ОБЩАЯ ТЕОРИЯ ИДЕАЛОВ КОММУТАТИВНЫХ КОЛЕЦ

В этой главе мы рассмотрим свойства делимости идеалов коммутативных колец и попытаемся перенести некоторые простые теоремы, имеющие место в области целых чисел, на кольца общего типа. Чтобы не сталкиваться с лишними трудностями, целесообразно ограничиться кольцами, в которых каждый идеал обладает конечным базисом; этот случай, как мы увидим, встречается очень часто.

§ 115. Нётеровы кольца

Мы говорим, что в кольце $\mathfrak{o}$ *справедлива теорема о базисе*, если каждый идеал в $\mathfrak{o}$ обладает конечным базисом. Коммутативные кольца, в которых выполняется теорема о базисе, называются *нётеровыми*.

Теорема о базисе имеет место в любом теле, потому что там есть лишь идеалы (0) и (1) Она имеет место и в кольце целых чисел и, говоря более общо, в любом кольце главных идеалов. Кроме того, она справедлива в любом конечном кольце. Позднее мы увидим, что теорема о базисе имеет место в факторкольце $\mathfrak{o}/\mathfrak{a}$, если она имеет место в самом кольце $\mathfrak{o}$. Наконец, справедливо следующее предложение, восходящее к Гильберту:

Теорема. *Если теорема о базисе выполняется в кольце* $\mathfrak{o}$, *содержащем единичный элемент, то она выполняется и в кольце многочленов* $\mathfrak{o}[x]$.

Доказательство. Пусть $\mathfrak{A}$ — произвольный идеал в $\mathfrak{o}[x]$. Коэффициенты при старших степенях переменных x в многочленах из идеала $\mathfrak{A}$ вместе с нулем составляют некоторый идеал в $\mathfrak{o}$, потому что если α и β — старшие коэффициенты в многочленах a и b:

$$a = \alpha x^n + \ldots,$$
$$b = \beta x^m + \ldots,$$

то, скажем, при $n \geqslant m$

$$a - bx^{n-m} = (\alpha x^n + \ldots) - (\beta x^n + \ldots) = (\alpha - \beta) x^n + \ldots$$

— вновь некоторый многочлен из $\mathfrak{A}$ и $\alpha - \beta$ — старший коэффициент или нуль. Точно так же, если α — старший коэффициент многочлена a, то $\lambda\alpha$ — либо старший коэффициент многочлена λa, либо нуль.

Согласно условию идеал $\mathfrak{a}$ старших коэффициентов имеет некоторый базис $(\alpha_1, \ldots, \alpha_r)$; будем считать, что α_i — старший коэффициент многочлена

$$a_i = \alpha_i x^{n_i} + \ldots$$

степени n_i и пусть n — наибольшее из чисел n_i.

Включим многочлены a_i в конструируемый базис идеала $\mathfrak{A}$. Посмотрим, какие еще многочлены необходимо включить в этот базис.

Если

$$f = \alpha x^N + \ldots$$

— произвольный многочлен из $\mathfrak{A}$ степени $N \geqslant n$, то элемент α должен принадлежать идеалу $\mathfrak{a}$:

$$\alpha = \sum \lambda_i \alpha_i.$$

Построим многочлен

$$f_1 = f - \sum (\lambda_i x^{N-n_i}) a_i.$$

Коэффициент при x^N в этом многочлене равен

$$\alpha - \sum \lambda_i \alpha_i = 0.$$

Таким образом, многочлен f_1 имеет степень, меньшую N. Следовательно, f можно заменить по модулю $(a_1, \ldots, a_r)$ многочленом меньшей степени. Мы можем таким путем понижать степень, пока она не станет меньше n. Поэтому достаточно ограничиться многочленами степеней, меньших n.

Коэффициенты при x^{n-1} в многочленах степени $\leqslant n-1$ из $\mathfrak{A}$, объединенные с нулем, составляют некоторый идеал $\mathfrak{a}_{n-1}$; пусть

$$(\alpha_{r+1}, \ldots, \alpha_s)$$

— базис этого идеала, и α_{r+i} — старший коэффициент многочлена

$$a_{r+i} = \alpha_{r+i} x^{n-1} + \ldots$$

Включим теперь в базис и многочлены $a_{r+1}, \ldots, a_s$. Тогда любой многочлен степени $\leqslant n-1$ можно заменить по модулю $(a_{r+1}, \ldots, a_s)$ многочленом степени $\leqslant n-2$; для этого, как и раньше, нужно из данного многочлена вычесть подходящую линейную комбинацию

$$\sum \lambda_{r+i} a_{r+i}.$$

Продолжим намеченную конструкцию. Коэффициенты при x^{n-2} в многочленах степени $\leqslant n-2$ вместе с нулем составляют идеал $\mathfrak{a}_{n-2}$, базисные элементы $\alpha_{s+1}, \ldots, \alpha_t$ которого соответствуют многочленам $a_{s+1}, \ldots, a_t$. Эти многочлены мы также включим в базис. В конце концов придем к идеалу $\mathfrak{a}_0$, состоящему из констант,

лежащих в $\mathfrak{A}$; базис этого идеала $(\alpha_{v+1}, \ldots, \alpha_w)$ приводит к многочленам $a_{v+1}, \ldots, a_w$. Таким образом, каждый многочлен из $\mathfrak{A}$ приводится к нулю по модулю

$$(a_1, \ldots, a_r, a_{r+1}, \ldots, a_s, \ldots, a_{v+1}, \ldots, a_w).$$

Следовательно, многочлены $a_1, \ldots, a_w$ составляют базис в $\mathfrak{A}$, чем и завершается доказательство теоремы о базисе.

Из этой теоремы с помощью n-кратного повторения сразу получается обобщение:

Если теорема о базисе имеет место в кольце $\mathfrak{o}$ с единицей, то она справедлива и в кольце многочленов $\mathfrak{o}[x_1, \ldots, x_n]$ от конечного множества переменных $x_1, \ldots, x_n$.

Наиболее важные частные случаи: кольцо целочисленных многочленов $\mathbb{Z}[x_1, \ldots, x_n]$ и любое кольцо многочленов $\mathsf{K}[x_1, \ldots, x_n]$ с коэффициентами в поле K. Все эти кольца нётеровы.

Гильберт высказал свою теорему только для этих случаев, но в более общей, на первый взгляд, формулировке:

В любом подмножестве $\mathfrak{M}$ кольца $\mathfrak{o}$ (не только в любом идеале) существует такой конечный набор элементов $m_1, \ldots, m_r$, что любой элемент m из $\mathfrak{M}$ представляется в виде

$$\lambda_1 m_1 + \ldots + \lambda_r m_r \qquad (\lambda_i \in \mathfrak{o}).$$

Эта теорема является, однако, непосредственным следствием теоремы о базисе для идеалов. В самом деле, если $\mathfrak{A}$ — идеал, порожденный множеством $\mathfrak{M}$, то $\mathfrak{A}$ обладает базисом:

$$\mathfrak{A} = (a_1, \ldots, a_s).$$

Каждый элемент a_i (как элемент идеала, порожденного множеством $\mathfrak{M}$) выражается через конечный набор элементов из $\mathfrak{M}$:

$$a_i = \sum_k \lambda_{ik} m_{ik}.$$

Следовательно, все элементы из $\mathfrak{A}$ линейно зависят от конечного набора элементов m_{ik}; в частности, это относится и к элементам из $\mathfrak{M}$.

Более важным является то обстоятельство, что теорема о базисе эквивалентна следующей «теореме о цепях делителей»:

Теорема о цепях делителей. Первая формулировка. *Если $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ — цепочка идеалов кольца $\mathfrak{o}$ и $\mathfrak{a}_{i+1}$ — собственный делитель идеала $\mathfrak{a}_i$:*

$$\mathfrak{a}_i \subset \mathfrak{a}_{i+1},$$

то цепь обрывается после конечного числа членов.

Иначе говоря, имеет место

Теорема о цепях делителей. Вторая формулировка. *Если $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ — бесконечная цепь делителей:*

$$\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1},$$

то, начиная с некоторого n, все $\mathfrak{a}_i$ должны быть равны:

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$$

То, что теорема о цепях делителей следует из теоремы о базисе, можно установить так:

Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots$ — бесконечная цепь и $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$. Объединение $\mathfrak{v}$ всех идеалов $\mathfrak{a}_i$ является некоторым идеалом, потому что если a и b лежат в $\mathfrak{v}$ и, скажем, a принадлежит $\mathfrak{a}_n$, а b принадлежит $\mathfrak{a}_m$, то a и b лежат в $\mathfrak{a}_N$, где N — наибольшее из чисел n и m; следовательно, $a-b$ лежит в $\mathfrak{a}_N$, а потому и в $\mathfrak{v}$. Если же a — произвольный элемент из $\mathfrak{v}$, взятый, например, из $\mathfrak{a}_n$, то λa лежит в $\mathfrak{a}_n$, а потому и в $\mathfrak{v}$.

Согласно условию идеал $\mathfrak{v}$ имеет конечный базис $(a_1, \dots, a_r)$. Каждый из элементов a_i лежит в некотором идеале $\mathfrak{a}_{n_i}$. Если n — наибольшее из чисел n_i, то все $a_1, \dots, a_r$ лежат в одном идеале $\mathfrak{a}_n$. Так как элементы из $\mathfrak{v}$ линейно выражаются через $a_1, \dots, a_r$, то все элементы из $\mathfrak{v}$ лежат в $\mathfrak{a}_n$, а отсюда следует, что

$$\mathfrak{v} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \dots$$

Наоборот, теорема о базисе следует из теоремы о цепях делителей. Действительно, пусть $\mathfrak{a}$ — идеал и a_1 — произвольный элемент из $\mathfrak{a}$. Если a_1 не порождает весь идеал, то в $\mathfrak{a}$ существуют элементы, не принадлежащие (a_1); пусть a_2 — один из этих элементов. Тогда

$$(a_1) \subset (a_1, a_2).$$

Если a_1 и a_2 все еще не порождают весь идеал $\mathfrak{a}$, то точно так же отыскивается третий элемент $a_3 \in \mathfrak{a}$, не принадлежащий (a_1, a_2), и т. д. Получается цепь делителей

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \dots$$

Но она обрывается после конечного числа (скажем, после r) шагов:

$$(a_1, a_2, \dots, a_r) = \mathfrak{a}.$$

Следовательно, идел $\mathfrak{a}$ имеет конечный базис.

Если теорема о целях делителей имеет место в кольце $\mathfrak{o}$, то она справедлива и в любом факторкольце $\mathfrak{o}/\mathfrak{a}$.

Доказательство. Любой идеал $\bar{\mathfrak{b}}$ в $\mathfrak{o}/\mathfrak{a}$ является некоторым множеством классов вычетов. Если составить объединение этих классов вычетов, то получится некоторый идеал $\mathfrak{b}$ в $\mathfrak{o}$. Наоборот, идеал $\mathfrak{b}$ однозначно определяет идеал $\bar{\mathfrak{b}}$:

$$\bar{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}.$$

Любая цепь идеалов $\bar{\mathfrak{b}}_1 \subset \bar{\mathfrak{b}}_2 \subset \bar{\mathfrak{b}}_3 \subset \dots$ в кольце $\mathfrak{o}/\mathfrak{a}$ задает таким способом некоторую цепь идеалов $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \dots$ в кольце $\mathfrak{o}$,

а так как последняя обрывается на одной из своих компонент, то первая цепь также конечна.

Тем самым доказано сформулированное в начале этого параграфа утверждение о том, что если теорема о базисе выполняется в кольце o, то она выполняется и в кольце o/a.

Теорема о цепях делителей имеет еще две формулировки, удобные для приложений:

Теорема о цепях делителей. Третья формулировка: условие максимальности. *Если в кольце o имеет место теорема о цепях делителей, то в любом непустом множестве идеалов существует максимальный идеал, т. е. такой идеал, который не содержится ни в одном другом идеале данного множества.*

Доказательство. Фиксируем в каждом непустом множестве идеалов какой-нибудь идеал. Если бы в некотором множестве $\mathfrak{M}$ не было максимального идеала, то любой из идеалов этого множества содержался бы в одном из других идеалов этого же множества. Возьмем в $\mathfrak{M}$ фиксированный в нем с самого начала идеал a_1, затем в множестве тех идеалов из $\mathfrak{M}$, которые содержат a_1 и не совпадают с a_1, возьмем фиксированный для этого множества идеал a_2 и т. д. В результате получится бесконечная цепь

$$a_1 \subset a_1 \subset a_3 \subset \ldots,$$

что, согласно условию, невозможно.

Теорема о цепях делителей. Четвертая формулировка: принцип индукции по делителям. *Если в кольце o имеет место теорема о цепях делителей и можно доказать наличие некоторого свойства E у каждого идеала a (в частности, у единичного идеала) в предположении, что это верно для всех собственных делителей идеала a, то свойством E обладает каждый идеал данного кольца.*

Доказательство. Предположим, что некоторый идеал не обладает свойством E. Тогда, в соответствии с третьей формулировкой теоремы о цепях делителей, существует максимальный идеал a, не обладающий свойством E. В силу максимальности все собственные делители идеала a должны обладать свойством E, а потому им должен обладать и идеал a. Получили противоречие.

§ 116. Произведения и частные идеалов

Как и в § 16, под *наибольшим общим делителем* (НОД) или *суммой* идеалов a, b, ... мы подразумеваем идеал $(a, b, \ldots)$, порожденный объединением (в теоретико-множественном смысле) идеалов a, b, ...; точно так же под *наименьшим общим кратным* (НОК)

этих идеалов мы подразумеваем пересечение $[\mathfrak{a}, \mathfrak{b}, \ldots] = \mathfrak{a} \cap \mathfrak{b} \cap \ldots$ Обозначение, используемое для суммы идеалов, сохраняется и для идеала, порожденного несколькими идеалами и несколькими элементами; например,

$$(\mathfrak{a}, b) = (\mathfrak{a}, (b)).$$

Само собой разумеется, что $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a})$, $((\mathfrak{a}, \mathfrak{b}), \mathfrak{c}) = (\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})) = (\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ и т. д. Далее,

$$((a_1, a_2, \ldots), (b_1, b_2, \ldots)) = (a_1, a_2, \ldots, b_1, b_2, \ldots)$$

или, словами: *базис наибольшего общего делителя получается объединением базисов отдельных идеалов.*

Если элементы одного идеала $\mathfrak{a}$ перемножить с элементами другого идеала $\mathfrak{b}$, то произведения ab в общем случае не составят идеала. Идеал, порожденный этими произведениями ab, называется *произведением* идеалов $\mathfrak{a}$, $\mathfrak{b}$ и обозначается через $\mathfrak{a} \cdot \mathfrak{b}$ или $\mathfrak{ab}$. Он состоит из всевозможных сумм $\sum a_i b_i$ $(a_i \in \mathfrak{a},\ b_i \in \mathfrak{b})$.

Очевидно, что

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a},$$
$$(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c});$$

следовательно, с произведениями идеалов можно обращаться так же, как с обычными произведениями чисел. В частности, имеет смысл говорить о *степени* $\mathfrak{a}^\rho$ идеала $\mathfrak{a}$; она определяется так:

$$\mathfrak{a}^1 = \mathfrak{a}; \quad \mathfrak{a}^{\rho+1} = \mathfrak{a} \cdot \mathfrak{a}^\rho.$$

Если $\mathfrak{a} = (a_1, \ldots, a_n)$ и $\mathfrak{b} = (b_1, \ldots, b_m)$, то, очевидно, произведение $\mathfrak{ab}$ порождается произведениями $a_i b_k$. *Таким образом, мы получаем некоторый базис произведения, умножая все базисные элементы одного идеала-сомножителя на все базисные элементы другого идеала-сомножителя.*

В частности, для главных идеалов имеет место равенство

$$(a) \cdot (b) = (ab).$$

Таким образом, для элементов кольца произведение, которое только что было определено, совпадает с обычным произведением.

Произведение $\mathfrak{a} \cdot (b)$ произвольного идеала и главного идеала состоит из всех произведений ab, где a пробегает множество элементов из $\mathfrak{a}$. В этом случае пишут просто $\mathfrak{a}b$ или $b\mathfrak{a}$.

Следующее правило — «закон дистрибутивности для идеалов»:

$$\mathfrak{a} \cdot (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{c}). \tag{1}$$

Вот его доказательство. Произведение $\mathfrak{a} \cdot (\mathfrak{b}, \mathfrak{c})$ порождается произведениями $a(b + c)$, которые в силу равенства

$$a(b + c) = ab + ac,$$

принадлежат идеалу $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$; наоборот, идеал $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$ порождается произведениями ab и произведениями ac, принадлежащими идеалу $\mathfrak{a}\cdot(\mathfrak{b},\ \mathfrak{c})$.

Правило, такое же, как (1), имеет место и тогда, когда в скобках вместо $\mathfrak{b}$, $\mathfrak{c}$ стоят несколько или даже бесконечное множество идеалов.

Так как все произведения ab лежат в $\mathfrak{a}$, то справедливо включение

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{a}$$

и точно так же

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{b}.$$

Отсюда следует, что

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq[\mathfrak{a},\ \mathfrak{b}],$$

или: *произведение делится на наименьшее общее кратное.*

В кольце целых чисел произведение наименьшего общего кратного и наибольшего общего делителя двух идеалов $\mathfrak{a}$ и $\mathfrak{b}$ равно произведению $\mathfrak{ab}$. Это справедливо не в любом кольце. Однако в общем случае имеет место соотношение:

$$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\ \mathfrak{b})\subseteq\mathfrak{ab}. \tag{2}$$

Доказательство.

$$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\ \mathfrak{b})=([\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{a},\ [\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{b})\subseteq(\mathfrak{b}\cdot\mathfrak{a},\ \mathfrak{a}\cdot\mathfrak{b})=\mathfrak{a}\cdot\mathfrak{b}.$$

Идеал $\mathfrak{o}$, состоящий из всех элементов рассматриваемого кольца, называется *единичным идеалом*. Разумеется, справедливо включение

$$\mathfrak{a}\cdot\mathfrak{o}\subseteq\mathfrak{a}.$$

Если же $\mathfrak{o}$ содержит единичный элемент e, то имеет место и обратное включение

$$\mathfrak{a}=\mathfrak{a}\cdot e\subseteq\mathfrak{a}\cdot\mathfrak{o}.$$

Таким образом,

$$\mathfrak{a}\cdot\mathfrak{o}=\mathfrak{a}.$$

Тем самым идеал $\mathfrak{o}$ играет в рассматриваемой ситуации роль единичного элемента относительно умножения. Он порожден в этом случае единичным элементом кольца.

Всегда выполнены следующие равенства:

$$(\mathfrak{a},\ \mathfrak{o})=\mathfrak{o};\quad \mathfrak{a}\cap\mathfrak{o}=\mathfrak{a}.$$

Под *частным* $\mathfrak{a}:\mathfrak{b}$, где $\mathfrak{a}$ — некоторый идеал, мы подразумеваем совокупность тех элементов γ из $\mathfrak{o}$, для которых

$$\gamma b\equiv 0\,(\mathfrak{a})\quad\text{при всех}\quad b\ \text{из}\ \mathfrak{b}. \tag{3}$$

Эта совокупность является идеалом, потому что если γ и δ обладают свойством (3), то и элемент $\gamma-\delta$ обладает этим свойством,

и если свойством (3) обладает элемент γ, то им обладает и любое произведение $r\gamma$. При этом предполагается, что $\mathfrak{a}$ — идеал; относительно $\mathfrak{b}$ такое предположение не обязательно: множество $\mathfrak{b}$ может быть произвольным и даже состоящим из одного-единственного элемента.

Если $\mathfrak{a}$ и $\mathfrak{b}$ — идеалы, то из определения следует, что

$$\mathfrak{b}\cdot(\mathfrak{a}:\mathfrak{b})\subseteq\mathfrak{a}.$$

В кольце целых чисел конструкция частного двух главных идеалов (a), $(b)\neq 0$ проводится так: множители, участвующие в разложении числа a и делящие b, отбрасываются; например,

$$(12):(2)=(6),$$
$$(12):(4)=(3),$$
$$(12):(8)=(3),$$
$$(12):(5)=(12).$$

Иначе говоря: число a делится в обычном смысле на наибольший общий делитель (a, b).

В кольцах общего вида выполняется соответствующее этому наблюдению правило:

$$\mathfrak{a}:\mathfrak{b}=\mathfrak{a}:(\mathfrak{a},\ \mathfrak{b}),$$

которое легко доказывается, но не является особенно важным.

Очевидно, имеет место включение $\mathfrak{a}\subseteq(\mathfrak{a}:\mathfrak{b})$, так как каждый элемент из $\mathfrak{a}$ обладает свойством (3). Таким образом, есть два крайних случая:

$$\mathfrak{a}:\mathfrak{b}=\mathfrak{o}\quad\text{и}\quad\mathfrak{a}:\mathfrak{b}=\mathfrak{a}.$$

Первый случай встречается, когда $\mathfrak{b}\subseteq\mathfrak{a}$, потому что тогда для каждого γ выполнены сравнения

$$\gamma\mathfrak{b}\equiv 0\,(\mathfrak{b})\equiv 0\,(\mathfrak{a}).$$

Второй случай встречается, когда из $\gamma\mathfrak{b}\equiv 0\,(\mathfrak{a})$ следует, что $\gamma\equiv 0\,(\mathfrak{a})$. Тем самым сравнение $\gamma\mathfrak{b}\equiv 0\,(\mathfrak{a})$ можно тогда делить на $\mathfrak{b}$. В этом случае говорят, что идеал $\mathfrak{b}$ *прост относительно* $\mathfrak{a}$; мы, однако, редко будем употреблять этот термин, который может привести к путанице, а будем писать $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$. В случае целых чисел a и b, отличных от нуля, утверждение:

$$\text{из } \gamma b\equiv 0\,(a)\quad\text{следует}\quad\gamma\equiv 0\,(a),$$

справедливо, очевидно, лишь тогда, когда a и b не имеют общих множителей. В более общих случаях предикат «прост относительно» *не симметричен*; например, если $\mathfrak{a}$ — простой идеал, а $\mathfrak{b}$ — отличный от $\mathfrak{o}$ идеал, являющийся собственным простым дели-

телем идеала $\mathfrak{a}$, то

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a} \quad \text{и} \quad \mathfrak{b} \text{ прост относительно } \mathfrak{a},$$

но

$$\mathfrak{b} : \mathfrak{a} = \mathfrak{o} \quad \text{и} \quad \mathfrak{a} \text{ не прост относительно } \mathfrak{b}.$$

Например,

$$(0) : (2) = (0),$$
$$(2) : (0) = (1).$$

Важным является следующее соотношение:

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_r] : \mathfrak{b} = [\mathfrak{a}_1 : \mathfrak{b}, \ldots, \mathfrak{a}_r : \mathfrak{b}]. \tag{4}$$

Доказательство. Из

$$\gamma\mathfrak{b} \subseteq [\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$$

следует, что

$$\gamma\mathfrak{b} \subseteq \mathfrak{a}_i \quad \text{для каждого} \quad i,$$

и обратно.

Задача 1. Доказать соотношения:

$$(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{b}\mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b},$$
$$\mathfrak{a} : (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c}).$$

Задача 2. Доказать равносильность трех уравнений:
а) $\mathfrak{a} : \mathfrak{b}_1 = \mathfrak{a}$ и $\mathfrak{a} : \mathfrak{b}_2 = \mathfrak{a}$;
б) $\mathfrak{a} : [\mathfrak{b}_1 \cap \mathfrak{b}_2] = \mathfrak{a}$;
в) $\mathfrak{a} : \mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{a}$.

§ 117. Простые идеалы и примарные идеалы

Ранее мы определили простые идеалы как идеалы, кольцо классов вычетов которых не имеет делителей нуля.

В кольце целых чисел каждое натуральное число a является произведением степеней различных простых чисел:

$$a = p_1^{\sigma_1} \ldots p_r^{\sigma_r}, \tag{1}$$

а потому каждый идеал (a) является произведением степеней простых идеалов:

$$(a) = (p_1)^{\sigma_1} \ldots (p_r)^{\sigma_r}.$$

В кольцах общего вида нельзя ожидать столь простых теорем о разложении идеалов. Например, в кольце целочисленных многочленов от одной переменной x идеал $(4, x)$, не являющийся простым, имеет, кроме единичного идеала $\mathfrak{o}$, лишь один простой делитель $(2, x)$, но не равен никакой степени идеала $(2, x)$. Таким образом, в общем случае нельзя ожидать представления идеалов в виде произведений; самое большее, что можно ожидать, это представление идеалов в виде наименьших общих кратных

(пересечений) по возможности простых компонент [1]) в соответствии с тем представлением, которое дает (1) для идеала (a) как наименьшего общего кратного:

$$(a) = \left[\left(p_1^{\sigma_1}\right), \ldots, \left(p_r^{\sigma_r}\right)\right].$$

Входящие в это представление идеалы (p^σ) обладают следующим одним характерным свойством: если произведение ab делится на p^σ, а один из сомножителей, скажем a, не делится на p^σ, то другой сомножитель b должен содержать по крайней мере какой-либо делитель элемента p^σ. Это означает, что некоторая степень b^ρ должна делиться на p^σ. Итак, из

$$ab \equiv 0\ (p^\sigma),$$
$$a \not\equiv 0\ (p^\sigma)$$

следует, что

$$b^\rho \equiv 0\ (p^\sigma).$$

Идеалы с таким свойством будут называться *примарными*.

Идеал $\mathfrak{q}$ *называется примарным, если из*

$$ab \equiv 0\ (\mathfrak{q}), \quad a \not\equiv 0\ (\mathfrak{q})$$

следует существование такого ρ, *что*

$$b^\rho \equiv 0\ (\mathfrak{q}).$$

Это определение можно высказать и так:

Если в кольце классов вычетов по идеалу $\mathfrak{q}$ *имеет место равенство* $\bar{a}\bar{b} = 0$ *и* $\bar{a} \neq 0$, *то некоторая степень* $\bar{b}^\rho$ *должна быть равна нулю.*

Если $\bar{a}\bar{b} = 0$ и $\bar{a} \neq 0$, то это означает, что $\bar{b}$ — делитель нуля. Если некоторая степень b^ρ элемента равна нулю, то элемент b называется *нильпотентным*. Таким образом,

Идеал является примарным, если в кольце классов вычетов по нему каждый делитель нуля нильпотентен.

Как видим, это определение — небольшая модификация определения простого идеала; в кольце классов вычетов по простому идеалу каждый делитель нуля должен быть не только нильпотентным, но и равным нулю.

Мы увидим, что примарные идеалы в кольцах общего вида играют ту же роль, что и степени простых чисел в кольце целых чисел, а именно: при очень общих предположениях каждый идеал

---

[1]) Представление в виде наименьшего общего кратного в ряде случаев естественнее, чем представление произведением, а именно, когда нужно выяснить, делится ли данный элемент b на идеал $\mathfrak{m}$, т. е. принадлежит ли он $\mathfrak{m}$. Если $\mathfrak{m} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$, то b принадлежит $\mathfrak{m}$ тогда и только тогда, когда b содержится в каждом $\mathfrak{a}_\nu$.

представляется как пересечение примарных идеалов и в этом представлении проявляются важнейшие структурные свойства идеалов.

Примарные идеалы не обязаны быть степенями простых идеалов, как показывает приведенный в начале пример идеала $(4, x)$, который, очевидно, примарен. Обратное также неверно; например, в кольце целочисленных многочленов $a_0+a_1x+\ldots+a_nx^n$, у которых a_1 делится на 3, идеал $\mathfrak{p}=(3x, x^2, x^3)$ простой, но $\mathfrak{p}^2=(9x^2, 3x^3, x^4, x^5, x^6)$ не примарный, потому что

$$9\cdot x^2\equiv 0\,(\mathfrak{p}^2),$$
$$x^2\not\equiv 0\,(\mathfrak{p}^2),$$
$$9^\rho\not\equiv 0\,(\mathfrak{p}^2)$$

для каждого ρ.

Свойства примарных идеалов, не зависящие от теоремы о цепях делителей

I. *Для каждого примарного идеала $\mathfrak{q}$ существует простой идеал $\mathfrak{p}$, делящий его и определяемый следующим образом: $\mathfrak{p}$ является совокупностью тех элементов b, для каждого из которых некоторая степень b^ρ принадлежит $\mathfrak{q}$.*

Доказательство. 1. Множество $\mathfrak{p}$ — идеал, потому что из $b^\rho\equiv 0\,(\mathfrak{q})$ следует, что $(rb)^\rho\equiv 0\,(\mathfrak{q})$, и из $b^\rho\equiv 0\,(\mathfrak{q})$ и $c^\sigma\equiv 0\,(\mathfrak{q})$ следует (ввиду того, что в выражении $(b-c)^{\rho+\sigma-1}$ после раскрытия скобок каждое слагаемое содержит либо b^ρ либо c^σ) сравнение

$$(b-c)^{\rho+\sigma-1}\equiv 0\,(\mathfrak{q}).$$

2. Идеал $\mathfrak{p}$ прост, потому что из

$$ab\equiv 0\,(\mathfrak{p}),$$
$$a\not\equiv 0\,(\mathfrak{p})$$

следует, что существует ρ, для которого

$$a^\rho b^\rho\equiv 0\,(\mathfrak{q})$$

и

$$a^\rho\not\equiv 0\,(\mathfrak{q}).$$

Следовательно, нужно взять такое σ, что

$$b^{\rho\sigma}\equiv 0\,(\mathfrak{q}).$$

Отсюда следует, что

$$b\equiv 0\,(\mathfrak{p}).$$

3. Идеал $\mathfrak{p}$ является делителем идеала $\mathfrak{q}$:

$$\mathfrak{q}\equiv 0\,(\mathfrak{p});$$

в самом деле, элементы из $\mathfrak{q}$, конечно, таковы, что некоторые их степени лежат в $\mathfrak{a}$.

Идеал $\mathfrak{p}$ называется *простым идеалом, ассоциированным с примарным идеалом* $\mathfrak{a}$; идеал же $\mathfrak{q}$ называют *ассоциированным с идеалом* $\mathfrak{p}$ *примарным идеалом*. Из определения примарного идеала следует:

II. *Если* $ab \equiv 0\,(\mathfrak{q})$ *и* $a \not\equiv 0\,(\mathfrak{q})$, *то* $b \equiv 0\,(\mathfrak{p})$.

В некотором смысле обращение этого предложения таково:

III. *Пусть* $\mathfrak{p}$ *и* $\mathfrak{q}$ *— идеалы, обладающие следующими свойствами*:

1) *из* $ab \equiv 0\,(\mathfrak{q})$ *и* $a \not\equiv 0\,(\mathfrak{q})$ *следует, что* $b \equiv 0\,(\mathfrak{p})$;

2) $\mathfrak{q} \equiv 0\,(\mathfrak{p})$;

3) *из* $b \equiv 0\,(\mathfrak{p})$ *следует, что* $b^{\rho} \equiv 0\,(\mathfrak{q})$ *для некоторого* ρ;

тогда идеал $\mathfrak{q}$ *примарный, а* $\mathfrak{p}$ *— ассоциированный с ним простой идеал.*

Доказательство. Из $ab \equiv 0\,(\mathfrak{q})$ и $a \not\equiv 0\,(\mathfrak{q})$ следует (в силу 1) и 3)), что $b^{\rho} \equiv 0\,(\mathfrak{q})$. Поэтому $\mathfrak{q}$ — примарный идеал. Остается лишь показать, что $\mathfrak{p}$ состоит из таких элементов b, что некоторая степень b^{ρ} лежит в $\mathfrak{q}$. Половина этого утверждения заключена в условии 3). Остается показать, что из $b^{\rho} \equiv 0\,(\mathfrak{q})$ вытекает $b \equiv 0\,(\mathfrak{p})$. Пусть ρ — наименьшее натуральное число, для которого $b^{\rho} \equiv 0\,(\mathfrak{q})$. Для $\rho = 1$ все следует из условия 2). Для $\rho > 1$ имеем: $b \cdot b^{\rho-1} \equiv 0\,(\mathfrak{q})$, но $b^{\rho-1} \not\equiv 0\,(\mathfrak{q})$, откуда (в силу 1)) $b \equiv 0\,(\mathfrak{p})$.

Эта теорема облегчает доказательство примарности и отыскание ассоциированных простых идеалов в частных случаях; кроме того, теорема показывает, какими свойствами ассоциированный простой идеал определяется однозначно.

Свойство II имеет место и тогда, когда a и b заменяются на идеалы $\mathfrak{a}$ и $\mathfrak{b}$:

IV. *Из* $\mathfrak{ab} \equiv 0\,(\mathfrak{q})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ *следует, что* $\mathfrak{b} \equiv 0\,(\mathfrak{p})$.

Действительно, если бы было $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$, то нашелся бы элемент b в идеале $\mathfrak{b}$, не принадлежащий идеалу $\mathfrak{p}$, и, точно так же, элемент a из $\mathfrak{a}$, не принадлежащий идеалу $\mathfrak{q}$. Произведение ab должно, однако, лежать в $\mathfrak{ab}$, а потому и в $\mathfrak{a}$, что противоречит доказанному ранее.

Точно так же доказывается соответствующее утверждение для простых идеалов:

из $\mathfrak{ab} \equiv 0\,(\mathfrak{p})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{p})$ *следует, что* $\mathfrak{b} \equiv 0\,(\mathfrak{p})$.

Вот одно следствие отсюда (получается $(h-1)$-кратным применением доказанного):

из $\mathfrak{a}^h \equiv 0\,(\mathfrak{p})$ *следует, что* $\mathfrak{a} \equiv 0\,(\mathfrak{p})$.

Другая формулировка предложения IV такова:

IV′. *Из* $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$ *следует, что* $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$.

В кольце классов вычетов $\mathfrak{o}/\mathfrak{q}$ лежит идеал $\mathfrak{p}/\mathfrak{q}$ (в силу $\mathfrak{p} \supseteq \mathfrak{a}$). Он состоит из всех нильпотентных элементов, а в случае $\mathfrak{q} \neq \mathfrak{o}$ из всех делителей нуля.

Свойства примарных идеалов в предположении справедливости теоремы о цепях делителей

Если $\mathfrak{p}$ — простой идеал, ассоциированный с $\mathfrak{q}$, то некоторая степень каждого из элементов идеала $\mathfrak{p}$ лежит в идеале $\mathfrak{q}$. Наименьшая из этих степеней зависит от выбираемых элементов и может неограниченно расти. Если же предположить, что в кольце o выполнена теорема о цепях делителей, то степень не может расти неограниченно, о чем говорит следующая теорема:

V. *Некоторая степень* $\mathfrak{p}^\rho$ *делится на* $\mathfrak{q}$:

$$\mathfrak{p}^\rho \equiv 0\,(\mathfrak{q}).$$

Доказательство. Пусть $(p_1, \ldots, p_r)$ — некоторый базис идеала $\mathfrak{p}$. Пусть в идеале $\mathfrak{q}$ лежат степени $p_1^{\rho_1}, \ldots, p_r^{\rho_r}$. Положим

$$\rho = \sum_1^r (\rho_i - 1) + 1;$$

тогда $\mathfrak{p}^\rho$ будет порождаться всевозможными произведениями элементов p_i по ρ штук в каждом из таких произведений. В каждом из этих произведений по крайней мере один из сомножителей p_i встречается более $(\rho_i - 1)$ раз, т. е. не менее ρ_i раз. Следовательно, все образующие идеала $\mathfrak{p}^\rho$ лежат в $\mathfrak{q}$, откуда и получается требуемое.

Итак, между примарным идеалом $\mathfrak{q}$ и ассоциированным с ним простым идеалом $\mathfrak{p}$ выполняются следующие соотношения:

$$\left.\begin{aligned} \mathfrak{q} &\equiv 0\,(\mathfrak{p}), \\ \mathfrak{p}^\rho &\equiv 0\,(\mathfrak{q}). \end{aligned}\right\} \tag{2}$$

Наименьшее число ρ, для которого выполняются эти соотношения, называется *показателем* идеала $\mathfrak{q}$. Показатель задает, в частности, верхнюю границу показателей тех степеней, в которые (по меньшей мере) нужно возвести элементы из $\mathfrak{p}$, чтобы получить элементы из $\mathfrak{q}$.

Если идеал $\mathfrak{q}$ примарен, то соотношения (2) являются характеристическими для ассоциированного простого идеала $\mathfrak{p}$. В самом деле, если другой простой идеал $\mathfrak{p}'$ также удовлетворяет соотношениям (2) при показателе ρ', то

$$\mathfrak{p}^\rho \subseteq \mathfrak{q} \subseteq \mathfrak{p}' \text{ и, следовательно, } \mathfrak{p} \subseteq \mathfrak{p}',$$
$$\mathfrak{p}'^{\rho'} \subseteq \mathfrak{q} \subseteq \mathfrak{p} \text{ и, следовательно, } \mathfrak{p}' \subseteq \mathfrak{p};$$

тем самым, $\mathfrak{p}' = \mathfrak{p}$.

VI. *Из* $\mathfrak{ab} \equiv 0\,(\mathfrak{q})$ *и* $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ *следует, что для некоторого* σ *имеет место соотношение*: $\mathfrak{b}^\sigma \equiv 0\,(\mathfrak{q})$.

Доказательство. Достаточно взять $\sigma = \rho$. Из $\mathfrak{ab} \equiv 0\,(\mathfrak{q})$ и $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ следует, как это было доказано раньше, что $\mathfrak{b} \equiv 0\,(\mathfrak{p})$

и потому

$$\mathfrak{b}^{\rho} \equiv 0\ (\mathfrak{p}^{\rho}) \equiv 0\ (\mathfrak{q}).$$

Идеал $\mathfrak{q}$ с только что описанным свойством называется *сильно примарным*, в противоположность определенным ранее *слабо примарным* или просто примарным идеалам. В случае выполнимости теоремы о цепях делителей оба эти понятия совпадают, потому что, как мы уже видели, примарные идеалы при этом являются сильно примарными, а обратное легко следует из возможности сведения идеалов $\mathfrak{a}$, $\mathfrak{b}$ к главным идеалам (a), (b). Если же теорема о цепях делителей не имеет места, то, хотя каждый сильно примарный идеал и является слабо примарным, обратное не всегда верно. См. реферат работы: Вальфиш (Walfisch A.). Über primäre Ideale. — Math. Rev., 1944, 5, S. 226.

Задача 1. Идеал $\mathfrak{a}=(x^2, 2x)$ в кольце целочисленных многочленов от одной переменной x не является примарным. Вместе с тем имеет место соотношение $(x^2) \subset \mathfrak{a} \subset (x)$ и идеал (x) простой.

Задача 2. Если в кольце $\mathfrak{o}$ есть единица, то само $\mathfrak{o}$ является единственным примарным идеалом, ассоциированным с простым идеалом $\mathfrak{o}$.

§ 118. Общая теорема о разложении

Начиная с этого места, будем считать, что $\mathfrak{o}$ — нётерово кольцо. Следовательно, в кольце $\mathfrak{o}$ будут иметь место теорема о базисе, теорема о цепях делителей, условие максимальности и принцип индукции по делителям.

Идеал $\mathfrak{m}$ называется *приводимым*, если он представляется в виде пересечения двух своих собственных делителей:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

Если же такое представление невозможно, то идеал называется *неприводимым*.

Примерами неприводимых идеалов служат простые идеалы; действительно, если бы для какого-то простого идеала $\mathfrak{p}$ оказалось выполненным равенство

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{p}, \quad \mathfrak{b} \supset \mathfrak{p},$$

то были бы справедливы соотношения

$$\mathfrak{ab} \equiv 0\ (\mathfrak{a} \cap \mathfrak{b}) \equiv 0\ (\mathfrak{p}), \quad \mathfrak{a} \not\equiv 0\ (\mathfrak{p}), \quad \mathfrak{b} \not\equiv 0\ (\mathfrak{p}),$$

что противоречит свойствам простого идеала.

В силу теоремы о цепях делителей, которая имеет место в рассматриваемой ситуации, оказывается выполненной

Первая теорема о разложении. *Каждый идеал является пересечением конечного множества неприводимых идеалов.*

Доказательство. Для неприводимых идеалов теорема верна. Пусть, таким образом, $\mathfrak{m}$ — приводимый идеал:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

Если считать доказываемую теорему верной для всех собственных делителей идеала $\mathfrak{m}$, то она будет верна, в частности, для

идеалов $\mathfrak{a}$ и $\mathfrak{b}$; пусть таким образом,

$$\mathfrak{a} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s],$$
$$\mathfrak{b} = [\mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r].$$

Отсюда следует, что

$$\mathfrak{m} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s, \mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r],$$

т. е. теорема верна и для идеала $\mathfrak{m}$. Так как она справедлива и для единичного идеала (всегда неприводимого), то в силу принципа индукции по делителям теорема верна в общем случае.

От представления с помощью неприводимых идеалов мы перейдем к представлению примарными идеалами.

Каждый неприводимый идеал примарен.

Доказательство. Пусть идеал $\mathfrak{m}$ не является примарным. Нужно показать, что $\mathfrak{m}$ приводим.

Так как $\mathfrak{m}$ непримарен, то существуют такие два элемента a, b, что

$$ab \equiv 0\ (\mathfrak{m}),$$
$$a \not\equiv 0\ (\mathfrak{m}),$$
$$b^\rho \not\equiv 0\ (\mathfrak{m}) \quad \text{для каждого } \rho.$$

В силу теоремы о цепях делителей ряд частных идеалов

$$\mathfrak{m} : b,\ \mathfrak{m} : b^2,\ \ldots$$

должен на каком-то шаге оборваться, т. е. для некоторого k должно быть выполнено равенство

$$\mathfrak{m} : b^k = \mathfrak{m} : b^{k+1}.$$

Мы утверждаем теперь, что

$$\mathfrak{m} = (\mathfrak{m},\ a) \cap (\mathfrak{m},\ \mathfrak{o}b^k). \tag{1}$$

Оба идеала в правой части являются делителями идеала $\mathfrak{m}$ и эти делители собственные, так как первый из них содержит элемент a, а второй — степень b^{k+1}. Мы должны показать, что каждый общий элемент этих двух идеалов обязательно принадлежит $\mathfrak{m}$. Любой такой элемент c, являясь элементом идеала $(\mathfrak{m},\ \mathfrak{o}b^k)$, должен иметь вид

$$c = m + rb^k;$$

с другой стороны, как элемент идеала $(\mathfrak{m},\ a)$, элемент c обладает свойством

$$cb \equiv 0\ (\mathfrak{m}b,\ ab) \equiv 0\ (\mathfrak{m}).$$

Отсюда следует, что

$$mb + rb^{k+1} = cb \equiv 0\ (\mathfrak{m}),$$
$$rb^{k+1} \equiv 0\ (\mathfrak{m}),$$

откуда в силу равенства $\mathfrak{m} : b^{k+1} = \mathfrak{m} : b^k$ получаем

$$rb^k \equiv 0 \ (\mathfrak{m}),$$
$$c = m + rb^k \equiv 0 \ (\mathfrak{m}).$$

Тем самым доказано (1), т. е. идеал $\mathfrak{m}$ оказался приводимым.

Так как каждый идеал представляется пересечением конечного множества неприводимых идеалов, а каждый неприводимый идеал примарен, то:

Каждый идеал представляется в виде пересечения конечного множества примарных идеалов.

Эту теорему можно усилить. Прежде всего, из представления

$$\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r]$$

можно исключить идеалы $\mathfrak{q}_i$, которые содержат пересечения остальных. Так получится *несократимое* представление, т. е. представление, в котором ни одна из составляющих не содержит пересечение остальных. Может оказаться, что в таком представлении некоторые примарные компоненты задают вновь примарный идеал, т. е. пересечение этих примарных компонент вновь примарно. Следующие предложения показывают, когда этот случай имеет место:

1. Пересечение конечного множества примарных идеалов, ассоциированных с одним простым идеалом, является вновь примарным идеалом, ассоциированным с тем же простым идеалом.

2. Несократимое пересечение конечного множества примарных идеалов, не ассоциированных с одним и тем же простым идеалом, не является примарным.

Эти теоремы выполняются независимо от теоремы о цепях делителей.

Доказательство предложения 1. Пусть

$$\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r],$$

где $\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r$ ассоциированы с идеалом $\mathfrak{p}$. Мы будем основываться на теореме III (§ 117). Из

$$ab \equiv 0 \ (\mathfrak{m}), \quad a \not\equiv 0 \ (\mathfrak{m})$$

следует, что

$$ab \equiv 0 \ (\mathfrak{q}_\nu)$$

для всех ν и

$$a \not\equiv 0 \ (\mathfrak{q}_\nu)$$

по крайней мере для одного ν, а отсюда получается, что $b \equiv 0 \ (\mathfrak{p})$.

Далее, очевидно, что

$$\mathfrak{m} \equiv 0 \ (\mathfrak{q}_\nu) \equiv 0 \ (\mathfrak{p}).$$

Наконец, если $b \equiv 0 \ (\mathfrak{p})$, то

$$b^{\omega_\nu} \equiv 0 \ (\mathfrak{q}_\nu) \quad \text{для всех } \nu;$$

следовательно, если $\rho = \max \rho_\nu$, то

$$b^\rho \equiv 0\,(\mathfrak{q}_\nu) \quad \text{для всех } \nu,$$
$$b^\rho \equiv 0\,(\mathfrak{m}).$$

Тем самым все свойства, перечисленные в теореме III, налицо. Поэтому идеал $\mathfrak{m}$ примарен и $\mathfrak{p}$ — ассоциированный простой идеал.

Доказательство предложения 2. Пусть дано несократимое представление

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] \quad (r \geqslant 2),$$

в котором по крайней мере два ассоциированных простых идеала $\mathfrak{p}_\nu$ различны. Мы будем считать с самого начала, что каждая группа примарных идеалов, ассоциированных с одним и тем же простым идеалом и пересекающихся по некоторому примарному идеалу, заменена на это пересечение. Представление при этом останется несократимым.

Среди конечного множества простых идеалов $\mathfrak{p}_\nu$ существует минимальный, т. е. такой, который не содержит ни одного из остальных. Пусть таковым является идеал $\mathfrak{p}_1$. Так как $\mathfrak{p}_1$ не содержит $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, то существует такой элемент a_ν, что

$$\left.\begin{aligned} a_\nu &\not\equiv 0\,(\mathfrak{p}_1) \\ a_\nu &\equiv 0\,(\mathfrak{p}_\nu) \end{aligned}\right\} \qquad (\nu = 2,\ 3,\ \ldots,\ r);$$

поэтому для достаточно большого ρ имеет место соотношение

$$a_\nu^\rho \equiv 0\,(\mathfrak{q}_\nu).$$

Если бы было $\mathfrak{q}_1 = \mathfrak{m}$, то представление $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ было бы сократимым (можно было бы удалить $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$). Следовательно, в $\mathfrak{q}_1$ существует элемент q_1 со свойством

$$q_1 \not\equiv 0\,(\mathfrak{m}).$$

Произведение

$$q_1 (a_2 \ldots a_r)^\rho$$

принадлежит как $\mathfrak{q}_1$, так и $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$, а потому и идеалу $\mathfrak{m}$. Но элемент q_1 не принадлежит идеалу $\mathfrak{m}$. Если бы $\mathfrak{m}$ был примарным, то это означало бы, что

$$(a_2 \ldots a_r)^{\rho\sigma} \equiv 0\,(\mathfrak{m}),$$
$$(a_2 \ldots a_r)^{\rho\sigma} \equiv 0\,(\mathfrak{p}_1);$$

следовательно, так как идеал $\mathfrak{p}_1$ прост, то

$$a_\nu \equiv 0\,(\mathfrak{p}_1)$$

по крайней мере для одного ν, что противоречит сказанному ранее.

Если в каком-либо несократимом представлении

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

Таким образом,

$$\mathfrak{m} = [\mathfrak{q}_1,\ \mathfrak{q}_2].$$

Это — несократимое представление и, так как ассоциированные с $\mathfrak{q}_1$ и $\mathfrak{q}_2$ простые идеалы (x) и $(x,\ y)$ различны, то это — представление наибольшими примарными компонентами. Наряду с ним есть еще одно:

$$\mathfrak{m} = [\mathfrak{q}_1,\ \mathfrak{q}_3],$$

где

$$\mathfrak{q}_3 = (x^2,\ y).$$

Действительно, чтобы многочлен принадлежал идеалу $\mathfrak{m}$, достаточно потребовать, чтобы он делился на x и в нем отсутствовало слагаемое, содержащее x. Когда поле K бесконечно, можно привести бесконечное множество представлений такого сорта:

$$\mathfrak{m} = [\mathfrak{q}_1,\ \mathfrak{q}^{(\lambda)}],\quad \mathfrak{q}^{(\lambda)} = (x^2,\ y + \lambda x).$$

Для всех указанных разложений идеала $\mathfrak{m}$ общим является одинаковое ч и с л о примарных компонент и н а б о р ассоциированных простых идеалов:

$$(x),\quad (x,\ y).$$

Это является общим фактом:

П е р в а я т е о р е м а е д и н с т в е н н о с т и. *В любых двух несократимых представлениях идеала* $\mathfrak{m}$ *наибольшими примарными компонентами количество компонент (но не обязательно сами компоненты) и наборы ассоциированных простых идеалов совпадают.*

Д о к а з а т е л ь с т в о. Для любого примарного идеала утверждение тривиально. Следовательно, мы можем провести индукцию по числу примарных компонент, появляющихся по крайней мере в одном представлении рассматриваемого идеала.

Пусть

$$\mathfrak{m} = [\mathfrak{q}_1,\ \ldots,\ \mathfrak{q}_l] = [\mathfrak{q}'_1,\ \ldots,\ \mathfrak{q}'_{l'}]. \tag{1}$$

Из всех ассоциированных простых идеалов $\mathfrak{p}_1,\ \ldots,\ \mathfrak{p}_l,\ \mathfrak{p}'_1,\ \ldots,\ \mathfrak{p}'_l$ выберем максимальный, т. е. не содержащийся в других. Пусть он входит, скажем, в левую часть и равен $\mathfrak{p}_1$. Тогда этот идеал входит и в правую часть. Действительно, иначе можно было бы в (1) построить частные от деления на $\mathfrak{q}_1$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1,\ \ldots,\ \mathfrak{q}_l : \mathfrak{q}_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1,\ \ldots,\ \mathfrak{q}'_{l'} : \mathfrak{q}_1];$$

для всех $\nu > 1$ имеет место $\mathfrak{q}_1 \not\equiv 0\,(\mathfrak{p}_\nu)$, так как в противном случае было бы $\mathfrak{p}_1 \equiv 0\,(\mathfrak{p}_\nu)$, что противоречит максимальности идеала $\mathfrak{p}_1$. Точно так же для всех ν имеет место $\mathfrak{q}_1 \not\equiv 0\,(\mathfrak{p}'_\nu)$. Следовательно, в силу теоремы IV′ (§ 117) имеем

$$\mathfrak{q}_\nu : \mathfrak{q}_1 = \mathfrak{q}_\nu \quad (\nu = 2,\ \ldots,\ l),$$
$$\mathfrak{q}'_\nu : \mathfrak{q}_1 = \mathfrak{q}'_\nu \quad (\nu = 1,\ \ldots,\ l').$$

Так как, далее, $\mathfrak{q}_1 : \mathfrak{q}_1 = \mathfrak{o}$, то

$$[\mathfrak{o}, \mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}_1', \ldots, \mathfrak{q}_{l'}'].$$

Справа стоит идеал $\mathfrak{m}$ и поэтому слева тоже должен быть идеал $\mathfrak{m}$; идеал $\mathfrak{o}$ можно отбросить. Следовательно,

$$\mathfrak{m} = [\mathfrak{q}_2, \ldots, \mathfrak{q}_l].$$

Это означает, что первое из двух данных представлений (1) при сделанном выше допущении оказывается сократимым, что противоречит условию.

Таким образом, каждый максимальный простой идеал входит в о б е части данного равенства.

Пусть теперь, например, $l \leqq l'$. Докажем, что $l = l'$ и что (при подходящей нумерации) $\mathfrak{p}_\nu' = \mathfrak{p}_\nu$. Для идеалов, которые представляются менее чем l примарными компонентами, все можно считать доказанным. Упорядочим идеалы $\mathfrak{q}$ и $\mathfrak{q}'$ так, чтобы $\mathfrak{p}_1 = \mathfrak{p}_1'$ был максимальным ассоциированным (с $\mathfrak{q}_1$ и $\mathfrak{q}_1'$) простым идеалом.

Разделим обе части (1) на произведение $\mathfrak{q}_1\mathfrak{q}_1'$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}_1', \ldots, \mathfrak{q}_l : \mathfrak{q}_1\mathfrak{q}_1'] = [\mathfrak{q}_1' : \mathfrak{q}_1\mathfrak{q}_1', \ldots, \mathfrak{q}_{l'}' : \mathfrak{q}_1\mathfrak{q}_1'];$$

тогда, так же как в предыдущем случае, получим

$$\left.\begin{aligned} \mathfrak{q}_\nu : \mathfrak{q}_1\mathfrak{q}_1' &= \mathfrak{q}_\nu, \\ \mathfrak{q}_\nu' : \mathfrak{q}_1\mathfrak{q}_1' &= \mathfrak{q}_\nu' \end{aligned}\right\} \quad (\nu > 1).$$

Далее, так как $\mathfrak{q}_1\mathfrak{q}_1'$ делится на $\mathfrak{q}_1$ и на $\mathfrak{q}_1'$, то

$$\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}_1' = \mathfrak{o},$$
$$\mathfrak{q}_1' : \mathfrak{q}_1\mathfrak{q}_1' = \mathfrak{o}.$$

Таким образом,

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}_2', \ldots, \mathfrak{q}_{l'}'].$$

Так как теперь слева и справа указано несократимое представление наименьшими примарными компонентами, то по предположению индукции имеет место равенство $l' - 1 = l - 1$, т. е. $l' = l$. Кроме того, при подходящей нумерации $\mathfrak{p}_\nu = \mathfrak{p}_\nu'$ для всех $\nu > 1$. Так как еще $\mathfrak{p}_1 = \mathfrak{p}_1'$, то все доказано.

Однозначно определенные в силу только что доказанной теоремы идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$, которые возникают как ассоциированные простые идеалы в несократимом представлении $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$, называются *простыми идеалами, ассоциированными с идеалом* $\mathfrak{a}$. Вот их важнейшее свойство:

Если идеал $\mathfrak{a}$ *не делится ни на один простой идеал, ассоциированный с идеалом* $\mathfrak{b}$, *то* $\mathfrak{b}$: $\mathfrak{a} = \mathfrak{b}$; *верно и обратное.*

Д о к а з а т е л ь с т в о. Пусть $\mathfrak{b} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$ — несократимое представление. Пусть сначала $\mathfrak{a} \not\equiv 0\,(\mathfrak{p}_i)$ для $i = 1, \ldots, l$, где $\mathfrak{p}_i$ —

идеал, ассоциированный с $\mathfrak{q}_i$. Отсюда следует, что

$$\begin{aligned}\mathfrak{q}_i : \mathfrak{a} &= \mathfrak{q}_i,\\ \mathfrak{b} : \mathfrak{a} &= [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] : \mathfrak{a} =\\ &= [\mathfrak{q}_1 : \mathfrak{a}, \ldots, \mathfrak{q}_l : \mathfrak{a}] =\\ &= [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] = \mathfrak{b}.\end{aligned}$$

Обратно, пусть $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$. Если бы было $\mathfrak{a} \equiv 0\ (\mathfrak{p}_i)$ для некоторого i, скажем, $\mathfrak{a} \equiv 0\ (\mathfrak{p}_1)$, то это означало бы, что $\mathfrak{a}^\rho \equiv 0\ (\mathfrak{q}_1)$, а потому

$$\mathfrak{a}^\rho [\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0\ ([\mathfrak{q}_1, \mathfrak{a}_2, \ldots, \mathfrak{q}_l]) \equiv 0\ (\mathfrak{b})$$

и, следовательно, в силу того, что каждое сравнение по $\mathrm{mod}\,\mathfrak{b}$ можно сокращать на $\mathfrak{a}$ и, стало быть, на $\mathfrak{a}^\rho$, имеем

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0\ (\mathfrak{b}),$$

что противоречит несократимости данного представления.

Важный частный случай: идеал $\mathfrak{a}$ является главным идеалом (a):

Если элемент a не делится ни на один из простых идеалов, ассоциированных с данным идеалом $\mathfrak{b}$, то $\mathfrak{b} : a = \mathfrak{b}$, т. е. из $ac \equiv 0\ (\mathfrak{b})$ следует, что $c \equiv 0\ (\mathfrak{b})$.

Общую теорему можно сформулировать и иным способом, представляя идеал $\mathfrak{a}$ в виде пересечения примарых идеалов $[\mathfrak{a}'_1, \ldots, \mathfrak{a}'_l]$. Идеал $\mathfrak{a}$ тогда и только тогда делится на $\mathfrak{p}_i$, когда этим свойством обладает одно из $\mathfrak{a}'_j$, или, что то же самое, одно из $\mathfrak{p}'_j$. Следовательно,

Если ни один из простых идеалов, ассоциированных с $\mathfrak{a}$, не делится на простой идеал, ассоциированный с $\mathfrak{b}$, то $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$; верно и обратное.

§ 120. Изолированные компоненты и символические степени

Пусть S — непустое множество в коммутативном кольце $\mathfrak{o}$, содержащее вместе с двумя любыми своими элементами s, t и их произведение st. Такое множество S называется *мультипликативно замкнутым*.

Пусть $\mathfrak{m}$ — идеал в $\mathfrak{o}$. Под $\mathfrak{m}_S$ мы подразумеваем множество всех тех элементов x из $\mathfrak{o}$, для которых sx лежит в $\mathfrak{m}$ при каком-то s из S.

Множество $\mathfrak{m}_S$ является идеалом (очевидно, делителем идеала $\mathfrak{m}$); действительно, если x и y лежат в $\mathfrak{m}_S$, то sx и $s'y$ принадлежат $\mathfrak{m}$, а потому

$$ss'(x - y) = s'(sx) - s(s'y)$$

лежит в $\mathfrak{m}$, так что $x-y$ принадлежит $\mathfrak{m}_S$; если x принадлежит $\mathfrak{m}_S$, то и rx лежит в $\mathfrak{m}_S$. То, что все элементы из $\mathfrak{m}$ принадлежат идеалу $\mathfrak{m}_S$, очевидно.

Идеал $\mathfrak{m}_S$ называется *S-компонентой идеала* $\mathfrak{m}$ или, более подробно, *компонентой идеала* $\mathfrak{m}$, *определенной множеством* S.

Начиная с этого места, пусть $\mathfrak{o}$ — нётерово кольцо. Если идеал $\mathfrak{m}$ представляется в виде произведения примарных идеалов

$$\mathfrak{m}=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r], \tag{1}$$

то примарные идеалы $\mathfrak{q}_i$ можно подразделить на те, которые пересекаются с S, т. е. имеют с S по крайней мере один общий элемент, и на все остальные. Если $\mathfrak{q}_i$ имеет с S общий элемент s, то ассоциированный простой идеал $\mathfrak{p}_i$ содержит тот же элемент s. Обратно, если $\mathfrak{p}$ содержит некоторый элемент s из S, то $\mathfrak{q}_i$ имеет с S общий элемент s^ρ при некотором натуральном ρ.

Перенумеруем идеалы $\mathfrak{q}_i$ так, чтобы $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$ не пересекались с S, а $\mathfrak{q}_{h+1}, \ldots, \mathfrak{q}_r$ пересекались. Утверждается:

$$\mathfrak{m}_S=[\mathfrak{q}_1, \ldots, \mathfrak{q}_h]. \tag{2}$$

В случае $h=0$ соотношение (2) означает попросту, что $\mathfrak{m}_S=\mathfrak{o}$.

Доказательство. Если x принадлежит идеалу $\mathfrak{m}_S$ и, следовательно, sx принадлежит $\mathfrak{m}$, то для $1\leqslant i\leqslant h$

$$sx\equiv 0\,(\mathfrak{q}_i), \quad s\not\equiv 0\,(\mathfrak{p}_i) \quad \text{и, следовательно,} \quad x\equiv 0\,(\mathfrak{q}_i),$$

т. е. x принадлежит идеалу $[\mathfrak{q}_1, \ldots, \mathfrak{q}_h]$. Обратно, если x принадлежит $[\mathfrak{q}_1, \ldots, \mathfrak{q}_h]$, то в случае $r>h$ для каждого i от $h+1$ до r можно выбрать элемент s_i из S, который делится на $\mathfrak{q}_i$. Положим

$$s=s_{h+1}\ldots s_r.$$

В случае $r=h$ выберем s из S произвольно. В обоих случаях элемент sx делится на все идеалы $\mathfrak{q}_i$, т. е. sx принадлежит идеалу $\mathfrak{m}$, а потому x принадлежит идеалу $\mathfrak{m}_S$.

Примарная компонента $\mathfrak{q}_i$ идеала $\mathfrak{m}$ называется *вложенной*, если ассоциированный простой идеал $\mathfrak{p}_i$ является делителем другого ассоциированного с $\mathfrak{m}$ простого идеала $\mathfrak{p}_j$; в противном случае компонента называется *изолированной*. В первом случае сам ассоциированный простой идеал $\mathfrak{p}_i$ называется *вложенным* (а именно — вложенным в идеал $\mathfrak{p}_j$), а во втором — этот идеал называется *изолированным*. Аналогично, подмножество $\{\mathfrak{q}_a, \mathfrak{q}_b, \ldots\}$ или $\{\mathfrak{p}_a, \mathfrak{p}_b, \ldots\}$ множества всех идеалов $\mathfrak{q}_i$, соответственно $\mathfrak{p}_i$, называется *изолированным*, если ни один из идеалов $\mathfrak{p}_a, \mathfrak{p}_b, \ldots$ не является делителем какого-либо $\mathfrak{p}_j$, не принадлежащего подмножеству.

При заданном идеале $\mathfrak{m}=[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ каждому мультипликативно замкнутому множеству S соответствует некоторое изолиро-

ванное подмножество $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$, состоящее из тех $\mathfrak{p}_i$, которые не содержат ни одного элемента из S. Это подмножество изолировано потому, что если $\mathfrak{p}_i$ — идеал этого подмножества, являющийся делителем идеала $\mathfrak{p}_j$, то и $\mathfrak{p}_j$ принадлежит подмножеству. Пересечение примарных идеалов, ассоциированных с $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$, является в этом случае изолированной компонентой $\mathfrak{a}_S$.

Важным частным случаем является тот, когда выбирается один изолированный идеал $\mathfrak{p}_i$, а в качестве S берется множество элементов кольца $\mathfrak{o}$, не делящихся на $\mathfrak{p}_i$. Это множество непусто, за исключением тривиального случая $\mathfrak{m} = \mathfrak{o}$. Любой другой идеал $\mathfrak{p}_j$ содержит элемент, не делящийся на $\mathfrak{p}_i$, т. е. элемент из S. Тем самым из (2) следует, что

$$\mathfrak{m}_S = \mathfrak{q}_i.$$

Следовательно, идеал $\mathfrak{m}_S$ однозначно определяется идеалом $\mathfrak{m}$ и множеством S, т. е. идеалом $\mathfrak{m}$ и идеалами $\mathfrak{p}_i$. Изолированные идеалы $\mathfrak{p}_i$ также определяются идеалом $\mathfrak{m}$ однозначно. В итоге имеем:

Изолированные примарные компоненты $\mathfrak{q}_i$ в (1) *определены однозначно.*

Задача. Тем же методом доказать вторую теорему единственности: пересечение $[\mathfrak{q}_a, \mathfrak{q}_b, \ldots]$ изолированного множества примарных компонент идеала $\mathfrak{m}$ однозначно определяется заданием ассоциированных простых идеалов $\mathfrak{p}_a, \mathfrak{p}_b, \ldots$

Символические степени. В § 117 мы видели, что степени $\mathfrak{p}^r$ простого идеала $\mathfrak{p}$ не обязаны являться примарными идеалами. Представим $\mathfrak{p}^r$ в виде пересечения примарных компонент:

$$\mathfrak{p}^r = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s];$$

тогда все ассоциированные простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ будут делителями идеала $\mathfrak{p}^r$, а потому и идеала $\mathfrak{p}$. Произведение $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_s$ таково, что некоторая его степень делится на все $\mathfrak{q}_i$, а потому на $\mathfrak{p}^r$ и, следовательно, на $\mathfrak{p}$. Отсюда вытекает, что один из сомножителей, скажем $\mathfrak{p}_1$, должен делиться на $\mathfrak{p}$. С другой стороны, $\mathfrak{p}_1$ — делитель идеала $\mathfrak{p}$, так что $\mathfrak{p}_1 = \mathfrak{p}$.

Остальные идеалы $\mathfrak{p}_i$ $(i \neq 1)$ являются собственными делителями идеала $\mathfrak{p}$. Отсюда следует, что $\mathfrak{q}_1$ является изолированной примарной компонентой идеала $\mathfrak{p}^r$ и в этом качестве определяется однозначно. Точнее, идеал $\mathfrak{q}_1$ является изолированной компонентой $\mathfrak{p}^r_S$ идеала $\mathfrak{p}^r$, определенной множеством S, где S — множество элементов кольца $\mathfrak{o}$, не делящихся на $\mathfrak{p}$.

Однозначно определенная таким способом примарная компонента идеала $\mathfrak{p}^r$, ассоциированная с простым идеалом $\mathfrak{p}_1 = \mathfrak{p}$, называется, по предположению Крулля, *r-й символической степенью идеала* $\mathfrak{p}$ и обозначается $\mathfrak{p}^{(r)}$.

§ 121. Теория взаимно простых идеалов

В дальнейшем будет предполагаться, что в кольце $\mathfrak{o}$ существует единица. Эта единица порождает единичный идеал $\mathfrak{o}$:

$$\mathfrak{o} = (1).$$

Два идеала $\mathfrak{a}$, $\mathfrak{b}$ называются *взаимно простыми*, если у них нет общих деталей, кроме $\mathfrak{o}$, т. е. если их наибольший общий делитель равен $\mathfrak{o}$:

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}.$$

Это означает, что каждый элемент из $\mathfrak{o}$ представляется в виде суммы некоторого элемента из $\mathfrak{a}$ и некоторого элемента из $\mathfrak{b}$.

Необходимым и достаточным для этого является условие представимости единицы (образующей идеала $\mathfrak{o}$) в виде суммы

$$1 = a + b \tag{1}$$

($a \in \mathfrak{a}$, $b \in \mathfrak{b}$). В этом случае

$$\left.\begin{aligned} a &\equiv 1\ (\mathfrak{b}), \qquad b \equiv 0\ (\mathfrak{b}), \\ a &\equiv 0\ (\mathfrak{a}), \qquad b \equiv 1\ (\mathfrak{a}). \end{aligned}\right\} \tag{2}$$

Если два примарных идеала $\mathfrak{q}_1$, $\mathfrak{q}_2$ взаимно просты, то ассоциированные простые идеалы $\mathfrak{p}_1$, $\mathfrak{p}_2$ тем более взаимно просты (каждый общий делитель $\mathfrak{p}_1$ и $\mathfrak{p}_2$ является общим делителем и идеалов $\mathfrak{q}_1$, $\mathfrak{q}_2$). Однако верно и обратное: *из взаимной простоты идеалов* $\mathfrak{p}_1$, $\mathfrak{p}_2$ *следует взаимная простота идеалов* $\mathfrak{q}_1$, $\mathfrak{q}_2$. В самом деле, из

$$1 = p_1 + p_2$$

при возведении в $(\rho + \sigma - 1)$-ю степень следует, что

$$1 = p_1^{\rho+\sigma-1} + \ldots + p_2^{\rho+\sigma-1};$$

выберем ρ и σ настолько большими, чтобы p_1^ρ лежало в $\mathfrak{q}_1$, а p_2^σ лежало в $\mathfrak{q}_2$; тогда каждое слагаемое лежит либо в $\mathfrak{q}_1$, либо в $\mathfrak{q}_2$ и, следовательно,

$$1 = q_1 + q_2.$$

Если два идеала взаимно просты, то они являются простыми друг относительно друга.

Доказательство. Пусть $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ и, скажем, $a + b = 1$. Достаточно показать, что $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{a}$. Если x принадлежит $\mathfrak{a} : \mathfrak{b}$, то $xb \subseteq \mathfrak{a}$ и $xb \equiv 0\ (\mathfrak{a})$; следовательно,

$$x(a + b) \equiv 0\ (\mathfrak{a}),$$
$$x \cdot 1 \equiv 0\ (\mathfrak{a});$$

это означает, что x принадлежит $\mathfrak{a}$, что и требовалось доказать.

Обращение неверно; вот пример: в кольце многочленов $K[x, y]$ идеалы (x) и (y) просты друг относительно друга, но не взаимно просты:

$$(x, y) \neq \mathfrak{o},$$
$$(x) : (y) = (x),$$
$$(y) : (x) = (y).$$

Если $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты, то, как и в теории чисел, сравнения по модулям этих идеалов можно решать одновременно. Пусть даны два сравнения:

$$\begin{aligned} f(\xi) &\equiv 0\ (\mathfrak{a}), \\ g(\xi) &\equiv 0\ (\mathfrak{b}) \end{aligned} \qquad (f(x),\ g(x) \in \mathfrak{o}\ [x]).$$

Будем считать, что каждое из сравнений разрешимо. Если $\xi \equiv \alpha$ — решение первого сравнения, а $\xi \equiv \beta$ — второго, то можно построить элемент ξ, удовлетворяющий обоим сравнениям, следующим образом. С помощью построенных ранее элементов a и b, удовлетворяющих соотношениям (1) и (2), составим

$$\xi = b\alpha + a\beta.$$

Тогда $\xi \equiv \alpha\ (\mathfrak{a})$ и $\xi \equiv \beta\ (\mathfrak{b})$, т. е. ξ — решение обоих заданных сравнений.

Для двух взаимно простых идеалов наименьшим общим кратным служит их произведение.

Доказательство. В § 116 было доказано, что

$$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b},$$
$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{ab}.$$

Если $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ и существует единица, то второе соотношение упрощается до

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab};$$

следовательно,

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}.$$

Чтобы сформулировать эту теорему более чем для двух взаимно простых идеалов, докажем предварительно следующую лемму:

Если идеал $\mathfrak{a}$ взаимно прост с $\mathfrak{b}$ и $\mathfrak{c}$, то $\mathfrak{a}$ взаимно прост с произведением $\mathfrak{bc}$ и пересечением $\mathfrak{b} \cap \mathfrak{c}$.

Доказательство. Из

$$a + b = 1,$$
$$a' + c = 1$$

следует, что

$$(a + b)(a' + c) = 1,$$
$$aa' + ac + a'b + bc = 1,$$
$$a'' + bc = 1,$$

где $a'' = aa' + ac + a'b$ — вновь некоторый элемент из $\mathfrak{a}$. Отсюда следует, что

$$(\mathfrak{a},\ \mathfrak{bc}) = \mathfrak{o}$$

и, тем более,

$$(\mathfrak{a},\ \mathfrak{b} \cap \mathfrak{c}) = \mathfrak{o}.$$

Тем самым доказаны оба утверждения.

Если теперь идеалы $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ попарно взаимно просты и уже доказано равенство

$$[\mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1}] = \mathfrak{b}_1 \ldots \mathfrak{b}_{n-1},$$

то

$$\begin{aligned}[\mathfrak{b}_1, \ldots, \mathfrak{b}_n] &= [\mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1}] \cap \mathfrak{b}_n = \\ &= (\mathfrak{b}_1 \ldots \mathfrak{b}_{n-1}) \cap \mathfrak{b}_n = \\ &= \mathfrak{b}_1 \ldots \mathfrak{b}_{n-1} \cdot \mathfrak{b}_n;\end{aligned}$$

следовательно, по индукции получается

Теорема. *Наименьшее общее кратное конечного множества попарно взаимно простых идеалов равно произведению этих идеалов.*

Сделанное раньше замечание о решении сравнений по модулям взаимно простых идеалов остается в силе и для нескольких попарно взаимно простых идеалов:

Если идеалы $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_r$ попарно взаимно просты, то существует элемент ξ, удовлетворяющий сравнениям

$$\xi \equiv \beta_i \ (\mathfrak{b}_i) \qquad (i = 1, 2, \ldots, r).$$

Доказательство проводится по индукции. Допустим, что уже получен элемент η, для которого

$$\eta \equiv \beta_i \ (\mathfrak{b}_i) \qquad (i = 1, 2, \ldots, r-1),$$

и найдем ξ из условий

$$\begin{aligned}\xi &\equiv \eta \ ([\mathfrak{b}_1, \ldots, \mathfrak{b}_{r-1}]), \\ \xi &\equiv \beta_r \ (\mathfrak{b}_r),\end{aligned}$$

что всегда возможно, так как идеал $\mathfrak{b}_r$ взаимно прост с идеалом $[\mathfrak{b}_1, \ldots, \mathfrak{b}_{r-1}]$.

Если в $\mathfrak{o}$ имеет место теорема о цепях делителей, то каждый идеал можно представить в виде пересечения попарно взаимно простых идеалов, ни один из которых уже не представляется как пересечение взаимно простых собственных делителей.

Для доказательства найдем в каком-нибудь несократимом представлении данного идеала $\mathfrak{m}$ примарными идеалами

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

все те примарные идеалы, которые с одним, произвольно фиксированным среди них идеалом соединяются цепью попарно не взаимно простых примарных идеалов, и составим их пересече-

ние $\mathfrak{b}_1$. Из оставшихся идеалов точно так же построим последовательно идеалы $\mathfrak{b}_2, \ldots, \mathfrak{b}_s$. Представление

$$\mathfrak{m} = [\mathfrak{b}_1, \ldots, \mathfrak{b}_s] \tag{3}$$

обладает нужными свойствами. Действительно, во-первых, $\mathfrak{b}_i$ и $\mathfrak{b}_k$ при $i \neq k$ взаимно просты, так как компоненты идеала $\mathfrak{b}_i$ взаимно просты с компонентами идеала $\mathfrak{b}_k$. Во-вторых, невозможно, скажем, идеал $\mathfrak{b}_1$ представить как пересечение двух взаимно простых собственных делителей. Если бы такое представление было возможно:

$$\mathfrak{b}_1 = \mathfrak{b} \cap \mathfrak{c} = \mathfrak{b}\mathfrak{c},$$
$$(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o},$$

то каждый простой идеал, ассоциированный с $\mathfrak{b}_1$, обязательно был бы делителем идеала $\mathfrak{b}\mathfrak{c}$, а потому делителем идеала $\mathfrak{b}$ или идеала $\mathfrak{c}$; так как все эти простые идеалы связаны с одним из них некоторой цепью попарно не взаимно простых идеалов (являющихся простыми), то из того, что один из них делит $\mathfrak{b}$, следует, что все они должны делить $\mathfrak{b}$ и ни один из них не должен делить $\mathfrak{c}$. Ассоциированные примарные компоненты делят $\mathfrak{b}\mathfrak{c}$; следовательно, они делят и $\mathfrak{b}$ (так как их простые идеалы не делят $\mathfrak{c}$). Отсюда следует, что пересечение $\mathfrak{b}_1$ является некоторым делителем идеала $\mathfrak{b}$:

$$\mathfrak{b} \subseteq \mathfrak{b}_1,$$

что противоречит предположению, согласно которому $\mathfrak{b}$ является собственным делителем идеала $\mathfrak{b}_1$.

Вместо представления (3) в соответствии с нашими теоремами можно записать следующее представление произведением:

$$\mathfrak{m} = \mathfrak{b}_1\mathfrak{b}_2 \ldots \mathfrak{b}_s.$$

Задача. Пересечение (3) является прямым пересечением в смысле § 92. Кольцо классов вычетов $\mathfrak{o}/\mathfrak{m} = \bar{\mathfrak{o}}$ является прямой суммой колец $\mathfrak{a}_i/\mathfrak{m} = \bar{\mathfrak{a}}_i$, каждое из которых изоморфно некоторому кольцу классов вычетов $\mathfrak{o}/\mathfrak{b}_i$. (Положить $\mathfrak{a}_i = [\mathfrak{b}_1, \ldots, \mathfrak{b}_{i-1}, \mathfrak{b}_{i+1}, \ldots, \mathfrak{b}_s]$ и применить теоремы из § 92.)

§ 122. Однократные идеалы

Пусть опять $\mathfrak{o}$ — нётерово кольцо с единицей.

Единичный идеал $\mathfrak{o}$, конечно, является простым. Какие примарные идеалы могут быть с ним ассоциированы? Ответ таков: лишь само кольцо $\mathfrak{o}$, потому что если $\mathfrak{q}$ — произвольный из ассоциированных с $\mathfrak{o}$ примарных идеалов, то $1^\rho \in \mathfrak{q}$, откуда $\mathfrak{q} = \mathfrak{o}$.

Если в такой ситуации некоторое представление идеала $\mathfrak{a} \neq \mathfrak{o}$ пересечением примарных идеалов $[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ таково, что среди ассоциированных примарных идеалов $\mathfrak{p}_i$ есть единичный идеал, то соответствующий ему идеал $\mathfrak{q}_i$ также равен $\mathfrak{o}$ и поэтому в представлении пересечением может быть сокращен. Следовательно,

если представление $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ *несократимо и* $\mathfrak{a} \neq \mathfrak{o}$, *то единичный идеал не входит в число ассоциированных простых идеалов.*

Отсюда немедленно следует предложение:

Каждый идеал $\mathfrak{a} \neq \mathfrak{o}$ *обладает по крайней мере одним простым делителем* $\mathfrak{p} \neq \mathfrak{o}$. *Если идеал* $\mathfrak{a}$ *не является примарным, то у него есть по крайней мере два простых делителя, отличных от* $\mathfrak{o}$.

Идеал, у которого не более одного отличного от $\mathfrak{o}$ простого делителя, называется *однократным* (по Дедекинду). В соответствии с последней теоремой каждый однократный идеал $\mathfrak{a}$ примарен. Кроме того, ассоциированный с ним простой идеал $\mathfrak{p}$ обязательно не имеет делителей, потому что если бы $\mathfrak{a}' \neq \mathfrak{o}$ был собственным делителем идеала $\mathfrak{p}$, то $\mathfrak{a}'$ в свою очередь обладал бы простым делителем $\mathfrak{p}' \neq \mathfrak{o}$, который был бы собственным делителем идеала $\mathfrak{p}$ и, значит, идеал $\mathfrak{q}$ обладал бы двумя различными и отличными от $\mathfrak{o}$ простыми делителями $\mathfrak{p}$ и $\mathfrak{p}'$, что противоречит предположенной однократности идеала $\mathfrak{q}$.

Имеем

$$\mathfrak{p}^\rho \equiv 0 \ (\mathfrak{a}). \tag{1}$$

Из соотношения (1) следует, что если $\mathfrak{p}$ свободен от делителей, то идеал $\mathfrak{q}$ однократен. Действительно, в этом случае для любого простого делителя $\mathfrak{p}'$ идеала $\mathfrak{q}$ из (1) следует, что

$$\mathfrak{p}^\rho \equiv 0 \ (\mathfrak{p}'),$$

откуда

$$\mathfrak{p} \equiv 0 \ (\mathfrak{p}')$$

и, следовательно, либо $\mathfrak{p}' = \mathfrak{p}$, либо $\mathfrak{p}' = \mathfrak{o}$. Таким образом, идеал $\mathfrak{q}$ не имеет простых делителей, отличных от $\mathfrak{p}$ и $\mathfrak{o}$.

Итак, равносильны следующие понятия:

1) однократный идеал;

2) примарный идеал, ассоциированный с простым идеалом, не имеющим делителей;

3) делитель некоторой степени $\mathfrak{p}^\rho$ простого идеала $\mathfrak{p}$, не имеющего делителей.

Далее имеет место предложение:

Пусть идеал $\mathfrak{m}$ *обладает изолированной однократной примарной компонентой* $\mathfrak{q}$, $\mathfrak{p}$ *— ассоциированный простой идеал этой компоненты, а* ρ *— ее показатель; тогда для любого целого числа* $\sigma \geqslant \rho$ *имеем*

$$\mathfrak{q} = (\mathfrak{m}, \ \mathfrak{p}^\sigma). \tag{2}$$

Доказательство. Из

$$\mathfrak{m} \equiv 0 \ (\mathfrak{q})$$

и

$$\mathfrak{p}^\sigma \equiv 0 \ (\mathfrak{q})$$

следует, что

$$(\mathfrak{m},\ \mathfrak{p}^{\sigma}) \equiv 0\ (\mathfrak{q}). \tag{3}$$

Пусть, с другой стороны,

$$\mathfrak{m} = [\mathfrak{q},\ \mathfrak{q}_2,\ \ldots,\ \mathfrak{q}_s]$$

— некоторое представление идеала $\mathfrak{m}$ примарными компонентами. Идеал $(\mathfrak{m},\ \mathfrak{p}^{\sigma})$ однократный, а потому примарный. Ассоциированным простым идеалом служит идеал $\mathfrak{p}$. Произведение $\mathfrak{q}\mathfrak{q}_2 \ldots \mathfrak{q}_s$ делится на $(\mathfrak{m},\ \mathfrak{p}^{\sigma})$. Однако произведение $\mathfrak{q}_2 \ldots \mathfrak{q}_s$ не делится на $\mathfrak{p}$, так как, по условию, $\mathfrak{q}$ — *изолированная* компонента. Следовательно, идеал $\mathfrak{q}$ должен делиться на $(\mathfrak{m},\ \mathfrak{p}^{\sigma})$:

$$\mathfrak{q} \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\sigma}). \tag{4}$$

Из (3) и (4) следует (2).

Следствие. *Для* $\sigma \geqslant \rho$

$$\mathfrak{p}^{\sigma} \equiv 0\ (\mathfrak{q}) \equiv (\mathfrak{m},\ \mathfrak{p}^{\sigma+1});$$

таким образом,

$$\mathfrak{p}^{\sigma} \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\sigma+1}). \tag{5}$$

Для $\sigma < \rho$ соотношение (5) не выполняется. Действительно, если бы было

$$\mathfrak{p}^{\sigma} \equiv 0\ (\mathfrak{m},\ \mathfrak{p}^{\sigma+1})$$

для некоторого $\sigma < \rho$, то умножением на $\mathfrak{p}^{\rho-\sigma-1}$ можно было бы получить

$$\mathfrak{p}^{\rho-1} \equiv 0\ (\mathfrak{m}\mathfrak{p}^{\rho-\sigma-1},\ \mathfrak{p}^{\rho}) \equiv 0\ (\mathfrak{m},\ \mathfrak{q}) \equiv 0\ (\mathfrak{q}),$$

что противоречит определению показателя ρ.

Показатель ρ *идеала* $\mathfrak{q}$ *является, таким образом, наименьшим числом* σ, *для которого выполнено соотношение* (5).

Существуют целостные кольца o с единицей, в которых (имеет место теорема о цепях делителей и) каждый отличный от нуля простой идеал не имеет делителей. Например, к числу таких колец относятся кольца главных идеалов (ср. § 18), а также определяемые ниже «порядки» в числовых и функциональных полях; типичный пример — кольцо $\mathbb{Z}\left[\sqrt{-3}\right]$. Теория идеалов этих колец особенно проста. Прежде всего, здесь все примарные идеалы, кроме нулевого, однократны. Далее, любые два отличных от нуля и друг от друга простых идеала в этом случае взаимно просты. Отсюда следует, что ассоциированные примарные идеалы для различных ненулевых простых идеалов также взаимно просты. Наконец, примарные компоненты любого идеала изолированы и, таким образом, однозначно определены. Итак: *каждый ненулевой идеал однозначно представляется в виде пересечения попарно взаимно простых однократных примарных идеалов.* Согласно § 121 это

пересечение равно произведению

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \ldots \mathfrak{q}_r.$$

В кольцах главных идеалов примарные идеалы $\mathfrak{q}_i$ равны степеням простых идеалов. В общем случае это верно при некотором условии, с которым мы познакомимся позже, — условии «целозамкнутости».

§ 123. Кольца частных

В § 13 мы построили поле частных произвольного коммутативного кольца без делителей нуля. Эта конструкция без изменений переносится и на кольца с делителями нуля, если только в кольце есть элементы, не являющиеся делителями нуля. Для этого строится кольцо дробей a/b, в которых знаменателями служат всевозможные элементы, не являющиеся делителями нуля, а числителем a может быть любой элемент кольца.

Множество знаменателей можно еще более ограничить. Пусть в коммутативном кольце R задано непустое множество S элементов, не являющихся делителями нуля, которое вместе с двумя любыми своими элементами s и t содержат их произведение st. Тогда дроби a/s (a принадлежит R, а s принадлежит S) образуют кольцо, содержащее кольцо R: *кольцо частных* $R' = \frac{R}{S}$. Это понятие восходит к Грелллю (Grell H. — Math. Ann., **97**, S. 499).

Если R' — коммутативное кольцо, содержащее R, то каждый идеал $\mathfrak{a}$ из R порождает некоторый идеал $\mathfrak{a}'$ в кольце R' — *расширение идеала* $\mathfrak{a}$ *в кольце* R'. Наоборот, пересечение кольца R с любым идеалом $\mathfrak{c}'$ из R' всегда является идеалом в R — *сужéнием идеала* $\mathfrak{c}'$ *в кольце* R. Сужéния идеалов $\mathfrak{c} \cap R'$ называются также *отмеченными идеалами* [1]) кольца R (относительно R').

Общее исследование о расширениях и сужéниях идеалов имеется в уже упоминавшейся работе Грелля. Здесь же мы рассмотрим лишь случай колец частных, где связи достаточно просты.

Если $\mathfrak{a}$ — идеал в R, то расширение $\mathfrak{a}'$ в кольце частных R' состоит из всевозможных дробей a/s (a принадлежит $\mathfrak{a}$, s принадлежит S). Если из идеала $\mathfrak{a}'$ построить сужéние $\mathfrak{a}' \cap R$, то получится в точности S-компонента $\mathfrak{a}_S$, определенная в § 120, а именно — множество всех x, для которых sx при некотором s из S лежит в $\mathfrak{a}$.

Обратно, если исходить из произвольного идеала $\mathfrak{a}'$ кольца частных R' и построить сужéние

$$\mathfrak{a} = \mathfrak{a}' \cap R,$$

то расширением идеала $\mathfrak{a}$ вновь будет $\mathfrak{a}'$. Пересечение этого рас-

[1]) В оригинале — ausgezeichnete Ideale, — *Прим. перев.*

ширения с R равно $\mathfrak{a}$ и в этом случае $\mathfrak{a}_S = \mathfrak{a}$. Наоборот, если $\mathfrak{a}_S = \mathfrak{a}$, то $\mathfrak{a}$ — сужéние некоторого идеала, а именно — идеала $\mathfrak{a}'$, являющегося его расширением. *Отмеченные идеалы $\mathfrak{a}$ кольца R характеризуются, следовательно, свойством*: $\mathfrak{a}_S = \mathfrak{a}$.

Из сказанного немедленно следует, что между идеалами $\mathfrak{a}'$ кольца R' и отмеченными идеалами $\mathfrak{a}$ кольца R есть взаимно однозначное соответствие по правилу: $\mathfrak{a}$ является сужéнием идеала $\mathfrak{a}'$, а $\mathfrak{a}'$ является расширением идеала $\mathfrak{a}$. При этом, очевидно, пересечению $\mathfrak{a}' \cap \mathfrak{c}'$ соответствует пересечение $\mathfrak{a} \cap \mathfrak{c}$.

Если в R имеет место теорема о цепях делителей, то она имеет место, в частности, и для отмеченных идеалов, а потому и для идеалов кольца R'. Упорядочим в пересечении

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] \tag{1}$$

примарные идеалы $\mathfrak{q}_i$ так, чтобы элементы из S содержались лишь в $\mathfrak{q}_{h+1}, \ldots, \mathfrak{q}_r$ (или в ассоциированных простых идеалах $\mathfrak{p}_{h+1}, \ldots, \mathfrak{p}_r$); тогда эти идеалы при расширении перейдут в единичный идеал кольца R' и, как в § 120, получится, что

$$\mathfrak{a}_S = [\mathfrak{q}_1, \ldots, \mathfrak{q}_h]. \tag{2}$$

Стоящие в правой части соотношения (2) идеалы $\mathfrak{q}_i$ обладают тем свойством, что $\mathfrak{q}_S = \mathfrak{q}$. Таким образом, идеал $\mathfrak{a}_S$ — отмеченный. В силу взаимно однозначной связи между отмеченными идеалами и их расширениями из (1) получается следующее представление для расширения идеала:

$$\mathfrak{a}' = [\mathfrak{q}_1', \ldots, \mathfrak{q}_h']. \tag{3}$$

Сравнение равенств (1) и (3) показывает, что при переходе от R к R' строение идеалов становится более бедным. Все те идеалы, которые содержат элементы из S, — в частности, идеалы $\mathfrak{q}_{h+1}, \ldots, \mathfrak{q}_r$, — дают в качестве расширения единичный идеал. Лишь отмеченные идеалы $\mathfrak{a}$ (обладающие свойством $\mathfrak{a}_S = \mathfrak{a}$) остаются при расширении неизменными в том смысле, что из $\mathfrak{a}'$ можно вновь получить исходный идеал $\mathfrak{a} = \mathfrak{a}_S$ как результат сужéния.

Задача 1. Если $\mathfrak{q}$ — примарный идеал, а $\mathfrak{p}$ — ассоциированный с ним простой идеал, то расширение $\mathfrak{q}'$ в кольце частных R' примарно и ассоциированным простым идеалом служит $\mathfrak{p}'$.

Задача 2. Если $\mathfrak{q}'$ — примарный идеал с ассоциированным простым идеалом $\mathfrak{p}'$ в кольце R', то и в произвольном подкольце R сужéние $\mathfrak{q} = \mathfrak{q}' \cap R$ примарно с ассоциированным простым идеалом $\mathfrak{p} = \mathfrak{p}' \cap R$.

Обобщенные кольца частных. Если S — мультипликативно замкнутое множество кольца R, содержащее делители нуля, но не содержащее самого нуля, то, следуя Шевалле, можно определить *обобщенное кольцо частных*. *Пусть* $\mathfrak{n} = (0)_S$ — S-компонента нулевого идеала в R. Построим сначала факторкольцо $R^* = R/\mathfrak{n}$.

Классы вычетов элементов из S по модулю $\mathfrak{n}$ составляют мультипликативно замкнутое множество S^* кольца R^*, не содержащее делителей нуля. Тогда можно построить обычное кольцо частных $R' = \frac{R^*}{S^*}$. Оно и называется *обобщенным кольцом частных кольца R относительно множества S*. Свойства этого объекта аналогичны свойствам обычных колец частных. Так, например, можно построить расширение идеала $\mathfrak{a}$ кольца R; для этого сначала строится образ $\mathfrak{a}^*$ идеала $\mathfrak{a}$ при гомоморфизме $R \to R^*$, а затем берется идеал кольца R', порождаемый идеалом $\mathfrak{a}^*$. Аналогично строится сужéние идеала $\mathfrak{c}'$ кольца R': сначала берется пересечение с кольцом R^*, а потом строится множество элементов, классы вычетов по модулю $\mathfrak{n}$ которых принадлежат этому пересечению.

Дальнейшие сведения можно найти в книге: Норткотт (Northcott D. G.). Ideal theory. — Cambridge Tracts in Math., **42**, section 2.7.

§ 124. Пересечение всех степеней идеала

Пусть в дальнейшем $\mathfrak{o}$ обозначает нётерово кольцо с единицей. Кольцо называется *нуль-примарным*, если примарен нулевой идеал, т. е. если из $ab = 0$ следует, что $a = 0$ или $b^r = 0$.

В фундаментальной работе В. Крулль[1]) показал, что в произвольном нуль-примарном кольце $\mathfrak{o}$, — в частности, в любом целостном кольце — пересечение всех степеней каждого отличного от $\mathfrak{o}$ идеала $\mathfrak{a}$ равно нулю. Для простых идеалов $\mathfrak{p} \neq \mathfrak{o}$ равно нулю даже пересечение всех символических степеней $\mathfrak{p}^{(r)}$. Из этих теорем оказывается возможным получить ряд утверждений и о произвольных кольцах. Мы изложим здесь основные идеи соответствующей теории.

Теорема 1. *Если $\mathfrak{a}$ и $\mathfrak{b}$ — идеалы в нуль-примарном кольце $\mathfrak{o}$ и*

$$\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}, \tag{1}$$

то $\mathfrak{a} = \mathfrak{o}$ или $\mathfrak{b} = (0)$.

Доказательство. Пусть $\mathfrak{b} = (d_1, \ldots, d_n)$. Тогда из (1) следует, что

$$d_i = \sum a_{ik} d_k. \tag{2}$$

Как обычно, положим, $\delta_{ik} = 0$ для $i = k$ и $\delta_{ii} = 1$; тогда вместо (2) можно записать

$$\sum (\delta_{ik} - a_{ik})\, d_k = 0. \tag{3}$$

Определитель этой системы уравнений равен

$$D = 1 - a,$$

[1]) Krull W. Primidealketten in allgemeinen Ringbereichen. — Sitzungsberichte Heidelberger Akad., 1928, 7. Abh.

где a принадлежит идеалу $\mathfrak{a}$. Умножим уравнения (3) на миноры элементов k-го столбца определителя D и сложим полученные равенства; получится [1])

$$Dd_k = 0,$$

а отсюда для каждого элемента d идеала $\mathfrak{b}$ получаем

$$(1-a)\,d = Dd = 0.$$

Это означает, что либо $(1-a)^r = 0$, либо, если ни одна из степеней элемента $(1-a)$ не равна нулю, $d = 0$ для всех d из $\mathfrak{b}$. В первом случае $1 \equiv 0\,(\mathfrak{a})$ и, следовательно, $\mathfrak{a} = \mathfrak{o}$. Во втором же случае $\mathfrak{b} = (0)$.

Теорема 2. *Если $\mathfrak{o}$ — нуль-примарное кольцо и $\mathfrak{a} \neq \mathfrak{o}$, то пересечение всех степеней идеала $\mathfrak{a}$ равно нулю*:

$$\mathfrak{b} = [\mathfrak{a},\ \mathfrak{a}^2, \ldots] = (0). \tag{4}$$

Доказательство. Прежде всего следует доказать включение $\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$. Для этой цели представим $\mathfrak{a}\mathfrak{b}$ в виде пересечения примарных идеалов

$$\mathfrak{a}\mathfrak{b} = [\mathfrak{q}_1, \ \ldots, \ \mathfrak{q}_r].$$

Для каждого i идеал $\mathfrak{a}\mathfrak{b}$ делится на $\mathfrak{q}_i$; следовательно, $\mathfrak{b}$ или некоторая степень $\mathfrak{a}^n$ делится на $\mathfrak{q}_i$. Но идеал $\mathfrak{b}$ делится на каждую степень $\mathfrak{a}^n$; следовательно, в обоих случаях $\mathfrak{b} \subseteq \mathfrak{q}_i$. Так как это включение имеет место для всех i, справедливо равенство $\mathfrak{b} = \mathfrak{a}\mathfrak{b}$. Согласно теореме 1 отсюда следует, что $\mathfrak{b} = (0)$.

Для простых идеалов $\mathfrak{p} \neq \mathfrak{o}$ имеет место более сильное утверждение:

Теорема 3. *В любом нуль-примарном кольце пересечение всех символических степеней $\mathfrak{p}^{(r)}$ отличного от $\mathfrak{o}$ простого идеала $\mathfrak{p}$ является нулевым идеалом*:

$$[\mathfrak{p},\ \mathfrak{p}^{(2)},\ \mathfrak{p}^{(3)}, \ldots] = (0) \tag{5}$$

Доказательство. Пусть S — совокупность всех элементов из $\mathfrak{o}$, не делящихся на $\mathfrak{p}$. Возьмем кольцо частных $\mathfrak{o}_S$. Пусть $\mathfrak{P}$ — расширение идеала $\mathfrak{p}$ в кольце $\mathfrak{o}_S$. Очевидно, расширением идеала $\mathfrak{p}^r$ будет $\mathfrak{P}^r$. Однако сужение идеала $\mathfrak{P}^r$ на исходное кольцо равно

$$(\mathfrak{P}^r)_S = \mathfrak{p}^{(r)}.$$

Пересечение всех символических степеней $\mathfrak{p}^{(r)}$ равно пересечению всех $\mathfrak{P}^r$ с кольцом $\mathfrak{o}$. Согласно теореме 2 пересечение всех идеалов $\mathfrak{P}^r$ равно нулю. Следовательно, пересечение всех $\mathfrak{p}^{(r)}$ является нулевым идеалом.

---

[1]) См. задачу 9 в § 25. — *Прим. ред.*

Теоремы 1 и 2 могут быть распространены на произвольные кольца рассмотренного здесь вида. Пусть S — множество всех элементов $s = 1 - a$, где a пробегает идеал $\mathfrak{a}$. Множество S мультипликативно замкнуто, а потому можно определить S-компоненту $(0)_S$ нулевого идеала как множество таких x, для которых выполняется равенство

$$(1 - a)\, x = 0 \quad \text{для} \quad a \in \mathfrak{a}.$$

Имеют место следующие предложения:

Теорема 1а. *Из* $\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$ *следует, что* $\mathfrak{b} \subseteq (0)_S$.

Теорема 2а. *Пересечение всех степеней идеала* $\mathfrak{a}$ *равно* $(0)_S$.

Доказательство теоремы 1а начинается точно так же, как доказательство теоремы 1, — с равенства

$$(1 - a)\, d = 0.$$

Из этого равенства немедленно следует утверждение:

$$d \in (0)_S \text{ для всех } d \text{ из } \mathfrak{b}.$$

Половина теоремы 2а — включение

$$[\mathfrak{a},\ \mathfrak{a}^2,\ \ldots] \subseteq (0)_S$$

— доказывается точно так же, как теорема 2. Вторую половину — включение

$$(0)_S \subseteq [\mathfrak{a},\ \mathfrak{a}^2,\ \ldots]$$

— доказать тоже легко. Действительно, если x лежит в $(0)_S$, то

$$(1 - a)\, x = 0,$$

откуда $x = ax$, и поэтому

$$x = ax = a^2x = a^3x = \ldots$$

Тем самым элемент x делится на любую степень элемента a.

Применим теоремы 1 и 2 к факторкольцу $\mathfrak{o}/\mathfrak{q}$ по некоторому примарному идеалу $\mathfrak{q}$; в результате получатся следующие утверждения:

Теорема 1б. *Если* $\mathfrak{q}$ — *примарный идеал и*

$$\mathfrak{b} \equiv 0\,(\mathfrak{a}\mathfrak{b},\ \mathfrak{q}), \tag{6}$$

то либо $(\mathfrak{a},\ \mathfrak{q}) = \mathfrak{o}$, *либо* $\mathfrak{b} \equiv 0\,(\mathfrak{q})$.

Теорема 2б. *Если элемент* y *кольца* $\mathfrak{o}$ *удовлетворяет при каждом натуральном* n *сравнению*

$$y \equiv 0\,(\mathfrak{a}^n,\ \mathfrak{q}), \tag{7}$$

то либо $(\mathfrak{a},\ \mathfrak{q}) = \mathfrak{o}$, *либо* $y \equiv 0\,(\mathfrak{q})$.

Задача 1. В любом нётеровом кольце с единицей пересечение всех символических степеней простого идеала $\mathfrak{p} \neq \mathfrak{o}$ равно $(0)_S$.

Задача 2. Как формулируются теоремы 1б и 2б, когда вместо примарного идеала $\mathfrak{q}$ берется произвольный идеал $\mathfrak{m}$? (Применить теоремы 1а и 2а к факторкольцу $\mathfrak{o}/\mathfrak{m}$.)

§ 125. Длина примарного идеала. Цепи примарных идеалов в нётеровых кольцах

Теорема 1 и 2 (§ 124) и их варианты были использованы в упоминавшейся работе Крулля для доказательства теорем об обрыве цепей простых идеалов

$$\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \dots$$

Прежде чем обратиться к этим теоремам, нам нужно ввести понятие длины примарного идеала.

Пусть $\mathfrak{q}$ — примарный идеал, ассоциированный с простым идеалом $\mathfrak{p}$ в нётеровом кольце $\mathfrak{o}$. Ряд примарных идеалов, ассоциированных с одним и тем же простым идеалом $\mathfrak{p}$, оканчивающийся идеалом $\mathfrak{q}$,

$$\mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \dots \supset \mathfrak{q}_l = \mathfrak{q},$$

называется *собственным нормальным рядом данного примарного идеала*. Слово «собственный» употребляется здесь для указания на то, что каждый последующий идеал является в данном ряде собственным делителем предыдущего. Число l называется *длиной* нормального ряда. Если в ряд нельзя более вставить ни одного примарного идеала, то он называется *композиционным рядом примарного идеала* $\mathfrak{q}$.

Докажем, что каждый нормальный ряд примарного идеала $\mathfrak{q}$ может быть уплотнен до некоторого композиционного ряда и что все композиционные ряды имеют одну и ту же длину. Она называется *длиной примарного идеала* $\mathfrak{q}$.

Для доказательства можно ограничиться случаем, когда $\mathfrak{q}$ — нулевой идеал. Общий случай сводится к этому переходом к кольцу классов вычетов по идеалу $\mathfrak{q}$. При таком гомоморфизме все идеалы, делившие $\mathfrak{q}$, станут делителями идеала $\mathfrak{p}$.

Ситуация упрощается еще больше, если перейти к кольцу частных $\mathfrak{o}' = \frac{\mathfrak{o}}{S}$, где S — множество элементов из $\mathfrak{o}$, не делящихся на $\mathfrak{p}$. Все собственные делители идеала $\mathfrak{p}$ при расширении $\mathfrak{o}$ до $\mathfrak{o}'$ переходят в единичный идеал $\mathfrak{o}'$; только $\mathfrak{p}$ переходит в отличный от $\mathfrak{o}'$ простой идеал $\mathfrak{p}'$. Так как каждый простой идеал в $\mathfrak{o}'$ является расширением некоторого простого идеала из $\mathfrak{o}$ (а именно — своего сужения), то в кольце $\mathfrak{o}'$ существует только один простой идеал $\mathfrak{p}'$, если не считать само $\mathfrak{o}'$. Поэтому в представление пересечением любого идеала $\mathfrak{m}' \neq \mathfrak{o}'$ может входить только один примарный идеал (ассоциированный с простым идеалом $\mathfrak{p}'$), т. е.:

В кольце $\mathfrak{o}'$ каждый идеал, отличный от $\mathfrak{o}'$, является примарным относительно простого идеала $\mathfrak{p}'$.

Начиная с этого места, кольцо $\mathfrak{o}'$ и идеал $\mathfrak{p}'$ обозначим через $\mathfrak{o}$ и $\mathfrak{p}$. Рассмотрим $\mathfrak{o}$ как аддитивную группу с областью операторов $\mathfrak{o}$. Допустимыми подгруппами являются тогда идеалы в $\mathfrak{o}$, т. е. само кольцо $\mathfrak{o}$ и идеалы, примарные относительно простого идеала $\mathfrak{p}$. Каждый собственный нормальный ряд в смысле теории групп

$$\mathfrak{o} \supset \mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \ldots \supset \mathfrak{q}_l = (0)$$

после отбрасывания начального члена $\mathfrak{o}$ дает собственный нормальный ряд примарного идеала $\mathfrak{q}_l = (0)$.

В главе 6 было доказано следующее утверждение: если в группе с операторами существует композиционный ряд, то каждый нормальный ряд можно уплотнить до некоторого композиционного ряда и все композиционные ряды имеют одну и ту же длину l. Поэтому нам нужно лишь доказать, что существует хоть один композиционный ряд.

Для этого построим нормальный ряд

$$\mathfrak{p} \supset \mathfrak{p}^2 \supset \ldots \supset \mathfrak{p}^\rho = (0).$$

Факторгруппу $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ можно рассматривать как векторное пространство с $\mathfrak{o}/\mathfrak{p}$ в качестве области операторов. Так как идеал $\mathfrak{p}$ максимален, факторкольцо $\mathfrak{o}/\mathfrak{p}$ является полем. Так как идеал $\mathfrak{p}^k$ имеет конечный базис, то указанное векторное пространство конечномерно; следовательно, существует конечный композиционный ряд от $\mathfrak{p}^k$ до $\mathfrak{p}^{k+1}$. Если для $k = 1, 2, \ldots, \rho - 1$ записать соответствующие композиционные ряды друг за другом от $\mathfrak{p}$ до (0), то получится требуемое.

Все теоремы Крулля о цепях простых идеалов опираются на следующую основную теорему:

Теорема о главных идеалах. *Если $(b) \neq \mathfrak{o}$ — главный идеал и $\mathfrak{p}$ — изолированный простой идеал, соответствующий (b), то любая собственная цепь простых идеалов*

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \ldots$$

обрывается уже на $\mathfrak{p}_1$.

Доказательство. Предположим, что существует цепь вида

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2. \tag{1}$$

С помощью перехода к кольцу классов вычетов по модулю $\mathfrak{p}_2$ можно сделать $\mathfrak{p}_2$ равным нулевому идеалу. При этом получится так, что само кольцо не будет содержать делителей нуля. Перейдем к кольцу частных $\frac{\mathfrak{o}}{S}$, где S — множество элементов из $\mathfrak{o}$, не делящихся на $\mathfrak{p}$; тогда все не делящиеся на $\mathfrak{p}$ элементы станут обратимыми, а делящиеся на $\mathfrak{p}$ идеалы из цепи (1) останутся

различными и простыми. Кольцо частных, которое мы вновь обозначим через $\mathfrak{o}$, содержит единицу и не имеет делителей нуля. Так как все простые идеалы, принадлежащие (b), переходят, за исключением $\mathfrak{p}$, в единичный идеал, то (b) является примарным идеалом для $\mathfrak{p}$. Равным образом, все делители идеала (b), кроме $\mathfrak{o}$, являются примарными для простого идеала $\mathfrak{p}$. При переходе к кольцу частных теория идеалов в $\mathfrak{o}$ существенно упрощается, что облегчает дальнейшее доказательство.

Обозначим через $\mathfrak{p}_1^{(r)}$, как и раньше, r-ю символическую степень идеала $\mathfrak{p}_1$. Идеалы цепи

$$(\mathfrak{p}_1^{(1)},\ b) \supseteq (\mathfrak{p}_1^{(2)},\ b) \supseteq \dots$$

являются делителями элемента b, а потому, в соответствии с отмеченным выше, эти идеалы примарны относительно простого идеала $\mathfrak{p}$. Число различных идеалов в этой цепи не может быть больше, чем длина примарного идеала (b); поэтому, начиная с некоторого места, идеалы в цепи станут равными:

$$(\mathfrak{p}_1^{(s)},\ b) = (\mathfrak{p}_1^{(s+1)},\ b) = \dots$$

Пусть теперь $m \geqslant s$. Докажем сначала, что

$$\mathfrak{p}_1^{(m)} \subseteq (b\mathfrak{p}_1^{(m)},\ \mathfrak{p}_1^{(m+1)}). \tag{2}$$

Действительно, пусть x — элемент из $\mathfrak{p}_1^{(m)}$. Тогда

$$x \in (\mathfrak{p}_1^{(m)},\ b) = (\mathfrak{p}_1^{(m+1)},\ b),$$

в силу чего

$$x = y + br, \text{ где } y \in \mathfrak{p}_1^{(m+1)},$$

так что

$$br = x - y \equiv 0\ (\mathfrak{p}_1^{(m)}).$$

По определению, идеал $\mathfrak{p}_1^{(m)}$ является примарным и элемент b не делится на соответствующий простой идеал $\mathfrak{p}_1$; следовательно, элемент r должен делиться на $\mathfrak{p}_1^{(m)}$. Отсюда

$$x = y + br \equiv 0\ (\mathfrak{p}_1^{m+1},\ b\mathfrak{p}_1^{(m)}),$$

чем и доказывается (2).

Согласно теореме 1б (§ 124), из (2) следует включение

$$\mathfrak{p}_1^{(m)} \subseteq \mathfrak{p}_1^{(m+1)},$$

так что $\mathfrak{p}_1^{(m)} = \mathfrak{p}_1^{(m+1)}$ для всех $m \geqslant s$, т. е.

$$\mathfrak{p}_1^{(s)} = \mathfrak{p}_1^{(s+1)} = \mathfrak{p}_1^{(s+2)} = \dots \tag{3}$$

Кольцо $\mathfrak{o}$ не имеет делителей нуля. Согласно теореме 3 (§ 124) пересечение символических степеней идеала $\mathfrak{p}_1$ является нулевым

идеалом. Таким образом, из (3) следует

$$\mathfrak{p}_1^{(s)} = (0). \tag{4}$$

Однако степень $\mathfrak{p}_1^{(s)}$ является примарным идеалом относительно простого идеала $\mathfrak{p}_1$, в то время как (0) является простым идеалом $\mathfrak{p}_2$ Получилось противоречие. Следовательно, любая цепь вида (1) невозможна.

С помощью повторного применения теоремы о главных идеалах Крулль доказал следующее обобщение:

Если $\mathfrak{p}$ — *изолированный простой идеал, принадлежащий идеалу* $\mathfrak{m} = (b_1, \ldots, b_r)$, $\mathfrak{m} \neq \mathfrak{o}$, *то любая собственная цепь простых идеалов*

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \ldots \tag{5}$$

обрывается не позднее, чем на $\mathfrak{p}_r$.

В частности, эта теорема имеет место тогда, когда

$$\mathfrak{m} = \mathfrak{q} = (b_1, \ldots, b_r)$$

— примарный идеал и $\mathfrak{p}$ — соответствующий простой идеал. Так как каждый идеал имеет конечный базис, оказывается справедливым следующее утверждение:

Каждая собственная цепь простых идеалов (5) *обрывается на конечном шаге.*

По поводу доказательства и применения результатов к теории локальных колец можно рекомендовать упомянутую выше книгу Норткотта.