfrak{p}$.

Предложение 11.5. $R_\mathfrak{p}$ — локально с максимальным идеалом $\mathfrak{p}R_\mathfrak{p}$.

Доказательство. Это уже почти очевидно. Биекция между идеалами в R и $R_\mathfrak{p}$ сохраняет включения, и мы хотим, чтобы идеал в R не пересекался с $S_\mathfrak{p}$, то есть он должен целиком лежать в $\mathfrak{p}$. Но максимальный среди таких идеалов это и есть $\mathfrak{p}$.

$\square$

12 Локализация модулей.

Тут во многом все то же самое.

Пусть есть гомоморфизм модулей $\alpha : M \to N$. Он индуцирует гомоморфизм локализаций $S^{-1}\alpha : S^{-1}M \to S^{-1}N$, который действует по правилу

$$S^{-1}\alpha\left(\frac{m}{s}\right) = \frac{\alpha(m)}{s}.$$

Замечание 12.1. Заданный таким образом гомоморфизм локализаций корректно действует на классах эквивалентности.

Точность локализации. Пусть $0 \to M'' \xrightarrow{\alpha} M \xrightarrow{\beta} M' \to 0$ точна, тогда $0 \to S^{-1}M'' \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}M' \to 0$ — тоже.

Доказательство. Нужно проверить точность в каждом из трех средних членах.

- Локализация сохраняет инъективность. Предположим, $S^{-1}\alpha\left(\frac{m''}{s}\right) = 0$. Это означает, что существует такой $u \in S$, что $0 = \alpha(m'')u = \alpha(m''u)$, но тогда $\frac{m''}{s} = 0$ из инъективности α.

- Точность в среднем члене. Рассмотрим произвольный элемент $\frac{\alpha(m'')}{s} \in \operatorname{im}(S^{-1}\alpha)$, посмотрим на его браз при $S^{-1}\beta$:

$$S^{-1}\beta\left(\frac{\alpha(m'')}{s}\right) = \frac{\beta(\alpha(m''))}{s} = 0.$$

  Таким образом, $\operatorname{im}(S^{-1}\alpha) \subset \ker(S^{-1}\beta)$.

  Рассмотрим произвольный элемент $\frac{m}{s} \in \ker(S^{-1}\beta)$, для него существует такой $u \in S$, что $mu \in \ker\beta$. Тогда найдется $m'' \in M''$, для которого $\alpha(m'') = mu$. Рассмотрим $\frac{m''}{su} \in S^{-1}M''$:

$$S^{-1}\alpha\left(\frac{m''}{su}\right) = \frac{mu}{su} = \frac{m}{s},$$

  откуда следует, что $\operatorname{im}(S^{-1}\alpha) \supset \ker(S^{-1}\beta)$.

- Локализация сохраняет сюръективность. Это видно из определения отображения $S^{-1}R$

$\square$

Предложение 12.1. Пусть $S \subset R$ — мультипликативное подмножество тогда

$$S^{-1}R \otimes_R M \simeq S^{-1}M.$$

Доказательство. Построим изоморфизм явно на образующих:

$$\frac{x}{s} \otimes m \mapsto \frac{mx}{s}.$$

Это отображение корректно определено на классах эквивалентности и действительно изоморфизм.

$\square$

Определение 12.1. Алгебра $\mathcal{A}$ называется *плоской*, если она плоская как R-модуль.

Следствие 12.1. $S^{-1}R$ — плоская алгебра.

13 Носитель модуля

Определение 13.1. *Спектром кольца* R называется

$$Spec(R) = \{\mathfrak{p} \subset R \mid \mathfrak{p} - \text{ простой идеал}\};$$

$$Specm(R) = \{\mathfrak{m} \subset R \mid \mathfrak{m} - \text{ максимальный идеал}\}.$$

Определение 13.2. *Многообразием* идеала $I \subset R$ называется

$$V(I) = \{\mathfrak{p} \mid I \subset \mathfrak{p} \in Spec(R)\}.$$

Замечание 13.1. Очевидно, что если $I \subset J$, то $V(I) \supset V(J)$.

Обратно, если $V(I) \supset V(J)$, то каждый идеал, содержащий J, содержит и I. Как мы помним, $\sqrt{J} = \bigcap\limits_{\mathfrak{p} \supset J} \mathfrak{p}$, таким образом, $\sqrt{J} \supset I$.

В случае, когда $V(I) = V(J)$ аналогичным образом получается $\sqrt{I} = \sqrt{J}$.

Определение 13.3. *Топологией Зарисского* на $Spec(R)$ называется такая топология, где замкнутые множества суть $V(I)$.

Пуст дан элемент $f \in R$. Тогда открытые множество

$$D_f = D(f) = Spec(R) - V(\langle f \rangle)$$

называется *главным открытым множеством.*

Такие множества образуют базу в топологии Зарисского.

Пусть есть отображение колец $\varphi : R \to R'$. Оно индуцирует отображение множеств $\varphi^* : Spec(R') \to Spec(R)$ (поскольку прообраз простого идеала прост).

Определение 13.4. Пусть M — $R-$модуль. Его *носитель* это множество

$$Supp(M) = \{\mathfrak{p} \in Spec(R) \mid M_{\mathfrak{p}} \neq 0\}.$$

Замечание 13.2. Если $Ann(M) \cap (R - \mathfrak{p}) \neq \varnothing$, то уж точно $M_{\mathfrak{p}} = 0$, следовательно $Supp(M) \subset V(Ann(M))$, а в случае, когда модуль конечнопорожден, достигается равенство.

Предложение 13.1. (1) Если последовательность $0 \to L \to M \to N \to 0$ точна, то $Supp(M) = Supp(L) \cup Supp(N)$.

(2) Пусть M_λ — подмодули M, причем $\sum M_\lambda = M$. Тогда $Supp(M) = \bigcup Supp(M_\lambda)$.

(3) $rad(M)$ содержится в пересечении всех максимальных идеалов в $Supp(M)$, Равенство достигается, когда модуль конечно порожден.

Доказательство. **(1)** Поскольку локализация сохраняет точность, $M_{\mathfrak{p}} \neq 0$ не может стоять в последовательности между двумя нулями. Следовательно, $Supp(M) \subset Supp(L) \cup Supp(N)$.

Обратно, если средний член точной последовательности нулевой, то два крайних тоже обязаны быть нулями.

(2) Если локализация по $\mathfrak{p}$ не зануляет хотя бы один M_λ, то не зануляет и их сумму. Обратно, предположим, локализация по $\mathfrak{p}$ зануляет все M_λ. По третьему пункту доказательства, при локализации сюръективное отображение $\oplus M_\lambda \to M$ переходит в сюръективное $0 = (M_\lambda)_\mathfrak{p} \to M_\mathfrak{p}$.

(3) По определению $rad(M)$ состоит из максимальных идеалов, которые содержат $Ann(M)$, в силу замечания 13.2 получаем требуемое.

□

Предложение 13.2. Пусть M — R−модуль, тогда следующие условия эквивалентны:

(1) $M = 0$;

(2) $M_\mathfrak{p} = 0$ для любого $\mathfrak{p} \in Spec(R)$;

(3) $M_\mathfrak{m} = 0$ для любого $\mathfrak{m} \in Specm(R)$.

Доказательство. Очевидно, что $(1) \Rightarrow (2), (2) \Rightarrow (3)$.

Докажем $(3) \Rightarrow (1)$. Известно, что для любого максимального идеала $Ann(M) \cap (R - \mathfrak{m})$ непусто. Тогда $Ann(M) = R$ (иначе он сам содержится в некотором максимальном идеале и предположение неверно). Тогда $M = 0$.

□

Следствие 13.1. $M = 0$ тогда и только тогда, когда $Supp(M) = \varnothing$.

Замечание 13.3. Пусть $\mathcal{A}$ — плоская алгебра, N — плоский модуль. Тогда $N \otimes \mathcal{A}$ — плоский $\mathcal{A}$ – модуль.

Предложение 13.3. Следующие условия эквивалентны:

(1) M плоский;

(2) $M_\mathfrak{p}$ плоский для любого $\mathfrak{p} \in Spec(R)$;

(3) $M_\mathfrak{m}$ плоский для любого $\mathfrak{m} \in Specm(R)$.

Доказательство. $(1) \Rightarrow (2)$ Это верно в силу предложения 12.1 и замечания 13.3.

$(2) \Rightarrow (3)$ Очевидно.

$(3) \Rightarrow (1)$ А вот тут нужно что-то написать. □

14 Еще про ассоциированные простые

Предложение 14.1. Если $\mathfrak{p} \in Spec(R)$, то $\mathfrak{p} \in Ass(M)$ тогда и только тогда, когда существует инъективное $R/\mathfrak{p} \hookrightarrow M$.

Доказательство. Пусть $\mathfrak{p} = Ann(m)$, тогда зададим искомую инъекцию явно:

$$[x] \mapsto mx,$$

это определение корректно (то есть не зависит от выбора представителя класса эквивалентности).

Обратно, пусть существует инъекция $\varphi : R/\mathfrak{p} \hookrightarrow M$. Положим $\varphi(1) = m$. Тогда $Ann(m) = \mathfrak{p}$.

$\square$

Лемма 14.1. Пусть $[x] \in R/\mathfrak{p}$ — ненулевой. Тогда $Ann([x]) = \mathfrak{p}$ и $Ass(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

Доказательство. Заметим, что $[x][y] = 0$ тогда и только тогда, когда $xy \in \mathfrak{p}$. По условию $x \notin \mathfrak{p}$, следовательно, это бывает только если $y \in \mathfrak{p}$. $\square$

Предложение 14.2. Пусть $N \subset M$ — подмодуль. Тогда

$$Ass(N) \subset Ass(M) \subset Ass(N) \cup Ass(M/N).$$

Доказательство. Первое включение верно просто по определению.

Пусть $Ann(m) = \mathfrak{p}$, в силу предложения 14.1 существует инъекция $\varphi : R/\mathfrak{p} \hookrightarrow M$. Если $\varphi(R/\mathfrak{p}) \cap N = 0$, то при факторизации φ перейдет в инъекцию $R/\mathfrak{p} \hookrightarrow M/N$, следовательно, по предложению 14.1 $\mathfrak{p} \in Ass(M/N)$.

Иначе рассмотрим ненулевой $\varphi(x) \in N$. Тогда по лемме 14.1 $Ann(x) = Ann(\varphi(x)) = \mathfrak{p}$. $\square$

Предложение 14.3. Пусть $\Psi \subset Ass(M)$. Тогда существует такой подмодуль $N \subset M$, что $Ass(M/N) = \Psi$ и $Ass(N) = Ass(M) - \Psi$.

Доказательство. По лемме Цорна выберем такое максимальное $N \subset M$, что $Ass(N) \subset Ass(M) - \Psi$. Тогда по предложению 14.2 выполнено $Ass(M/N) \supset \Psi$.

Пусть $\mathfrak{p} \in Ass(M/N)$. Из предложения 14.1 следует, что некоторый подмодуль N'/N изоморфен $R/\mathfrak{p}$. По предложению 14.2 $Ass(N') \subset Ass(N) \cup \{\mathfrak{p}\}$. Поскольку N максимально, $\mathfrak{p} \notin Ass(M) - \Psi$. Тогда $\mathfrak{p} \in \Psi$ и $Ass(M/N) = \Psi$.

$\square$

Предложение 14.4. Пусть S — мультипликативное подмножество. Если $\mathfrak{p} \cap S = \varnothing$ и $\mathfrak{p} \in Ass(M)$, то $S^{-1}\mathfrak{p} \in Ass(S^{-1}M)$.

Доказательство. Заметим, что $S^{-1}\mathfrak{p}$ — простой по предложению 11.4. Если $\mathfrak{p} = Ann(m)$, то $S^{-1}\mathfrak{p} = Ann\left(\frac{m}{s}\right)$ в силу того, что $\mathfrak{p} \cap S = \varnothing$.

$\square$

Лемма 14.2. Пусть $\mathfrak{p}$ — максимальный элемент в множестве аннуляторов ненулевых $m \in M$. Тогда $\mathfrak{p} \in Ass(M)$.

Доказательство. Предположим, что $\mathfrak{p} = Ann(m)$ не является простым. Тогда наудутся два таких $x, y \in R$, что $xy \in \mathfrak{p}$, но $x, y \notin \mathfrak{p}$. Тогда $mx \neq 0$ и $y \in Ann(mx)$. Но $\mathfrak{p} \subset Ann(mx)$, следовательно, $(\mathfrak{p}, y) \subset Ann(mx)$, противоречие с максимальностью. □

Следствие 14.1. Пусть R или M нётеров. Тогда $M = 0$ тогда и только тогда, когда $Ass(M) = \varnothing$.

Доказательство. В одну сторону утверждение очевидно, докажем во вторую. Понятно, что мы хотим воспользоваться леммой 14.2, то есть доказать, что во множестве аннуляторов есть максимальный элемент.

Пусть R — нётерово. Тогда в любом множестве идеалов есть максимальный элемент по лемме Цорна.

Пусть M — нётеров. Посмотрим на лемму 10.3, на самом деле мы там нигде не пользовались простотой, то есть не существует строго возрастающей цепочки аннуляторов и опять все верно по лемме Цорна. □

Предложение 14.5. Пусть M — нётеров модуль. Тогда можно построить цепочку

$$0 = M_0 \subset \ldots \subset M_n = M$$

так, чтобы $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ ($\mathfrak{p}_i$ — простой) и для любой такой цепочки $Ass(M) \subset \{\mathfrak{p}_i\}_i \subset Supp(M)$, кроме того, множества минимальных простых $Ass(M)$ и $Supp(M)$ совпадают, а $Ass(M)$ — конечно.

Доказательство. Предположим, что это утверждение не верно для модуля M, рассмотрим его максимальный подмодуль N, для которого оно выполнено ($M/N \neq 0$). По следствию 14.1 найдется такой подмодуль M', что $Ass(N'/N) = \mathfrak{p}$, противоречие с максимальностью.

Первое включение верно по индукции. Заметим, что в силу замечания 13.2 простой идеал $\mathfrak{p}_i$ принадлежит $Supp(M)$, если содержит его аннулятор, таким образом второе включение тоже верно.

Рассмотрим произвольный минимальный простой $\mathfrak{p} \in Supp(M)$. Кольцо $R_\mathfrak{p}$ локально и других простых там нет в силу минимальности. Таким образом (поскольку $M_\mathfrak{p} \neq 0$) по следствию 14.1 $Ass(M_\mathfrak{p}) = \mathfrak{p}R_\mathfrak{p}$. Тогда $\mathfrak{p} \in Ass(M)$. □

Теорема Акизуки – Хопкинса. Пусть M — конечнопорожденный R – модуль. Следующие условия эквивалентны:

(1) R нетерово и любой простой идеал макисмален;

(2) R артиново.

Доказательство. (1) $\Rightarrow$ (2) Поскольку простые идеалы совпадают с максимальными, в силу нётеровости $nil(R) = \bigcap\limits_{\mathfrak{m} \in Specm(R)} \mathfrak{m}$ — нильпотентен, тогда по предложению 14.5 получился композиционный ряд, то есть R имеет конечную длину и является артиновым (по теореме 10.2).

(2) $\Rightarrow$ (1) В силу следствия 9.1 выполнено условие леммы 10.4(нужно возвести нильрадикал в нужную степень и именно столько раз продублировать максимальные идеалы, которых конечно по предложению 9.2), то есть кольцо нётерово, а все простые максимальны по предложению 9.1.

$\square$

Предложение 14.6. Пусть M — конечнопорожденный модуль над артиновым кольцом. Тогда M имеет конечную длину.

Доказательство. По теореме Акизуки – Хопкинса это кольцо нётерово, а любой простой максимален, тогда по предложению 14.5 получается композиционный ряд. $\square$

Определение 14.1. Число $x \in R$ называется *делителем нуля для* M, если существует такое ненулевое $m \in M$, что $xm = 0$ (ну или отображение не регулярно).

Обозначение 14.1. Множество всех делитель нуля для M обозначается

$$ZD(M) = \{x \in R \mid x - \text{ делитель нуля}\}.$$

Предложение 14.7. Если R или M нётеров, то

$$ZD(M) = \bigcup_{\mathfrak{p} \in Ass(M)} \mathfrak{p}.$$

Доказательство. Если $x \in ZD(M)$, то существует такой $m \in M$, что $x \in Ann(m)$. Тогда в обоих случаях существует максимальный среди аннуляторов элемент, содержащий $Ann(m)$, который лежит в $Ass(M)$ по лемме 14.2.

$\square$

Определение 14.2. Число $x \in R$ называется M *– регулярным,* если отображение

$$\mu_x : M \to M,$$

$$\mu_x : m \mapsto mx - \text{ инъективно.}$$

15 Примарное разложение

Соглашение. Все кольца нётеровы, все модули конечно порождены.

Определение 15.1. Подмодуль $N \subset M$ называется $\mathfrak{p}$ – *примарным*, если $Ass(M/N) = \{\mathfrak{p}\}$.

Предложение 15.1. Пусть $N_1, N_2 \subset M$ — $\mathfrak{p}$ – примарные подмодули, тогда $N_1 \cap N_2$ — тоже $\mathfrak{p}$ – примарный.

Доказательство. Заметим, что $N_1 \cap N_2 = \ker(M \to M/N_1 \oplus M/N_2)$, тогда

$$M/(N_1 \cap N_2) \hookrightarrow M/N_1 \oplus M/N_2.$$

Следовательно,

$$Ass(M/(N_1 \cap N_2)) \subset Ass(M/N_1 \oplus M/N_2) = \{\mathfrak{p}\}.$$

По следствию 14.1 $Ass(M/(N_1 \cap N_2)) = \{\mathfrak{p}\}$. □

Определение 15.2. Подмодуль $\mathfrak{N} \subset M$ называется *разложимым*, если он нетривиально представляется в виде пересечения подмодулей: $N = N_1 \cap N_2$. В противном случае подмодуль называется *неравзложимым.*

Предложение 15.2. Любой подмодуль $N \subset M$. Он представляется в виде конечного пересечения неразложимых.

Доказательство. Пусть $\mathcal{F}$ — множество подмодулей, которые не имеют такого представления. В случае, когда $\mathcal{F} \neq \varnothing$, в $\mathcal{F}$ существует масимальный элемент N_0, он обязательно разложим: $N_0 = N_1 \cap N_2$. Модули N_1 и N_2 содержат максимальный элемент $\mathcal{F}$, а это значит, что сами они там не лежат. То есть для них искомые представления существуют, тогда такое представление существует и для N_0, противоречие. □

Тут нужно что-то дописать

16 Расширения колец

Определение 16.1. Пусть S — R – алгебра (обозначение S/R), $x \in S$ называется *целым над* R, если является корнем некоторого многочлена

$$x^n + a_1 x^{n-1} \ldots + a_n = 0, a_i \in R.$$

Предложение 16.1. Следующие условия эквивалентны:

(1) x — целый над R степени n;

(2) $R[x]$ порожден $1, x, \ldots, x^{n-1}$;

(3) x лежит в некоторой подалгебре R', порожденной как R – модуль n элементами.

(4) Существует *точный* $R[x]$ – модуль M ($Ann(M) = 0$), порожденный n элементами.

Доказательство. (1) $\Rightarrow$ (2) любой одночлен x^k, где $k \geqslant n$ представляется как комбинация меньших.

(2) $\Rightarrow$ (3) Достаточно положить $R' = R[x]$.

(3) $\Rightarrow$ (4) Достаточно положить $M = R'$.

(4) $\Rightarrow$ (1) Пусть $m_1, \ldots, m_n$ — порождающие. Запишем матрицу A отображения $m \mapsto mx$. По теореме Гамильтона-Кэли характеристический многочлен этого оператора его зануляет, то есть $0 = \chi_A(A)M = \chi_A(x)M$. Поскольку $Ann(M) = 0$, $\chi_A(x) = 0$.

$\square$

Определение 16.2. $R \subset S$ — расширение колец. *Целым замыканием R в S* называется

$$\overline{R} = \left\{x \in S \;\middle|\; x \text{ целое над } R\right\}.$$

Замечание 16.1. Аналогично определяется *замыкание $\overline{I}$ идеала I в S*, только теперь коэввициенты многочленов должны лежать в I.

Определение 16.3. Если $R = \overline{R}$, то расширение S/R называется *целым (или алгебраическим).*

Определение 16.4. Если R — область целостности, то $\overline{R}$ в его поле частных Q_R называется *нормализацией*, если $R = \overline{R}$ в своем поле частных, то кольцо R *нормально.*

Замечание 16.2. Если $\overline{R} \subset S$ — подкольцо.

Предложение 16.2. Пусть $R \subset S \subset T$ и расширения S/R, T/S — целые, тогда T/R — тоже целое расширение.

Доказательство. Рассмотрим какой-то элемент $x \in T$, он целый над S:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,\ a_i \in S.$$

Положим $R_m = R[a_0, \ldots, a_m]$. Заметим, что по предложению 16.1 (2) R_0 конечно порожден над R и R_i конечно порожден над R_{i-1}. Таким образом, R_{n-1} конечно порожден над R и по предложению 16.1 (3) x — целый над R. $\square$

Следствие 16.1. Если $R \subset S$ — расширение, то $\overline{R}$ — целозамкнуто в S.

Лемма 16.1. Пусть $A \subset B$, где B — область целостности, целая над A. Тогда A — поле, тогда и только тогда, когда B — поле.

Доказательство. Предположим, A — поле, рассмотрим произвольный ненулевой $b \in B$. Запишем для него многочен (такой есть в силу того, что b — не делитель нуля):

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0, \; a_i \in A, a_0 \neq 0.$$

Тогда $b^{-1} = -\dfrac{1}{a_0}(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1)$, то есть B — тоже поле.

Предположим, что B — поле. Нужно показать, что для любого ненулевого $a \in A$ его обратный элемент a^{-1} тоже лежит в A. Для начала заметим, что $\dfrac{1}{a} \in B$, то есть можно записать многочлен:

$$\left(\frac{1}{a}\right)^n + a_{n-1}\left(\frac{1}{a}\right)^{n-1} + \ldots + a_0 = 0, \; a_i \in A.$$

Домножим все на a^{n-1} и выразим $\dfrac{1}{a}$:

$$\frac{1}{a} = -(a_{n-1} + a_{n-2}a + \ldots + a_0a^{n-1}) \in A.$$

Таким образом, A — поле. □

Определение 16.5. Пусть $R \subset S$ — расширение, $\mathfrak{p} \subset R$, $\mathfrak{p}' \subset S$ — простые идеалы. Будем говорить, что $\mathfrak{p}'$ *лежит над* $\mathfrak{p}$, если $R \cap \mathfrak{p}' = \mathfrak{p}$.

Замечание 16.3. Пусть S/R — целое расширение, $U \subset R$ — мультипликативное. Тогда $(U^{-1}S)/(U^{-1})R$ — тоже целое расширение.

Теорема 16.1. Пусть S/R — целое расширение колец, $\mathfrak{p} \subset R$ — простой идеал, $\mathfrak{p}' \subset \mathfrak{q}' \subset S$ — вложенные простые, а $\mathfrak{a}' \subset S$ — произвольный идеал.

(1) Максимальность. Предположим, $\mathfrak{p}'$ лежит над $\mathfrak{p}$. Идеал $\mathfrak{p}'$ — максимальный тогда и только тогда, когда $\mathfrak{p}$ — максимальный.

(2) «Единственность». Предположим, оба идеала $\mathfrak{p}', \mathfrak{q}'$ лежат над $\mathfrak{p}$. Тогда $\mathfrak{p}' = \mathfrak{q}'$.

(3) Существование. Существует простой идеал $\mathfrak{r}' \subset S$, лежащий над $\mathfrak{p}$.

(4) Поднятие. Предположим, что $\mathfrak{a}' \cap S \subset \mathfrak{p}$. Тогда можно в **(3)** выбрать $\mathfrak{r}'$ так, чтобы $\mathfrak{a}' \subset \mathfrak{r}'$

Доказательство. **(1)** Поскольку расширение S/R — целое, то расширение $(S/\mathfrak{p}')/(R/\mathfrak{p})$ тоже. Тогда в силу леммы 16.1 $(S/\mathfrak{p}')$ и $(R/\mathfrak{p})$ являются или не являются полями одновременно.

(2) Локализуем все по $R - \mathfrak{p}$:

$$\begin{tikzcd} S \arrow[r] \arrow[d, hook, "i"] & S_{\mathfrak{p}} \arrow[d, hook, "S^{-1}i"] \\ R \arrow[r] & R_{\mathfrak{p}} \end{tikzcd},$$

где $S^{-1}i$ — тоже инъекция по предложению о точности локализации, а $R_{\mathfrak{p}}$ — локальное по предложению 11.5. Идеалы $\mathfrak{p}'R_{\mathfrak{p}}, \mathfrak{q}'R_{\mathfrak{p}}$ — вложенные простые по предложению 11.4 и все еще лежат над $\mathfrak{p}R_{\mathfrak{p}}$ (который максимальный по предложению 11.5), тогда по **(1)** идеалы $\mathfrak{p}'R_{\mathfrak{p}}, \mathfrak{q}'R_{\mathfrak{p}}$ — максимальные, следовательно совпадают. Значит, они и раньше совпадали.

(3) Опять локализуем точно так же. Выберем любой максимальный идеал $\mathfrak{r} \subset S_{\mathfrak{p}}$. Он лежит (по предложению 11.4) над некоторым максимальным (по **(1)**) идеалом в $R_{\mathfrak{p}}$, но такой только один — $\mathfrak{p}R_{\mathfrak{p}}$ по предложению 11.5

(4) В пункте **(3)** была свобода в выборе максимального $\mathfrak{r}$, выберем тот, который содержит $\mathfrak{a}'R_{\mathfrak{p}}$.

□

Лемма 16.2. Пусть I — идеал, тогда

$$\overline{I} = \sqrt{I\overline{R}}.$$

Доказательство. Рассмотрим произвольный $x \in \overline{I} \subset \overline{R}$, тогда

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0.$$

Заметим, что $x^n = -(a_{n-1}x^{n-1} + \ldots + a_0) \in I\overline{R}$, следовательно, $x \in \sqrt{I\overline{R}}$.

Обратно, рассмотрим произвольный $x \in \sqrt{I\overline{R}}$ (то есть для некоторого $n \in \mathbb{N}$ $x^n \in I\overline{R}$). Это означает, что

$$x^n = \sum_{i=1}^{k} b_i x_i, \ \ b_i \in I, x_i \in \overline{R}.$$

Рассмотрим конечнопорожденный модуль $M = R[x_1, \ldots, x_k]$ (он конечнопорожден по предложению 16.1) и отображение

$$M \to IM,$$

$$m \mapsto x^n m.$$

Тогда по теореме Гамильтона – Кэли x — целый над I. □

Замечание 16.4. Отметим, что в случае, когда I прост, коэффициенты минимального члена $x \in \overline{I}$ будут лежать в I.

Лемма 16.3. Пусть A — нормальное кольцо с полем частных Q_A и B — произвольная Q_A – алгебра. Если элемент $b \in B$ цел над A, то его минимальный многочлен $\mu(x)$ над Q_A принадлежит $A[x]$.

Доказательство. Пусть $f(x) \in A[x]$ — минимальный приведенный многочлен b. Тогда $f(x) = \mu(x)q(x)$ и по лемме Гаусса $\mu \in A[x]$.

□

Теорема 16.2. Предположим, $R \subset S$ — целое расширение областей целостности, причем R — нормально. Идеалы $\mathfrak{q} \subset \mathfrak{p} \subset R$ — простые, $\mathfrak{p}' \subset S$ — простой идеал, лежащий над $\mathfrak{p}$, тогда существует простой $\mathfrak{q}' \subset \mathfrak{p}'$, лежащий над $\mathfrak{q}$.

Доказательство. Достаточно показать, что $\mathfrak{q}S_{\mathfrak{p}'} \cap R = \mathfrak{q}$ (тут R нужно воспринимать как образ при локализации $\dfrac{x}{1}$, где $x \in R$), тогда по теореме 16.1 (4) получаем требуемое. Включение $\mathfrak{p} \subset \mathfrak{q}S_{\mathfrak{p}'} \cap R$ очевидно, докажем в другую сторону.

Рассмотрим произвольное $x \in \mathfrak{q}S_{\mathfrak{p}'} \cap R$. Положим $x = \dfrac{y}{s}$, где $y \in \mathfrak{q}S$, $s \in S - \mathfrak{p}'$. По лемме 16.2 имеем $y \in \overline{\mathfrak{q}}$:

$$y^n + u_{n-1}y^{n-1} + \ldots + u_0 = 0,\ \ u_i \in \mathfrak{q}.$$

Выразим $s = \dfrac{y}{x}$, разделим предыдущее равенство на x^n:

$$s^n + \frac{u_{n-1}}{x}s^{n-1} + \ldots + \frac{u_0}{x^n} = 0,\ \ \frac{u_i}{x^{n-i}} \in Q_R.$$

Заметим, что в силу замечания 16.4 минимальному многочлену для y соответствует минимальный многочлен для s. Тогда по лемме 16.3 коэффициенты $\dfrac{u_i}{x^{n-i}} \in R$.

Если так получилось, что $x \notin \mathfrak{q}$, то $\dfrac{u_i}{x^{n-i}} \in \mathfrak{q}$, но тогда $s \in \mathfrak{p}$, противоречие. □

17 Конечные целые сепарабельные расширения

Определение 17.1. Многочлен называется *сепарабельным*, если он имеет ровно столько различных корней, какова его степень.

Определение 17.2. Конечное расширение L/K — *сепарабельно*, если для любого $x \in L$ его минимальный многочлен сепарабельный.

Лемма 17.1. Конечное расширение L/K — сепарабельно тогда и только тогда, когда форма $(x, y) = tr(xy)$ — невырождена ($tr(x)$ — след оператора $\ell \mapsto \ell x$ в базисе над K).

Доказательство. Надо написать $\square$

Теорема 17.1. Пусть R — нётерова нормальная область целостности. Пусть K/Q_R — конечное сепарабельное расширение полей, $S = \overline{R}$ в поле K. Тогда S — конечнопорожденный модуль над R.

Доказательство. Предположим, $v_1, \ldots, v_n$ — базис K над Q_R. Без ограничения общности можно считать, что $v_i \in S$ (достаточно домножить на НОД знаменателей коэффициентов минимального многочлена). Пусть $v'_1, \ldots, v'_n$ — двойственный базис относительно билинейной формы $(x, y) = tr(xy)$.

Рассмотрим $s \in S$

$$s = \sum_{i=1}^{n} a_i v'_i \; a_i \in Q_R,$$

$$a_i = (s, v_i) \in R.$$

Таким образом, S — подмодуль R^n, который нётеров по следствию следствию 8.2. $\square$

18 Алгебры конечного типа

Определение 18.1. Пусть $K \subset L$ — расширение полей. Набор алгебраически независимых над K элементов $l_1, \ldots, l_k \in L$ называется *трансцендентным базисом*, если $K(l_1, \ldots, l_k) \subset L$ — алгебраическое. *Трансцендентной размерностью* $tr.deg_{\Bbbk} R$ целостного кольца R называется количество элементов трансцендентного базиса $Frac(R)$ над $\Bbbk$.

Замечание 18.1. Для трансцендентного базиса верно многое, что верно для обычного: любую алгебраически независимую систему можно дополнить до базиса, все базисы равномощны. Этого я доказывать не буду. Хотя, возможно, и стоило бы.

Лемма Эмми Нётер о нормализации. Пусть B — конечнопоржденная $\Bbbk$ – алгебра. Пусть $tr.deg_{\Bbbk} B = s$. Тогда существуют такие алгебраически независимые элементы $b_1, \ldots, b_s$, что B — целое над $\Bbbk[b_1, \ldots, b_s]$.

Доказательство. **(1)** Пусть $\operatorname{char} \Bbbk = 0$. Начнем с системы породающих $x_1, \ldots, x_l$. Если они алгебрически зависимы, то для некоторого $F \in \Bbbk[y_1, \ldots, y_l]$ выполнено $F(x_1, \ldots, x_l) = 0$. Сделаем линейную замену

$$\begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_l \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_l \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 - \alpha_2 x_1 \\ \ldots \\ x_l - \alpha_l x_1 \end{pmatrix}$$

Можно подобрать такие $\alpha_i \in \Bbbk$, что коэффициент при старшем x_1^k будет в точности 1. Тогда y_1 зависит от $y_2, \ldots, y_l$. Так можно делать, пока порождающие алгебраически зависимы.

(2) Пусть $\operatorname{char} \Bbbk = p$. Хотим сделать похожую замену:

$$\begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_l \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_l \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 - x_1^{k_2} \\ \ldots \\ x_l - x_1^{k_l} \end{pmatrix}$$

Подберем l_i так, чтобы все одночлены имели разную степень по x_1 (Тода автоматически при старшем x^k коэффициент из поля $\Bbbk$). Пусть в записи F был одночлен $a_J x_1^{j_1} x_2^{j_2} \ldots x_l^{j_n}$ (J пробегает все одночлены F). При такой замене он перейдет в

$$a_J x_1^{j_1} (x_2 + x_1^{k_2})^{j_2} \ldots (x_l + x_1^{k_l})^{j_n}.$$

Таким образом, при раскрытии скобок вынесется самый старший по x_1 одночлен со степенью $d_J = j_1 + k_2 j_2 + \ldots + k_l j_n$. Пусть $l > \max\limits_{J,k}(j_k)$. Тогда установим $k_i = l^i$.

$\square$

Обозначение 18.1. Если $\mathfrak{a}$ — идеал в кольце многочленов $\Bbbk[y_1, \ldots, y_n]$, определим V

$$V(\mathfrak{a}) = \{y \in \mathbb{A}^n \mid f(y) = 0 \text{ для любого } f \in \mathfrak{a}\}$$

Другими словами, $V(\mathfrak{a})$ — множество нулей всех многочленов $\mathfrak{a}$. Соответственно, если $\mathfrak{a}$ — конечно порожденный, то это множество решений конечной системы уравнений.

Обозначение 18.2. Если X — подмножество $\mathbb{A}^n$, определим I

$$I(X) := \{f \in \Bbbk[y_1, \ldots, y_n] \mid I(x) = 0 \text{ для любого } x \in X\}.$$

Другими словами, $I(X)$ — множество всех многочленов, зануляющихся на X.

Теорема Гильберта о нулях Пусть $\Bbbk$ — алгебраически замкнутое поле. Тогда

(1) для каждого максимального идеала $\mathfrak{m}$ справедливо $V(\mathfrak{m}) = P$ для некоторой точки $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$;

(2)если $\mathfrak{a}$ — идеал, отличный от $\Bbbk[Y_1, \ldots, Y_n]$, то $V(\mathfrak{a}) \neq \varnothing$;

(3) Пусть $I = (f_1, \ldots, f_k)$. Предположим, что $f(x) = 0$ для любого $x \in V(I)$. Тогда $f^n \in I$ ($f \in \sqrt{I}$).

Доказательство. **(1)** Достаточно показать, что $\mathfrak{m} = ((x_1 - a_1), \ldots, (x_n - a_n))$ для некоторых a_i. А для этого достаточно показать, что $k = \Bbbk[x_1, \ldots, x_n]/\mathfrak{m} \simeq \Bbbk$. Тогда $x_i \equiv_{\mathfrak{m}} a_i$.

k — поле. Тогда по теореме Нётер о нормализации существуют такие алгебраически независимые $y_1, \ldots, y_s \in k$, что расширение $A = \Bbbk[y_1, \ldots, y_s] \subset k = B$ — алгебраическое. По лемме 16.1 $A = \Bbbk[y_1, \ldots, y_s]$ — поле. Но тогда $s = 0$. Что и требовалось.

(2) Очевидно следует из **(1)**, поскольку любой идеал содержится в некотором максимальном.

(3) Заметим, что $(f_1, \ldots, f_n, tf - 1) = (1)$ по условию (это называется Rabinovich trick). Тогда существуют такие $g_i(x_1, \ldots, x_n, t)$, что $\sum\limits_i g_i f_i + g_0(f-1) = 1$. Подставим $t = \dfrac{1}{f}$ и домножим на очень большую степень f. Получим то, что нужно.

$\square$

19 Градуированные и фильтрованные кольца и модули

Определение 19.1. Кольцо R называется *градуированным*, если оно представимо в виде

$$R = \bigoplus_{k \geqslant 0} R_k,$$

где R_n — абелева подгруппа и $R_n R_m \subset R_{n+m}$.

Аналогичное определение для модуля.

Определение 19.2. Модуль M над градуированным кольцом R называется *градуированным*, если он представимо в виде

$$M = \bigoplus_{k \in \mathbb{Z}} M_k,$$

где M_n — абелева подгруппа и $R_n M_m \subset M_{n+m}$.

Определение 19.3. Элементы групп R_i, M_j называются *однородными* между собой.

Определение 19.4. Гомоморфизм градуированных модулей $f : M \to N$ называется *градуированным*, если для всех $i \in \mathbb{Z}$

$$f(N_i) \subset M_i.$$

Предложение 19.1. Пусть $R = \bigoplus\limits_{k \geqslant 0} R_k$ — градуированное кольцо. Следующие условия эквивалентны:

(1) R — нётерово кольцо.

(2) R_0 — нетерово и R — алгебра конечного типа над R_0.

Доказательство. (1) $\Rightarrow$ (2) Заметим, что $R_0 = R/R_+$ — нётерово, выберем образующие идеала $R_+ = (v_1, \ldots, v_n)$, $\deg v_i = k_i$. Покажем, что $R' := R_0[v_1, \ldots, v_n] = R$. Проверим по индукции, что $R_i \subset R'$. Для $i = 0$ утверждение очевидно. Рассмотрим $x \in R_i$. Выразим через образующие:

$$x = \sum_{j=1}^{n} a_j v_j, \ \ \deg a_j = i - k_j.$$

По предположению индукции $a_j \in R'$, что и требовалось.

(2) $\Rightarrow$ (1) Это верно по теореме Гильберта о базисе. □

Определение 19.5. Подмодуль N градуированного модуля M называется *градуированным*, если $N = \bigoplus N_k$ и $N_k = M_k \cap N$.

Определение 19.6. Предположим, $I \subset R$ — идеал. Модуль M называется *фильтрованным*, если существует последовательность подмодулей

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_n \supseteq \ldots.$$

Фильтрация называется

- I – *фильтрацией*, если $IM_n \subseteq M_{n+1}$ для всех n.
- I –*адической фильтрацией*, если $IM_n = M_{n+1}$ для всех n.
- *стабильной* I – *фильтрацией*, если $IM_n = M_{n+1}$ для всех достаточно больших n.

Положим $A = \bigoplus\limits_{k \geqslant 0} I^k$, $I^0 = R$ $R^* = \bigoplus\limits_{k>0} I^K$. Предположим, есть I – фильтрованный модуль M. Заметим, что $M^* = \bigoplus\limits_{k>0} M_n$ — R^* – модуль.

Предложение 19.2. Пусть R — нётерово кольцо, M — конечнопорожденный модуль с I – фильтрацией. Тогда следующие утверждения эквивалентны:

(1) M^* — конечнопорожденный над R^*:

(2) фильтрация стабильна.

Доказательство. (1) $\Rightarrow$ (2) R — нётеров, следовательно, $I = (v_1, \ldots, v_s)$. По теореме Гильберта о базисе $R[v_1, \ldots, v_s]$ — нётеоров, тогда его подмодуль R^* — тоже нётеров. По следствию 8.2 M^* — нётеоров. Полседовательность модулей

$$L_k = M_0 \oplus \ldots \oplus M_k \oplus IM_k \oplus I^2 M_k \oplus \ldots$$

— возрастающая по условию фильтрации, то есть должна стабилизироваться с некоторого момента N, это означает, что $M_k = I^{N-k} M_N$ для всех $k \geqslant N$.

(2) $\Rightarrow$ (1) Если $M_k = I^{N-k} M_N$ для всех $k \geqslant N$, то M^* порождается $\bigoplus\limits_{k=0}^{N} M_k$, а каждая из компонент конечно порождается над R. □

Замечание 19.1. Во всех утверждениях, которые будут следовать из этого утверждения, R — нётеров, а M — конечнопорожден.

Теорема Артина – Риса. Пусть R — нётерово, M — конечнопорожденный R – модуль со стабильной I – фильтрацией, $L \subset M$ — произвольный подмодуль. Тогда $L_k = M_k \cap L$, — тоже стабильная I — фильтрация.

Доказательство. Для начала заметим, что получилась I – фильтрация:

$$IL_k \subset IM_k \cap IL \subset M_{k+1} \cap L \subset L_{k+1}.$$

Чтобы доказать, что фильтрация стабильна, нужно проверить, что модуль L^* конечно порожден над L^* (тогда побеждаем по предложению 19.2), а это так, потому что он является подмодулем M^*. □

Следствие 19.1. Существует такое $s > 0$, что для любого d выполнено

$$I^d(L \cap I^s M) = L \cap I^{d+s} M.$$

Доказательство. Положим $M_n = I^n M$. Тогда равенство превращается в $I^d L_s = L_{d+s}$, а это так по определению стабильной фильтрации. □

Теорема Крулля о пересечении. Положим $M' = \bigcap I^n M$, тогда $IM' = M'$.

Доказательство. Заметим, что $I^n M \cap M' = M'$. По следствию 19.1 при $d = 1$

$$IM' = I(M' \cap I^s M) = M' \cap I^{s+1} M = M'.$$

□

Следствие 19.2. Если $I \subset J(R)$ или модуль M — точный, то $\bigcap I^n M = \{0\}$.

Доказательство. По теореме Крулля о пересечении $IM' = M'$. Поскольку $J(R) \subset rad(M)$, в случае, когда $I \subset J(R)$, по лемме Накаямы $M' = IM'$. Во втором случае по следствию 4.1 найдется такое $a \in I$, что $(1 + a)M = 0$, что противоречит точности. □

Определение 19.7. Пусть $I \subset R$ — идеал, M — модуль с I – фильтрацией, тогда хорошо определено градуированное кольцо:

$$gr_I(R) = \bigoplus_{n \geqslant 0} I^n / I^{n+1},$$

$$gr_I(M) = \bigoplus_{n \geqslant 0} M_n / M_{n+1}$$

Замечание 19.2. Если R нётерово, то $gr_I(R)$ — тоже.

Замечание 19.3. Если M — конечно порожденный модуль и фильтрация стабильна, то $gr_I(M)$ конечно порожден над $gr_I(R)$.

20 Многочлены Гильберта

Пусть $A = \bigoplus\limits_{n \geqslant 0} A_n$ — нётерова градуированная алгебра, M — конечнопорожденный градуированный A – модуль, λ — аддитивная функция на A_0 – модулях со значениями в $\mathbb{Z}$, для которой для любой точной последовательности

$$0 \to M' \to M \to M'' \to 0$$

выполнено тождество

$$\lambda(M') - \lambda(M) + \lambda(M'') = 0.$$

Пример 20.1. В случае, когда A_0 – артиново (по теореме о точности длины), подойдет $\lambda(M) = \ell(M)$.

Определение 20.1. *Серией Гильберта – Пуанкаре* называется

$$P(M,t) = \sum_{n \geqslant 0} \lambda(M_n) t^n \in \mathbb{Z}[[t]].$$

Теорема Гильберта – Серра. Пусть A порождается $x_1, \ldots, x_s$, $\deg x_i = k_i$. Тогда существует такая функция $f(t) \in \mathbb{Z}[t]$, что

$$P(M,t) = \frac{f(t)}{\prod\limits_{i=1}^{s} (1 - t^{k_i})}.$$

Доказательство. Будем доказывать индукцией по s. При $s = 0$ модуль M конечно порожден над $A = A_0$, пусть $m_1, \ldots, m_k$ — порождающие. Тогда начиная с какого-то момента M_N не содержит ни одной из порождающих, с этого момента $M_N = 0$. Тогда $P(M,t) \in \mathbb{Z}[t]$ и можно положить $f(t) = P(M,t) \cdot \prod\limits_{i=1}^{s}(1 - t^{k_i})$. Таким образом, база доказана.

Переход. Рассмотрим гомоморфизм, получающийся домножением на x_s:

$$x_s : M_n \to M_{n+k_s}.$$

Построим точную последовательность для этого гомоморфизма (K_n — ядро, L_{n+k_s} — коядро):

$$0 \to K_n \to M_n \xrightarrow{x_s} M_{n+k_s} \to L_{n+k_s} \to 0.$$

Положим $K = \bigoplus\limits_{n \geqslant 0} K_n$, $L = \bigoplus\limits_{n \geqslant 0} L_n$, заметим, что x_s аннулирует K и L. Таким образом, K и L — модули над $A_0[x_1, \ldots, x_{x-1}]$ и для них верно индукционное предположение (обозначим искомые для них многочлены как $a(t)$ и $b(t)$ соответственно). Из точности последовательностей имеем равенство:

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0.$$

Домножим каждое из равенств на t^{n+k_s} и сложим:

$$t^{k_s}(P(K,t) - P(M,t)) + (P(M,t) - P(L,t) - g(t))$$

где $g(t) \in \mathbb{Z}[t]$ — разность «хвостов» двух последних членов (потому что там суммирование ведется не с нуля). Выразим $P(M,t)$ (тут пользуемся предположением индукции):

$$P(M,t) = \frac{b(t) + g(t) \cdot \prod_{i=1}^{s}(1 - t^{k_i}) - a(t)t^{k_s}}{\prod_{i=1}^{s}(1 - t^{k_i})}.$$

□

Обозначение 20.1. Обозначим $d(M) = -ord_{(1-t)}P(M,t)$ — степень вхождения $(1-t)$ в знаменатель $P(M,t)$.

Предложение 20.1. Если $k_i = 1$ при всех i, то $\lambda(M_n)$ — многочлен от n степени $d(M) - 1 = d - 1$ (при больших n).

Доказательство. По теореме Гильберта – Серра можем считать, что

$$\sum_{n \geqslant 0} \lambda(M_n)t^n = P(M,t) = \frac{f(t)}{(1-t)^d} = f(t)\sum_{k \geqslant 0} t^k \binom{d+k-1}{d-1},$$

причем $f(1) \neq 0$. Если явно посчитать коэффициент при t^n (тут $n \geqslant \deg f$), получится полином степени не больше $d-1$ (из такой цэшки в принципе больше ничего вылезти не сможет). Если посчитать коэффициент при $d-1$ степени явно, то получится $\dfrac{f(1)}{(d-1)!} \neq 0$. □

21 Функция Гильберта – Самуэля

Соглашение. Все модули в этой главе будут конечнопорожденными, $(R, \mathfrak{m})$ — нётерово локальное кольцо.

Предложение 21.1. Пусть $\mathfrak{q} \subset R$ — идеал. Следующие утверждения эквивалентны:

(1) $R/\mathfrak{q}$ — артиново;

(2) существует $n > 0$, для которого $\mathfrak{m}^n \subset \mathfrak{q}$;

(3) $\mathfrak{q}$ — $\mathfrak{m}$ – примарный.

Доказательство. Пусть $f : R \to R/\mathfrak{q}$ — каноническая проекция. Заметим, что $f(\mathfrak{m})$ — единственный простой идеал в $R/\mathfrak{q}$.

(1) $\Rightarrow$ (2) В артиновом кольце нильрадикал $nil(R/\mathfrak{q}) = \mathfrak{m}$ нильпотентен по следствию 9.1.

(2) $\Rightarrow$ (3) Рассмотрим такое первое N, что $(f(\mathfrak{m}))^N = 0$, тогда для любого ненулевого $x \in (f(\mathfrak{m}))^{N-1}$ идеал $\mathfrak{m} = Ann(x)$. Покажем, что других ассоциированных простых нет. Предположим, нашелся другой ассоциированный простой $\mathfrak{p}$, тогда обязательно $\mathfrak{q} \subset \mathfrak{p} \subsetneq \mathfrak{m}$. Рассмотрим $x \in \mathfrak{m} - \mathfrak{p}$, $x^N \in R - \mathfrak{p} \subset R - \mathfrak{q}$, противоречие.

(3) $\Rightarrow$ (1) Заметим, что $\mathfrak{m} = nil(R/\mathfrak{q})$. В нётеровом кольце нильрадикал нильпотентен (по следствию 8.1), тогда по лемме 10.4 нётеровость кольца равносильна его артиновости. □

Определение 21.1. Такой идеал $\mathfrak{q}$ называется *параметрическим.*

Соглашение. Далее в этой главе $\mathfrak{q} = (x_1, \dots, x_s)$ будет обозначать параметрический идеал.

Предложение 21.2. Предположим, M_n — стабильная $\mathfrak{q}$ – фильтрация модуля M. Тогда для всех $n \geqslant 0$ выполнено $\ell(M/M_n) < \infty$.

Доказательство. Модуль M_n/M_{n+1} — нётеров и зануляется q, поэтому он конечнопорожден над $R/\mathfrak{q}$. По предложению 21.1 кольцо $R/\mathfrak{q}$ — артиново, тогда по теореме Акизуки – Хопкинса $\ell(M_n/M_{n+1}) < \infty$. Тогда

$$\ell_n = \ell(M/M_n) = \sum_{i=1}^{n-1} M_i/M_{i+1} < \infty.$$

□

Предложение 21.3. Для достаточно больших n число $\ell_n = \ell(M/M_n)$ — это значения фиксированного многочлена, степень которого не больше s.

Доказательство. В силу замечания 19.3 модуль $gr_{\mathfrak{q}}(M)$ конечнопорожден над $gr_{\mathfrak{q}}(M)$, тогда по предложению 20.1 $\ell_n = \sum\limits_{i=1}^{n-1} g_i$, где $g_i = \ell(M_i/M_{i+1})$ — значения многочлена степени степени не больше $s-1$. Нетрудно заметить, что сумма таких многочленов — многочлен на 1 большей степени. □

Предложение 21.4. Степень и старший коэффициент многочлена $\alpha(n) = \ell(M/M_n)$ (при больших n) не зависят от выбора фильтрации.

Доказательство. Достаточно доказать, что эти многочлены $\alpha(n)$ для произвольной стабильной фильтрации M_n и $\beta(n)$ для $\mathfrak{q}$ – адической $\mathfrak{q}^n M$ устроены так, что

$$\lim_{n\to\infty} \frac{\alpha(n)}{\beta(n)} = 1.$$

Заметим, что $\alpha(n) = \ell(M/M_n) \leqslant \ell(M/\mathfrak{q}^n M) = \beta(n)$ (потому что $\mathfrak{q}^n M \subset M_n$ по определению фильтрации), поэтому

$$\lim_{n\to\infty} \frac{\alpha(n)}{\beta(n)} \leqslant 1.$$

В силу стабильности фильтрации $\mathfrak{q}^n M_{n_0} = M_{n+n_0}$. Поэтому $M_{n+n_0} \subset \mathfrak{q}^n M$ и

$$\lim_{n\to\infty} \frac{\alpha(n)}{\beta(n)} = \lim_{n\to\infty} \frac{\alpha(n+n_0)}{\beta(n)} \geqslant 1.$$

□

Определение 21.2. Многочлен $\ell(M/M_n)$ называется *многочленом Гильберта – Самуэля* и обозачается

$$\chi_{\mathfrak{q}}^M(n) = \ell(M/\mathfrak{q}^n M).$$

Обозначение 21.1. Наименьшее количество образующих $\mathfrak{m}$ – примарного идеала обозначается $\delta(R)$.

Замечание 21.1. В силу предложения 20.1 $\delta(R) \geqslant d(R)$.

Предложение 21.5. Пусть $x \in R$ — не делитель нуля для M. Положим $M' = M/xM$, тогда

$$\deg \chi_{\mathfrak{q}M'} \leqslant \deg \chi_{\mathfrak{q}}^M - 1.$$

Доказательство. Пусть $N = xM$, поскольку x — не делитель нуля, $M \simeq N$. По теореме Артина – Рисса $N_k = N \cap \mathfrak{q}^n M$ — стабильная фильтрация и по предложению 21.4 многочлен $\chi_{\mathfrak{q}}^N$ имеет тот же старший коэффициент и степень, что и $\chi_{\mathfrak{q}}^M$. Рассмотрим точную последовательность

$$0 \to N/N_k \to M/\mathfrak{q}^n M \to M'/\mathfrak{q}^n M' \to 0.$$

По теореме о точности длины

$$\ell(N/N_k) - \ell(M/\mathfrak{q}^n M) + \ell(M'/\mathfrak{q}^n M') = \chi_{\mathfrak{q}}^N(k) - \chi_{\mathfrak{q}}^M(k) + \chi_{\mathfrak{q}}^{M'}(k) = 0.$$

□

22 Размерность Крулля

Теперь R — произвольное коммутативное кольцо. Выберем $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ — последовательность вложенных простых идеалов.

Определение 22.1. *Размерностью Крулля* $\dim(R)$ называется

$$\dim(R) = \sup\big\{n \;\big|\; \text{существует цепочка вложенных простых длины } n\big\}.$$

Определение 22.2. *Высотой* простого идеала $\mathfrak{p}$ называется $ht(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$. *Ковысотой* называется $coht(\mathfrak{p}) = \dim(R/\mathfrak{p})$.

Замечание 22.1. $coht(\mathfrak{p}) + ht(\mathfrak{p}) < \dim(R)$.

Пример 22.1. В случае, когда $R = F$ — поле, $\dim F = 0$, $\dim F[x] = 1$

Пример 22.2. Если $R = \mathbb{Z}$, то $\dim \mathbb{Z} = 1$.

Пример 22.3. Условие, что $\dim R = 0$, равносильно тому, что ножество максимальных идеалов совпадает с множеством простых. Следовательно (по теореме Акизуки-Хопкинса), R — артиново тогда и только тогда, когда R — нётерово и $\dim R = 0$.

Предложение 22.1. В случае, когда R — локальное нётерово, $d(R) \geqslant \dim(R)$.

Доказательство. Будем доказывать по индукции по $d = d(R)$. Если $d = 0$, то $\ell(A/\mathfrak{m}^n) = const$ при больших n, следовательно, $\mathfrak{m}^{n+1} = \mathfrak{m}^n$ и по лемме Накаямы $\mathfrak{m}^n = 0$. Рассмотрим произвольный простой $\mathfrak{p} \subset \mathfrak{m} \subset R$. Поскольку $0 = \mathfrak{m}^n \subset \mathfrak{p}$, в силу простоты $\mathfrak{p}$ имеем:

$$\mathfrak{m} \subset \mathfrak{p} \subset \mathfrak{m}.$$

Таким образом, $\mathfrak{m} = \mathfrak{p}$ и $\dim R = 0$.

Пусть теперь $d > 0$. Рассмотрим цепочку вложенных простых:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n.$$

Рассмотрим ненулевой $x \in \mathfrak{p}_1/\mathfrak{p}_0$, пусть $x' \in R' = R/\mathfrak{p}_0$ — его образ при вложении, заметим, что x' — не делитель нуля и по предложению 21.5

$$d(R'/(x')) \leqslant d(R') - 1.$$

Пусть $\mathfrak{m}'$ — максимальный идеал в R'. Тогда $R'/\mathfrak{m}'^n$ — образ $R/\mathfrak{m}^n$ и $\ell(R/\mathfrak{m}^n) \geqslant \ell(R'/\mathfrak{m}'^n)$. Следовательно, $d(R) \geqslant d(R')$ и

$$d(R'/(x')) \leqslant d(R) - 1.$$

Таким образом, для $R'/(x')$ выполнено предположение индукции и $d(R'/(x')) \geqslant \dim(R'/(x'))$. Образ простых идеалов $\mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ в $R'/(x')$ образует цепочку длины $n-1$. Таким образом,

$$n - 1 \leqslant d - 1,$$

что и требовалось. □

Следствие 22.1. Для локального нётерового кольца $\dim(R) < \infty$.

Следствие 22.2. Пусть R — нётерово, $\mathfrak{p} \subset R$ — простой, тогда $ht(\mathfrak{p}) < \infty$.

23 Теорема о размерности

Предложение 23.1. Кольцо $(R, \mathfrak{m})$ — локально и нётерово, тогда $\dim(R) \geqslant \delta(R)$.

Доказательство. Будем строить по индукции такое подмножество $\{x_1, \ldots, x_r\} \subset R$, чтобы высота любого простого идеала, содержащего $(x_1, \ldots, x_i)$, была хотя бы i. Этот процесс должен закончится при $r = ht(\mathfrak{m})$ (иначе будет видно, что его можно продолжать), в этом случае мы победим.

Предположим, мы уже построили множество $\{x_1, \ldots, x_{i-1}\}$, для которого условие выполнено. Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ — все простые идеалы высоты ровно $i-1$. Заметим, что все они минимальны по предположению индукции, тогда по предложению 14.5 их действительно конечно. Положим $d_1 = ht(\mathfrak{m})$, предположим, что $i - 1 < d_1$. Тогда по Prime Avoidance найдется такое $x_i \in \mathfrak{m} - \bigcup\limits_{j=1}^{s} \mathfrak{p}_j$ (иначе $\mathfrak{m} = \mathfrak{p}_j$ для некоторого j). Этим элементом и дополним текущее множество. □

Теорема о размерности. Для локальных нётеровых колец выполнено неравенство:

$$\delta(R) \geqslant d(R) \geqslant \dim(R) \geqslant \delta(R),$$

следовательно, неравенства можно заменить на равенства.

Доказательство. Первое неравенство было в замечании 21.1, второе неравенство доказано в предложении 22.1, а третье — в предложении 23.1. □

Следствие 23.1. Пусть $\Bbbk = R/\mathfrak{m}$, тогда $\dim(R) \leqslant \dim_{\Bbbk}(\mathfrak{m}/\mathfrak{m}^2)$.

Доказательство. Достаточно доказать, что прообразы базиса $\mathfrak{m}/\mathfrak{m}^2$ в $\mathfrak{m}$ будут образующими. Для этого нужно рассмотреть $\mathfrak{n}\mathfrak{m}$ — идеал, который порождают эти прообразы, и из того, что $\mathfrak{n} + \mathfrak{m} \cdot \mathfrak{m} = \mathfrak{m}$ с помощью леммы Накаямы вывести $\mathfrak{m}/\mathfrak{n} = 0$. □

Определение 23.1. Размерность $\dim_{\Bbbk}(\mathfrak{m}/\mathfrak{m}^2)$ называется *вложенной размерностью* кольца $(R, \mathfrak{m})$.

Определение 23.2. В случае, когда $\dim(R) = \dim_{\Bbbk}(\mathfrak{m}/\mathfrak{m}^2)$, кольцо $(R, \mathfrak{m})$ называется *регулярным*.

Следствие 23.2. Пусть R — нётерово, $x_1, \ldots, x_r$ — произвольные элементы кольца. Рассмотрим минимальный простой $\mathfrak{p} \supset (x_1, \ldots, x_r)$. Тогда $ht(\mathfrak{p}) \leqslant r$.

Доказательство. По условию имеем $(x_1, \ldots, x_s)R_{\mathfrak{p}} \subset \mathfrak{p}R_{\mathfrak{p}}$. Заметим, что $\mathfrak{p}R_{\mathfrak{p}}$ — максимальный и единственный простой, содержащий $(x_1, \ldots, x_r)R_{\mathfrak{p}}$, тогда по теореме 2.2 $\sqrt{(x_1, \ldots, x_r)R_{\mathfrak{p}}} = \mathfrak{p}R_{\mathfrak{p}}$. По только что доказанной теореме, получаем:

$$ht(\mathfrak{p}) = \dim(R_{\mathfrak{p}}) = \delta(R_{\mathfrak{p}}) \leqslant r.$$

□

Теорема Крулля о главных идеалах. Пусть R —нётерово, $x \in R$ — необратим и не является делителем нуля, $\mathfrak{p}$ — минимальный простой, содержащий (x). Тогда $ht(p) = 1$.

Доказательство. По следствию 23.2 мы знаем, что $ht(\mathfrak{p}) \leqslant 1$. Предположим, что $ht(\mathfrak{p}) = 0$. Тогда $\mathfrak{p}$ — минимальный простой в $Supp(R)$, а по предложению 14.5 $\mathfrak{p} \in Ass(R)$. По предложению 14.7 $x \in \mathfrak{p} \subset ZD(R)$ — противоречие. □

Предложение 23.2. Пусть $(R, \mathfrak{m})$ — локальное нётерово, $x \in \mathfrak{m}$ — не делитель нуля. Тогда $\dim(R/(x)) = \dim(R) - 1$.

Доказательство. По теореме о размерности и предложению 21.5 имеем:

$$d = \dim(R/(x)) = d(R/(x)) \leqslant d(R) - 1 = \dim(R) - 1.$$

Пусть $\overline{x}_1, \ldots, \overline{x}_d$ — минимальная система образующих $\mathfrak{m}/(x)$. Тогда $(x_1, \ldots, x_d, x) = \mathfrak{m}$ и

$$\dim(R) = \delta(R) \leqslant d + 1.$$

□