

Н. Бурбаки

Коммутативная алгебра

**Москва
«Книга по Требованию»**

УДК 51
ББК 22.1
Б91

Б91 **Бурбаки Н.**
Коммутативная алгебра / Н. Бурбаки – М.: Книга по Требованию, 2012. –
708 с.

ISBN 978-5-458-31413-8

ISBN 978-5-458-31413-8

© Издание на русском языке, оформление
«YOYO Media», 2012

© Издание на русском языке, оцифровка,
«Книга по Требованию», 2012

Эта книга является репринтом оригинала, который мы создали специально для Вас, используя запатентованные технологии производства репринтных книг и печати по требованию.

Сначала мы отсканировали каждую страницу оригинала этой редкой книги на профессиональном оборудовании. Затем с помощью специально разработанных программ мы произвели очистку изображения от пятен, клякс, перегибов и попытались отбелить и выровнять каждую страницу книги. К сожалению, некоторые страницы нельзя вернуть в изначальное состояние, и если их было трудно читать в оригинале, то даже при цифровой реставрации их невозможно улучшить.

Разумеется, автоматизированная программная обработка репринтных книг – не самое лучшее решение для восстановления текста в его первозданном виде, однако, наша цель – вернуть читателю точную копию книги, которой может быть несколько веков.

Поэтому мы предупреждаем о возможных погрешностях восстановленного репринтного издания. В издании могут отсутствовать одна или несколько страниц текста, могут встретиться невыводимые пятна и кляксы, надписи на полях или подчеркивания в тексте, нечитаемые фрагменты текста или загибы страниц. Покупать или не покупать подобные издания – решать Вам, мы же делаем все возможное, чтобы редкие и ценные книги, еще недавно утраченные и несправедливо забытые, вновь стали доступными для всех читателей.

ВВЕДЕНИЕ

Вопросы, рассматриваемые в предлагаемой книге, появились при развитии теории алгебраических чисел и (позднее) алгебраической геометрии (см. исторический очерк). Большое сходство этих теорий обнаружилось еще в XIX веке. В процессе работы над возникшими в них проблемами был сформулирован ряд общих идей, область применения которых не ограничивается кольцами алгебраических функций, и, как обычно, чтобы глубже понять истинное значение и связи объектов, лучше всего рассмотреть их в наиболее общей форме. Поэтому в нашей книге обсуждаются понятия, которые можно применить в принципе ко всем коммутативным кольцам и модулям над ними. Следует, однако, подчеркнуть, что результаты часто получаются при предположениях о *конечности* (всегда выполняющихся в классическом случае), например при условии, что модули имеют конечный тип или рассматриваются над нётеровыми кольцами.

Изложение первых глав группируется в основном вокруг следующих понятий.

I. *Локализация и глобализация.* Обратимся, например, к системе диофантовых уравнений

$$P_i(x_1, \dots, x_m) = 0 \quad (1 \leq i \leq n), \quad (*)$$

где P_i — многочлены с целыми рациональными коэффициентами и где требуется найти решения (x_i) , образованные *целыми* рациональными числами. К этой задаче можно приступить, отыскивая решения, образованные *рациональными числами*. Такой подход приводит к аналогичной задаче, где коэффициенты многочленов P_i рассматриваются как элементы *поля частных* $\mathbf{Q}$ кольца $\mathbf{Z}$ и надо найти решения в поле $\mathbf{Q}$. Следующий этап заключается в выяснении вопроса о существовании рациональных решений, знаменатели которых не делятся на заданное простое число p (очевидно, что *целые* решения этому условию удовлетворяют). На этот раз мы приходим к подкольцу $\mathbf{Z}_{(p)}$ в поле $\mathbf{Q}$; состоящему из рациональных чисел указанного вида; оно называется *локальным кольцом* кольца $\mathbf{Z}$, соответствующим простому числу p . Ясно, что переход от кольца $\mathbf{Z}$ к полю $\mathbf{Q}$ и переход от кольца $\mathbf{Z}$ к кольцу $\mathbf{Z}_{(p)}$ имеют одинаковую природу: в обоих случаях в знаменатели допускаются только те числа, которые не принадлежат некоторому *простому идеалу* (в данном

случае — идеалу (0) или идеалу (p)). Само понятие «локальное кольцо» происходит из алгебраической геометрии, где оно возникает наиболее естественным образом: например, в кольце $C(X)$ рациональных функций от одной переменной с комплексными коэффициентами локальное кольцо, соответствующее простому идеалу $(X - \alpha)$, является кольцом рациональных дробей, регулярных в точке α (т. е. не имеющих в этой точке полюса).

Всякая диофантова задача и, если говорить более общим языком, задача об A -модулях (A — коммутативное кольцо) может быть разложена на две части: в первой надо найти решение в локальных кольцах A_p , соответствующих различным простым идеалам p кольца A («локализация»), а во второй — выяснить, следует ли из существования решения «локализованной» задачи при *всяком* p существование решения исходной задачи («переход от локального случая к глобальному»). Именно этим двум процессам посвящена гл. II, где, впрочем, мы видим, что локализация связана не только с простыми идеалами, но может иметь более общую природу.

II. *Пополнение локальных колец.* Любое локальное кольцо A , подобно полю, обладает *единственным* максимальным идеалом $\mathfrak{m}$. С помощью этого факта задача об A -модулях сводится в некоторой степени к аналогичной задаче о *векторных пространствах*: сведение состоит в переходе к факторкольцу $A/\mathfrak{m}$, являющемуся полем. Если, например, вернуться к диофантовой системе (*), то указанная идея станет не чем иным, как появившимся еще в первых работах по теории чисел принципом «редукции по модулю p », согласно которому уравнения переводятся в сравнения $\bmod p$.

Очевидно, однако, что нельзя ожидать получения на таком пути полных результатов для исходной задачи. Чтобы иметь более точные сведения об искомом ответе, надо рассматривать не только сравнения по модулю $\mathfrak{m}$, но и «высшие» сравнения по модулю $\mathfrak{m}^n$ при всевозможных целых $n > 0$: чем больше n , тем «ближе» мы, в некотором смысле, к данной задаче (возьмем, например, случай $A = \mathbb{Z}$: любое отличное от нуля целое число не может делиться на *все* степени p^n заданного простого числа p ; следовательно, если n будет взято достаточно большим, то после редукции $\bmod p^n$ целое число будет отлично от нуля). Математическое выражение этой идеи состоит в рассмотрении *топологии* на кольце A (*Общая топология*, 1969, гл. III, § 6¹⁾),

¹⁾ Автором книг, на которые делаются такого вида ссылки, является Н. Бурбаки. Ссылки цитируются по-русски или по-французски в зависимости от того, вышел ли уже соответствующий русский перевод или нет. В последнем случае мы по возможности старались помочь читателю подстрочными примечаниями. — *Прим. перев.*

в которой идеалы $\mathfrak{m}^n$ образуют фундаментальную систему окрестностей нуля. Дело в том, что если, например, система сравнений

$$P_i(x_1, \dots, x_m) \equiv 0 \pmod{p^k} \quad (1 \leq i \leq n) \quad (**)$$

решена при всех целых $k > 0$, то отсюда еще не следует, что система уравнений (*) имеет решение в локальном кольце $\mathbf{Z}_{(p)}$; отсюда можно лишь сделать заключение о существовании решения этой системы в *пополнении* $\mathbf{Z}_{(p)}$ топологического кольца $\mathbf{Z}_{(p)}$.

Ослабленная таким образом исходная задача свелась, наконец, к аналогичному вопросу для локальных колец типа $A/\mathfrak{m}^n$; они еще больше похожи на поля, чем локальные кольца общего вида, так как содержат лишь нильпотентный радикал. В классической алгебраической геометрии это соответствует «дифференциальному» изучению вопроса в окрестности заданной точки.

В гл. III рассматриваются в общем виде эти приложения топологических понятий к теории локальных колец. В гл. VI изучаются более специальные вопросы, связанные с более тонкими рассмотрениями из алгебраической геометрии и, в особенности, с арифметикой полей алгебраических чисел; встречающиеся там локальные кольца (такие, как $\mathbf{Z}_{(p)}$) принадлежат к наиболее простому классу «колец нормирования», в которых делимость является отношением совершенного *предпорядка* в множестве главных идеалов (Алгебра, гл. VI, § 1).

Сравнивая переход от кольца A к его локализации A_p с переходом от A к пополнению $\bar{A}$, мы обнаруживаем сходство этих операций. Оба A -модуля — как A_p , так и $\bar{A}$ — являются *плоскими*. Тензорными произведениями таких A -модулей с произвольными можно оперировать в некотором смысле так же, как тензорными произведениями векторных пространств, т. е. без всяких предосторожностей, необходимых при рассмотрении тензорных произведений в общем случае. Вопросы, связанные с понятием плоского модуля, которое применимо, впрочем, и к модулям над некоммутативными кольцами, изучаются в гл. I.

III. *Целые элементы и разложение идеалов*. Для исследования делимости в полях алгебраических чисел с самого начала оказывается необходимым введение понятия *целого элемента* в таком поле K , обобщающего понятия целого рационального числа в поле $\mathbf{Q}$. Общая теория «целых алгебраических элементов» связана, как мы это увидим, с очень строгими условиями конечности; она развивается в гл. V. Эта теория применяется при рассмотрении *всевозможных* коммутативных колец и представляет большой интерес не только для арифметики, но и для алгебраической геометрии и даже для современной теории «аналитических пространств» над полем $\mathbf{C}$.

Одна из основных трудностей, с которой приходилось сталкиваться при распространении классической арифметики на кольца целых алгебраических элементов, с давних пор заключалась в том, что классическое разложение целого рационального числа на простые множители не переносится, вообще говоря, на кольца указанного типа. Чтобы преодолеть эту трудность, потребовалось создание теории идеалов; для идеалов снова имеется искомое однозначное разложение, причем, разумеется, понятие простого числа заменяется понятием простого идеала. Это можно рассматривать как типичный случай, в котором «переход от локального к глобальному» приводит к удовлетворительному результату: зная для некоторого $x \in K$ значения в x всех «нормирований» поля K , можно восстановить по ним x с точностью до целого обратимого множителя.

Однако результат об однозначном разложении идеала в произведение простых перестает быть верным в кольцах более сложных, чем кольца алгебраических чисел (и даже, кстати сказать, в кольцах многочленов от нескольких переменных). Тем не менее с каждым идеалом можно связать некоторым каноническим образом множество вполне определенных простых идеалов; в алгебраической геометрии, например, если рассматривать в n -мерном аффинном пространстве K^n (K — какое-нибудь поле) подмногообразие, определенное системой полиномиальных уравнений $P_\alpha = 0$, то неприводимые компоненты этого подмногообразия взаимно однозначно соответствуют минимальным элементам множества простых идеалов, которые упомянутым образом связаны с идеалом, порожденным многочленами P_α . Можно, кроме того (если ограничиться нётеровыми кольцами), для каждого идеала задать «разложение», не столь точное, как в произведение простых идеалов; произведения в этом случае заменяются пересечениями, а степени простых идеалов — идеалами «примарными», связанными с теми простыми идеалами, которые в свою очередь ассоциированы с рассматриваемым идеалом (примарные идеалы, однако, не являются прямым обобщением степеней простых). Введение простых идеалов, ассоциированных с данным идеалом, и изучение их свойств составляют содержание гл. IV; там же устанавливается существование упомянутого выше «примарного разложения» и рассматриваются некоторые свойства его единственности. В настоящее время, однако, уже ясно, что это разложение играет в приложениях лишь второстепенную роль, а главным объектом является простой идеал, ассоциированный с данным идеалом.

В гл. VII более детально изучаются кольца, которые в том, что касается разложения в произведение простых идеалов, еще больше похожи на кольца целых алгебраических чисел; кроме

того, в этих кольцах оказывается возможным ввести понятие *дивизора*, которое дает геометрическую интерпретацию указанного разложения и играет важную роль в алгебраической геометрии.

Наконец, гл. VIII и следующие будут посвящены вопросам, представляющим для алгебраической геометрии больший интерес, чем для арифметики (в которой они становятся тривиальными), а именно вопросам *размерности*.

Эти понятия находятся на границе алгебраической геометрии в собственном смысле — границе, которая всегда подвижна и которую трудно провести. Дело в том, что коммутативная алгебра является чрезвычайно важным инструментом для развития алгебраической геометрии во всей ее общности; и наоборот (как это уже можно было заметить выше), язык геометрий оказывается необыкновенно удобным для теорем коммутативной алгебры и очень полезным для создания некоторой интуиции, которая, по понятным причинам, в значительной мере отсутствует в абстрактной алгебре. Вместе с современной тенденцией все большего и большего расширения рамок алгебраической геометрии наблюдается как никогда сильное стремление к слиянию алгебраического и геометрического языков.

ГЛАВА I¹⁾

ПЛОСКИЕ МОДУЛИ

В этой главе, если не оговорено противное, предполагается, что все рассматриваемые кольца содержат единичный элемент, а все гомоморфизмы переводят единичный элемент в единичный. Подкольцом кольца A считается такое подкольцо, которое содержит единичный элемент из A .

Если A — кольцо, M — левый A -модуль и U (соответственно V) — некоторая аддитивная подгруппа кольца A (соответственно модуля M), то через UV или $U \cdot V$ обозначается аддитивная подгруппа модуля M , порожденная произведениями $u \cdot v$, где $u \in U$, $v \in V$ (Алгебра, гл. VIII, § 6, п° 1). Если $\mathfrak{a}$ — идеал кольца A , то будем считать, что $\mathfrak{a}^0 = A$. Для всякого множества E через 1_E (или через 1 , если не грозит путаница) обозначается тождественное отображение множества E на себя.

Напомним, что аксиомы модулей включают в себя требование о том, что если E — левый (соответственно правый) A -модуль над кольцом A и если 1 — единичный элемент кольца A , то $1 \cdot x = x$ (соответственно $x \cdot 1 = x$) для всякого $x \in E$ (Алгебра, чар. II, 3^e éd, § 1, п° 1)²⁾. Если E и F — два левых (соответственно правых) A -модуля, то через $\text{Hom}_A(E, F)$ (или просто через $\text{Hom}(E, F)$) обозначается аддитивная группа гомоморфизмов модуля E в модуль F (loc. cit., § 1, п° 2)³⁾. Для краткости через 0 обозначается модуль, состоящий только из одного нулевого элемента.

§ 1. Диаграммы и точные последовательности

1. Диаграммы

Пусть, например, A, B, C, D, E — пять множеств, и пусть f — отображение из A в B , g — отображение из B в C , h — отображение из D в E , u — отображение из B в D и v — отображение

¹⁾ Материал этой главы, за исключением § 4, не зависит ни от одной другой книги второй части.

²⁾ См. также Алгебра, гл. II § 1, п° 2. — Прим. перев.

³⁾ См. также Алгебра, гл. II, § 2, п° 1, где гомоморфизм называется линейным отображением. — Прим. перев.

из C в E . Для того чтобы кратко описать такую ситуацию, часто используют диаграммы; в частности, наш пример может быть описан с помощью следующей диаграммы (Теория множеств, гл. II, § 3, п° 4):

$$\begin{array}{ccc} A & \xrightarrow{f} B & \xrightarrow{g} C \\ \downarrow u & & \downarrow v \\ D & \xrightarrow{h} & E \end{array} \quad (1)$$

В такой диаграмме запись $A \xrightarrow{f} B$ схематически выражает тот факт, что f является отображением множества A в множество B . Когда речь идет только об отображении f , буква f опускается и пишут просто $A \rightarrow B$.

Когда A, B, C, D, E — группы (соответственно коммутативные группы) и f, g, h, u, v — гомоморфизмы групп, то для краткости говорят, что диаграмма (1) есть *диаграмма групп* (соответственно *диаграмма коммутативных групп*).

Строго говоря, диаграмма не является математическим объектом; она всего лишь *рисунок*, предназначенный для того, чтобы облегчить чтение того или иного рассуждения. На практике диаграммы часто вводятся как *символы сокращения*, избавляющие от перечисления всех множеств и отображений, которые требуется рассмотреть. Вместо того чтобы сказать «Пусть A, B, C, D, E — пять множеств ... и v — отображение из C в E », часто говорят: «Рассмотрим диаграмму (1)» (см., например, формулировку предложения 1 п° 4).

2. Коммутативные диаграммы

Рассмотрим для примера следующую диаграмму:

$$\begin{array}{ccccccc} A & \xrightarrow{f} B & \xrightarrow{g} C & \xrightarrow{h} D \\ a \downarrow & b \downarrow & c \downarrow & d \downarrow \\ A' & \xrightarrow{f'} B' & \xrightarrow{g'} C' & \xrightarrow{h'} D' \end{array} \quad (2)$$

Каждому пути, составленному из некоторого числа отрезков диаграммы и пробегаемому в том направлении, которое указано стрелками, ставится в соответствие отображение множества, стоящего в начале первого отрезка, в множество, стоящее в конце последнего, а именно композиция отображений, представляемых пробегаемыми отрезками. При этом считается, что для любой вершины диаграммы, например вершины B , имеется путь, состоящий из одной этой вершины, и ему соответствует тождественное отображение 1_B .

В диаграмме (2), например, есть три пути, начинающиеся в A и кончающиеся в C' ; им соответствуют отображения $c \circ g \circ f$, $g' \circ b \circ f$ и $g' \circ f' \circ a$. Говорят, что диаграмма *коммутативна*, если для любых двух ее путей, имеющих общее начало и общий конец, соответствующие отображения равны; например, если у кого-то пути совпадают начало и конец, то соответствующее отображение должно быть тождественным.

Для того чтобы диаграмма (2) была коммутативна, необходимо и достаточно, чтобы выполнялись следующие соотношения:

$$f' \circ a = b \circ f, \quad g' \circ b = c \circ g, \quad h' \circ c = d \circ h; \quad (3)$$

иначе говоря, необходимо и достаточно, чтобы три квадратные диаграммы из диаграммы (2), взятые порознь, были коммутативны. Действительно, из соотношений (3) следует, что $c \circ g \circ f = g' \circ b \circ f$, так как $c \circ g = g' \circ b$, и что $g' \circ b \circ f = g' \circ f' \circ a$, так как $b \circ f = f' \circ a$; следовательно, все три пути, начинающиеся в A и заканчивающиеся в C' , дают одно и то же отображение. Так же проверяется, что четыре пути с началом в A и с концом в D' (соответственно три пути с началом в B и с концом в D') дают одно и то же отображение. Соотношения (3) означают, что отображения, соответствующие путям с началом в A (соответственно в B, C) и концом в B' (соответственно в C', D') одинаковы. Все другие пары вершин диаграммы (2) могут быть соединены только одним путем, так что она коммутативна.

В дальнейшем мы будем представлять читателю формулировку и проверку аналогичных результатов для других видов диаграмм.

3. Точные последовательности

Напомним (*Algèbre*, chap. II, 3^e éd., § 1, n° 4) следующее определение:

ОПРЕДЕЛЕНИЕ. Пусть A — кольцо, F, G, H — три правых (соответственно левых) A -модуля, f — гомоморфизм модуля F в G и g — гомоморфизм модуля G в H . Говорят, что пара (f, g) составляет точную последовательность, если $g^{-1}(0) = f(F)$, т. е. если ядро гомоморфизма g равно образу гомоморфизма f .

В этом случае говорят также, что диаграмма

$$F \xrightarrow{f} G \xrightarrow{g} H \quad (4)$$

является *точной последовательностью*.

Рассмотрим аналогичным образом диаграмму, образованную четырьмя модулями и тремя гомоморфизмами:

$$E \xrightarrow{f} F \xrightarrow{g} G \xrightarrow{h} H \quad (5)$$

Эта диаграмма называется *точной в члене F* , если диаграмма $E \xrightarrow{f} F \xrightarrow{g} G$ представляет собой точную последовательность; если же диаграмма $F \xrightarrow{g} G \xrightarrow{h} H$ — точная последовательность, то данная диаграмма (5) называется *точной в члене G* . Если она точна и в члене F , и в члене G , то говорят, что диаграмма (5) *точна* или что она является *точной последовательностью*. Тем же способом определяются точные последовательности с любым числом членов.

Напомним также следующие результаты (loc. cit.). Пусть E, F, G — правые (соответственно левые) A -модули, стрелки обозначают гомоморфизмы и 0 — модуль, состоящий только из нулевого элемента. Тогда

а) утверждение, что $0 \rightarrow E \xrightarrow{f} F$ является точной последовательностью, равносильно утверждению, что гомоморфизм f *инъективен*;

б) утверждение, что последовательность $E \xrightarrow{f} F \rightarrow 0$ точна, эквивалентно утверждению, что гомоморфизм f *сюръективен*;

в) утверждение, что последовательность $0 \rightarrow E \xrightarrow{f} F \rightarrow 0$ точна, эквивалентно утверждению, что гомоморфизм f *биективен*, т. е. что f — *изоморфизм* модуля E на модуль F ;

г) если F является подмодулем модуля E , i — канонический инъективный гомоморфизм модуля F в E , а p — канонический сюръективный гомоморфизм модуля E на E/F , то диаграмма

$$0 \rightarrow F \xrightarrow{i} E \xrightarrow{p} E/F \rightarrow 0 \quad (6)$$

представляет собой точную последовательность;

д) для произвольного гомоморфизма $f: E \rightarrow F$ диаграмма

$$0 \rightarrow f^{-1}(0) \xrightarrow{i} E \xrightarrow{f} F \xrightarrow{p} F/f(E) \rightarrow 0, \quad (7)$$

в которой i — канонический инъективный гомоморфизм подмодуля $f^{-1}(0)$ в E , а p — канонический сюръективный гомоморфизм модуля F на $F/f(E)$, есть точная последовательность;

е) для того чтобы диаграмма

$$E \xrightarrow{f} F \xrightarrow{g} G \quad (8)$$

была точной последовательностью, необходимо и достаточно, чтобы существовали такие модули S, T и гомоморфизмы $a: E \rightarrow S, b: S \rightarrow F, c: F \rightarrow T$ и $d: T \rightarrow G$, что $f = b \circ a, g = d \circ c$ и три последовательности

$$\begin{aligned} E &\xrightarrow{a} S \rightarrow 0 \\ 0 &\rightarrow S \xrightarrow{b} F \xrightarrow{c} T \rightarrow 0 \\ 0 &\rightarrow T \xrightarrow{d} G \end{aligned} \quad (9)$$

точны,