Н. Бурбаки

Алгебра

Часть 3. Модули, кольца, формы

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Н11

Н. Бурбаки
Н11 Алгебра: Часть 3. Модули, кольца, формы / Н. Бурбаки – М.: Книга по Требованию, 2021. – 554 с.

ISBN 978-5-458-31377-3

Группа французских математиков, объединенных под псевдонимом "Бурбаки", поставила перед собой цель — написать под общим заглавием "Элементы математики" полный трактат по современной математике. Многие выпуски этого трактата уже вышли во Франции, вызвав большой интерес математиков всего мира.Книга рассчитана на математиков — научных работников, аспирантов и студентов старших курсов университетов и пединститутов.

ISBN 978-5-458-31377-3

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.

Серия Книжный Ренессанс
www.samizday.ru/reprint

ГЛАВА VII
МОДУЛИ НАД КОЛЬЦАМИ ГЛАВНЫХ ИДЕАЛОВ

Если не оговорено противное, все кольца, рассматриваемые в этой главе, предполагаются коммутативными и имеющими единицу, а модули — унитарными.

§ 1. Кольца главных идеалов

1. Определение кольца главных идеалов

Определение 1. *Кольцо A называется кольцом главных идеалов, если оно является кольцом целостности* (гл. I, § 8, n° 3, определение 3) *с единицей и всякий его идеал — главный.*

Примеры. Кольцо Z целых рациональных чисел является кольцом главных идеалов (гл. I, § 8, n° 5, пример 4). Кольцо $K[X]$ многочленов от одного переменного над полем K является кольцом главных идеалов (гл. V, IV, § 1, n° 5, предложение 7); таковым же будет и кольцо $K[[X]]$ формальных степенных рядов, так как всякий идеал этого кольца имеет вид (X^n) (гл. IV, § 5, n° 7). Кольцо целых p-адических чисел является кольцом главных идеалов.

Пусть $Q(i)$ — поле, полученное из поля Q рациональных чисел присоединением корня i неприводимого многочлена X^2+1. Элементы этого поля $a+bi$, где a и b — целые рациональные числа, образуют подкольцо A поля $Q(i)$, называемое «кольцом целых гауссовых чисел» и являющееся кольцом главных идеалов (упражнение 7).

Напротив, в поле $Q(\varrho)$, где ϱ — корень многочлена X^2+5, подкольцо B, составленное из элементов вида $a+b\varrho$ (a и b — целые рациональные), не будет кольцом главных идеалов.

Кольцо $K[X, Y]$ многочленов от двух переменных над полем K не является кольцом главных идеалов, так как только ненулевые константы делят одновременно X и Y, но ни одна из них не будет образующей идеала, порожденного X и Y.

2. *Делимость в кольцах главных идеалов*

Пусть A — кольцо главных идеалов, K — его поле дробей; ранее мы видели, что упорядоченная группа $\mathcal{F}^*$ главных дробных идеалов (гл. VI, § 1, n° 5) поля K решеточно упорядочена. Более точно:

Предложение 1. *Пусть K — поле дробей кольца главных идеалов A и $(x_\iota)_{\iota \in I}$ — семейство элементов K с общим знаменателем $b \in K^*$ (то есть $bx_\iota \in A$ при любом ι). Тогда:*

1) *Семейство (x_ι) имеет н. о. д. в K.*

2) *Всякий н.о.д. семейства (x_ι) имеет вид $d = \sum_\iota a_\iota x_\iota$, где a_ι — элементы кольца A, причем лишь конечное число их отлично от нуля.*

Действительно, идеал $\sum_\iota Abx_\iota$ кольца A — главный и, следовательно, имеет вид Ad'. Положим $d' = bd$. Из равенства $d' = \sum_\iota a_\iota bx_\iota$ следует $d = \sum_\iota a_\iota b_\iota$, так что всякий общий делитель элементов x_ι делит d. С другой стороны, bd, очевидно, общий делитель элементов bx_ι, и поэтому d является общим делителем элементов x_ι, что и требовалось доказать.

Замечание. Предложение 1 применимо также к любому семейству (x_ι) элементов кольца A (достаточно взять $b = 1$), а также к любому *конечному* семейству (x_ι) элементов K (в самом деле, если $x_\iota = c_\iota b_\iota^{-1}$, $c_\iota \in A$, $b_\iota \in A$, то в качестве b достаточно взять произведение всех b_ι).

Следствие. *Пусть (x_ι) — произвольное семейство элементов в подкольце главных идеалов A кольца целостности и d — н. о. д. этого семейства в A. Тогда семейство (x_ι) обладает н. о. д. в B и d является одним из этих н. о. д.*

В самом деле, d является общим делителем элементов x_ι в B. С другой стороны, равенство $d = \sum_\iota a_\iota x_\iota$ $(a_\iota \in A)$ показывает, что всякий общий делитель элементов x_ι в B делит d.

Важным применением этого следствия является тот случай, когда $A = K[X]$, $B = E[X]$, где K — некоторое поле, E — его расширение.

Первое утверждение предложения 1 означает, что группа $\mathfrak{P}^*$ *решеточно упорядочена* (гл. VI, § 1, n° 9). В частности, всякое конечное семейство элементов поля K обладает н. о. к. Следовательно, к кольцам главных идеалов можно применять результаты гл. VI, n°n° 9, 10, 11 и 12, отмеченные знаком (ДЕЛ).

Из второго утверждения предложения 1 следует

Теорема 1 («тождество Безу»). *Для того чтобы элементы x_ι ($\iota \in I$) кольца главных идеалов A были в совокупности независимы, необходимо и достаточно, чтобы существовали такие элементы a_ι ($\iota \in I$) кольца A, что $\sum_\iota a_\iota x_\iota = 1$, причем лишь конечное число a_ι отлично от нуля.*

Необходимость этого условия следует из предложения 1. Обратно, если $\sum_\iota a_\iota x_\iota = 1$, то всякий общий делитель элементов x_ι делит 1, и следовательно, 1 — н. о. д. этих элементов.

Предложение 2. *Пусть a, b, d, m и p — элементы поля дробей K кольца главных идеалов A. Тогда следующие утверждения равносильны:*

1) *«d — н. о. д. элементов a и b» и «$(d) = (a) + (b)$».*

2) *«m — н. о. к. элементов a и b» и «$(m) = (a) \cap (b)$».*

3) *«p — экстремальный элемент A» и «(p) — максимальный идеал A».*

Утверждение 1) уже доказано (предложение 1). Далее, общие кратные элементов a и b образуют идеал $(a) \cap (b)$, который, по предположению, является главным идеалом (m), то есть m — н. о. к. элементов a и b. Это доказывает утверждение 2). Наконец, первое из утверждений 3), по определению (гл. VI, § 1, n° 13), равносильно утверждению, что (p) — максимальный элемент упорядоченного по включению множества отличных от A главных идеалов кольца A. Так как все идеалы кольца A — главные, это означает, что (p) — максимальный идеал кольца A, откуда следует 3).

Сумму (соответственно пересечение) конечного числа идеалов кольца главных идеалов A называют иногда н. о. д. (соответственно н. о. к.) этих идеалов.

Предложение 3. *Пусть a, b, c — элементы поля дробей кольца главных идеалов A и d — н. о. д. элементов a и c. Сравнение*

$ax \equiv b \pmod{c}$ *имеет целое решение* $x_0 \in A$ *тогда и только тогда, когда* d *делит* b; *в этом случае все целые решения* $x \in A$ *этого сравнения совпадают с целыми решениями сравнения* $x \equiv x_0 \pmod{cd^{-1}}$.

Если $ax \equiv b \pmod{c}$ и $x \in A$, то существует такой элемент $y \in A$, что $b = ax + cy$. Следовательно, d делит b. Обратно, если d делит b, то $b = ax_0 + cy_0$, где x_0, $y_0 \in A$ (предложение 1). Поэтому $ax_0 \equiv b \pmod{c}$. Кроме того, в этом случае сравнение $ax \equiv b \pmod{c}$ равносильно сравнению $a(x - x_0) \equiv 0 \pmod{c}$; положив $a = da'$ и $c = dc'$, получим $a'(x - x_0) \equiv 0 \pmod{c'}$. Но это сравнение (для всех $x \in A$) равносильно сравнению $x - x_0 \equiv 0 \pmod{c'}$, так как a' и c' — независимые целые элементы (гл. VI, § 1, предложение 10 (ДЕЛ) и следствие 1 предложения 11 (ДЕЛ)).

Предложение 4. *Пусть* $(a_i)_{1 \leqslant i \leqslant n}$ — *конечное семейство попарно независимых элементов кольца главных идеалов* A. *Тогда фактор-кольцо* (соответственно *A-модуль*) $A/(\prod_{i=1}^{n} a_i)$ *изоморфно* (соответственно *изоморфен*) *произведению колец* (соответственно *A-модулей*) $A/(a_i)$.

Так как элемент a_n не зависит от $a_1, \ldots, a_{n-1}$ (гл. VI, § 1, n° 12, следствие 3 предложения 11 (ДЕЛ)), то индукцией по n доказательство сводится к случаю $n = 2$.

Пусть a и b — независимые элементы кольца A. Тогда $(a) + (b) = A$ и $(a) \cap (b) = (ab)$ (гл. VI, § 1, n° 12, предложение 12 (ДЕЛ)). Пусть g (соответственно h) — каноническое отображение кольца A на $A/(a)$ (соответственно на $A/(b)$). Рассмотрим отображение $f = (g, h)$ кольца A в $(A/(a)) \times (A/(b))$. Ясно, что f — гомоморфизм (структуры кольца и структуры A-модуля) и его ядро равно $(a) \cap (b) = (ab)$. Поэтому достаточно показать, что f является отображением кольца A «на» $(A/(a)) \times (A/(b))$, то есть для произвольных элементов c и d кольца A нужно доказать существование такого элемента $x \in A$, что $x \equiv c \pmod{a}$, $x \equiv d \pmod{b}$. Но в силу независимости элементов a и b существуют элементы u, $v \in A$, удовлетворяющие условию $ua + vb = 1$. Поэтому достаточно положить $x = dua + cvb$.

Заключение предложения 4 неверно без предположения о попарной независимости элементов a_i (см. § 4, предложение 6).

3. *Разложение на экстремальные элементы в кольцах главных идеалов*

Теперь мы применим к кольцам главных идеалов результаты гл. VI, § 1, n° 13, относящиеся к разложению на экстремальные элементы. По предложению 2 элемент p кольца главных идеалов A экстремален тогда и только тогда, когда кольцо $A/(p)$ является полем (гл. I, § 9, n° 3, теорема 2), то есть сравнение $ax \equiv b \pmod{p}$ имеет в A решение при любых a и b, не кратных p.

Определение 2. *Системой представителей экстремальных элементов кольца главных идеалов A называется такое семейство (p_α) экстремальных элементов, что всякий экстремальный элемент кольца A ассоциирован с одним и только одним p_α.*

Теорема 2. *Пусть A — кольцо главных идеалов и (p_α)— система представителей его экстремальных элементов. Тогда всякий ненулевой элемент x поля дробей кольца A имеет единственное представление вида*

$$x = u \prod_\alpha p_\alpha^{n_\alpha}, \tag{1}$$

где u — обратимый элемент кольца A, n_α — целые рациональные числа, из которых лишь конечное число отлично от нуля. Для того чтобы элемент x был целым, необходимо и достаточно, чтобы все n_α были положительными.

Для доказательства применим теорему о разложении в сумму экстремальных элементов (гл. VI, § 1, теорема 2 и предложение 15), наше утверждение, по существу, является ее перефразировкой. Так как группа $\mathfrak{P}^*$ решеточно упорядочена, условия упомянутой теоремы будут выполнены, если мы убедимся в том, что всякое непустое множество главных идеалов кольца A имеет максимальный элемент; но это следует из леммы:

Лемма. *Пусть A — кольцо* (быть может, некоммутативное и без единицы), *в котором всякий левый идеал имеет конечное число образующих. Тогда всякое непустое множество Φ левых идеалов кольца A, упорядоченное по включению, имеет максимальный элемент.*

В силу теоремы Цорна (Теор. мн., Рез., § 6, n° 10) достаточно доказать, что множество Φ индуктивно. Если $(\mathfrak{a}_\lambda)$ — совершенно упорядоченное множество элементов Φ, то объединение $\mathfrak{a}$ идеалов $\mathfrak{a}_\lambda$ является левым идеалом кольца A и имеет, следовательно, конечное число образующих $(a_i)_{1\leqslant i\leqslant n}$. Но всякий элемент a_i принадлежит некоторому идеалу $\mathfrak{a}_{\lambda_i}$, и так как множество $(\mathfrak{a}_\lambda)$ совершенно упорядочено, то все a_i $(1\leqslant i\leqslant n)$ входят в наибольший из идеалов $\mathfrak{a}_{\lambda_i}$, скажем $\mathfrak{a}_\mu$. Тогда $\mathfrak{a}=\mathfrak{a}_\mu$ принадлежит Φ, то есть множество Φ индуктивно.

В дальнейшем мы будем изучать *нетеровы кольца*, то есть коммутативные кольца, в которых каждое непустое множество идеалов имеет максимальный элемент.

Замечание. Правая часть равенства (1) называется разложением элемента x на экстремальные множители. Если $x=u\prod\limits_\alpha p_\alpha^{n_\alpha}$ и $y=v\prod\limits_\alpha p_\alpha^{m_\alpha}$ — разложения элементов x и y на экстремальные множители, то x делит y тогда и только тогда, когда для всякого α $n_\alpha\leqslant m_\alpha$; отсюда

$$\text{н. о. д. } (x, y)=\prod_\alpha p_\alpha^{\inf(n_\alpha,\, m_\alpha)}, \tag{2}$$

$$\text{н. о. к. } (x, y)=\prod_\alpha p_\alpha^{\sup(n_\alpha,\, m_\alpha)}. \tag{3}$$

Свойство, описываемое теоремой 2, справедливо для колец более широкого класса; эти кольца появятся у нас ниже под названием *факториальных колец*. Мы увидим, что кольца многочленов и формальных степенных рядов от любого числа переменных являются факториальными кольцами.

4. *Делимость целых рациональных чисел*

Как было сказано, кольцо $\boldsymbol{Z}$ целых рациональных чисел является кольцом главных идеалов; его поле дробей есть $\boldsymbol{Q}$. Мультипликативная группа U обратимых элементов кольца $\boldsymbol{Z}$ состоит из двух элементов: 1 и —1. Группа $\boldsymbol{Q}_+^*$ строго положительных рациональных чисел содержит единственный элемент из каждого класса ассоциированных элементов кольца Q; следовательно, она изоморфна группе $\mathcal{F}^*=\boldsymbol{Q}^*/U$ главных дробных идеалов поля $\boldsymbol{Q}$, с которой ее обычно и отождествляют. В дальнейшем, когда речь будет о н. о. д. или н. о. к. в поле $\boldsymbol{Q}$ (относительно кольца $\boldsymbol{Z}$), будет предполагаться, что эти элементы $\geqslant 0$; это