Ю. А. ДРОЗД

О ПОЛУГРУППЕ ДИВИЗОРОВ КОММУТАТИВНОГО КОЛЬЦА

Исследования полугруппы идеалов в кольцах алгебраических чисел занимают важное место в теории чисел и теории целочисленных представлений. Один из основных результатов здесь был получен Е. Дейдом, О. Таусской и Х. Цассенхаузом [1], которые доказали, что если A — порядок в поле алгебраических чисел степени n, то для любого A-идеала I идеал I^{n-1} обратим (в своем кольце множителей). Для случая $n=3$ этот результат другими методами был получен Д. К. Фаддеевым [2]. В работе [3] показано, что при $n=3$ условие на A можно ослабить: достаточно (а если у A нет полей вычетов из двух элементов, и необходимо), чтобы A-модуль A_0/A, где A_0 — максимальный порядок, имел две образующие. В настоящей статье (§ 1) этот результат распространяется на общую ситуацию: доказывается, что для обратимости I^m для любого идеала I достаточно (а если поля вычетов A состоят не менее чем из $m+1$ элементов, и необходимо), чтобы A-модуль A_0/A имел m образующих. Отсюда, конечно, следует теорема Дейда, Таусской и Цассенхауса.

Этот результат без труда переносится на идеалы произвольного нетерова одномерного кольца A без нильпотентных элементов. Для того чтобы отказаться от ограничения на размерность Крулля, естественно от идеалов перейти к дивизорам, подобно тому как делается, например, в [4]. Заметим, что определение полугруппы дивизоров, которое мы вводим в § 2, существенно отличается от определения [4], хотя и равносильно ему для колец Крулля. Наше определение подобрано так, чтобы для одномерных колец получалась просто полугруппа дробных идеалов.

Как обычно, наряду с полугруппой дивизоров $D(A)$ естественно рассмотреть две ее фактор-полугруппы: полугруппу классов дивизоров $C(A)$ и полугруппу родов, или локальных классов, $G(A)$. В § 3 решается вопрос о конечности полугруппы родов, а также получаются некоторые результаты относительно конечности полугрупп классов дивизоров. Заметим также, что большинство полученных результатов переносится на произвольные локально нетеровы редуцированные схемы, подобно тому как это было сделано в § 5 работы [3].

§ 1. Локальные теоремы

Мы будем пользоваться терминологией и обозначениями работы [3]. В частности, слово «кольцо» будет всегда означать коммутативное нетерово кольцо без нильпотентов; $Q=Q(A)$ будет обозначать полное кольцо частных кольца A (это полупростое артиново кольцо), A_0 — целое замыкание A в Q, $\mu_A(M)$ — минимальное число образующих A-модуля M. Поле k назовем n-совершенным, если всякое его расширение степени $d \leqslant n$ сепарабельно. В этом параграфе кольцо A будет предполагаться локальным одномерным кольцом. Обозначим p его максимальный идеал, $k=A/p$ — поле вычетов, $m=\mu_A(A_0/A)$. Как показано в [3], m всегда конечно и $\mu_A(I) \leqslant m+1$ для любого дробного идеала* I кольца A.

Основным результатом этого параграфа является следующая теорема.

Теорема 1. *Для любого дробного идеала I кольца A идеал I^m обратим. Если, кроме того, поле вычетов k содержит не менее m элементов и является $[(m+1)/2]$-совершенным, то найдется такой идеал I, что все его степени I^n при $n < m$ необратимы.*

Доказательство. Поскольку при $A=A_0$ теорема очевидным образом верна, а A_0/A является A-модулем конечной длины [3], мы можем применить «нетерову индукцию», т. е. считать, что для всех собственных надколец кольца A теорема верна. Тогда можно считать, что I — точный идеал, т. е. $A=O(I)$ (кольцо множителей I). Обозначим $A'=O(p)$, $F=A'/p$, $I'=IA'$, $M=I'\otimes k$, $V=I\otimes k$ (тензорное произведение всюду берется над кольцом A). Если $A\neq A_0$, то $A'\neq A$ ([3], предложение 4). F является конечномерной k-алгеброй размерности $d=\mu_A(A') \leqslant m+1$. M — конечномерный модуль над алгеброй F, а V — порождающее подпространство в M (т. е. подпространство, содержащее систему образующих модуля M). Воспользуемся следующей леммой, доказанной в [3] (§ 3).

Лемма 1. *Сопоставляя идеалу I подпространство V, мы получаем взаимно-однозначное соответствие между идеалами I, такими, что $IA'=I'$, и порождающими подпространствами в M. Два таких идеала, I и J, изоморфны тогда и только тогда, когда соответствующие подпространства, V и U, подобны в том смысле, что $U=\alpha V$ для некоторого обратимого элемента $\alpha \in F$. Идеал I является точным тогда и только тогда, когда I' — точный A'-идеал, а V — точное подпространство в M в том смысле, что из включения $\alpha V\subset V$ для какого-либо $\alpha \in F$ следует, что $\alpha \in k$. Наконец, $\dim V=\mu_A(I)$.*

Предположим вначале, что I' — необратимый A'-идеал. По индукционному предположению, $(I')^m$ обратим. Следовательно, $(I')^m$ — неточный A'-идеал и, поскольку $I^mA'=(IA')^m=(I')^m$, A-идеал I^m также неточен. Иными словами, $I^m=I^mB=(IB)^m$ для некоторого собственного надкольца B кольца A. Но тогда I^m обратим, по индукционному предположению.

Итак, можно считать, что I' — обратимый точный A'-идеал, т. е., ввиду локальности A, $I'\simeq A'$, а значит, можно считать, что $I'=A'$, а $M=F$. Пусть $M_1, \ldots M_s$ — все максимальные идеалы алгебры F (всегда $s \leqslant d$). Поскольку V — порождающее подпространство, $V\not\subset M_i$ ни для какого i. Если в поле k содержится не меньше $s+1$ элементов, то отсюда следует, что найдется элемент $\alpha \in V$, такой, что $\alpha \notin M_i$ ни для какого i. Тогда α — обратимый элемент алгебры F и, заменяя V на $\alpha^{-1} V$, можно считать, что $V \ni 1$. Заметим, что если $\dim V=1$, то I — главный идеал, т. е. обратим.

* Дробным идеалом кольца A называется произвольный конечнопорожденный A-подмодуль в Q. Допуская вольность, мы будем часто вместо «дробный идеал» говорить «идеал».

Пусть $\dim V \geqslant 2$. Рассмотрим возрастающую цепочку подпространств $V \subset V^2 \subset V^3 \subset \ldots$ алгебры F. Поскольку $\dim F \leqslant m+1$, найдется такое $n \leqslant m$, что $V^n = V^{n+1} = \ldots = V^{2n}$, т. е. V^n — подалгебра в F. Следовательно, $I^n = B$ — подкольцо в A', т. е. обратимый идеал, а потому и I^k обратим при любом $k \geqslant n$, в частности при $k=m$.

Пусть теперь k — «маленькое» поле, т. е. число элементов в нем $q \leqslant s$. Найдем такое n, что $q^n > s$, и рассмотрим неразветвленное расширение B степени n кольца A (см., например, [3], § 4), т. е. фактор-кольцо $B = A[x]/(f_n(x))$, где $f_n(x)$ — многочлен степени n со старшим коэффициентом 1, неприводимый по модулю p. Поскольку B — строго плоский A-модуль, из результатов [4] (гл. I, § 3) следует, что A-идеал J и B-идеал $J \otimes B$ обратимы одновременно. Кроме того, $p \otimes B = pB$ — максимальный идеал B и $B' = O(pB) = A' \otimes B$. Но из вышесказанного тогда следует, что идеал $I^m \otimes B = (I \otimes B)^m$ обратим. Следовательно, I^m также обратим и первое утверждение теоремы доказано. Доказательство второго утверждения основывается на следующей лемме.

Лемма 2. *Пусть F — коммутативная алгебра размерности $m+1$ над полем k, всякий идеал которой — главный, причем $F \not\simeq k^{m+1}$ (прямая сумма $m+1$ экземпляров поля k). Если поле k содержит не менее m элементов и $[(m+1)/2]$-совершенно, то алгебра F моногенна, т. е. $F = k[\omega]$ для некоторого $\omega \in F$.*

Доказательство. Если F является полем, то оно либо сепарабельно над k, либо является простым чисто несепарабельным расширением. В обоих случаях F моногенна. Пусть теперь $R = \mathrm{rad}\, F$, $S = F/R = F_1 \oplus \ldots \oplus F_t$, где F_i — поля. Тогда можно считать, что либо $R \neq 0$, либо $t > 1$. В обоих случаях S — сепарабельная k-алгебра и, значит, в F есть подалгебра $\bar{S} \simeq S$, такая, что $F = \bar{S} \oplus R$ (см. [5], гл. 5, § 20). Если $\bar{S}$ моногенна, $\bar{S} = k[\theta]$, а r — образующий идеала R, то, как легко видеть, $F = k[\omega]$, где $\omega = \theta + r$. Поэтому достаточно проверить моногенность S.

Каждое поле F_i является простым расширением k, т. е. $F_i = k[\theta_i]$, где θ_i — корень неприводимого многочлена $p_i(x) \in k[x]$. Если все многочлены $p_t(x)$ различны, то $S \simeq k[x]/(f(x))$, где $f(x) = p_1(x) p_2(x) \ldots p_t(x)$. Но если поле k бесконечно, то, заменяя θ_i на $\theta_i + c_i$, где $c_i \in k$, можно добиться того, чтобы все многочлены $p_i(x)$ были различны. Пусть теперь k — поле из q элементов, причем $q \geqslant m$. Поскольку $\dim S = \sum_{i=1}^{t} \deg p_i(x) \leqslant \leqslant m+1$, среди $p_i(x)$ есть не больше $[(m+1)/d]$ многочленов данной степени d. Но из формулы для числа неприводимых многочленов данной степени над конечным полем (см., например, [6], с. 464) легко следует, что при $d > 1$ над полем k есть не меньше, чем $[(m+1)/d]$ различных неприводимых многочленов степени d. Поскольку все они задают изоморфные расширения поля k, мы можем все нелинейные $p_i(x)$ считать различными. Наконец, число линейных многочленов среди $p_i(x)$ не больше m (иначе $F \simeq k^{m+1}$), значит, и их можно считать различными, что завершает доказательство леммы 2.

Вернемся к доказательству второго утверждения теоремы 1. Заменяя A локальным над кольцом $A_0 p + A$ с тем же полем вычетов (см. [3], доказательство теоремы 3), мы можем считать, что $A_0 p = p$, т. е. $A' = O(p) = A_0$.

Положим $F=A_0/p$. Поскольку A_0 — прямая сумма полулокальных дедекиндовых колец, всякий идеал в A_0, а потому и в F — главный (см. [4], гл. VII, § 2). Если $F\not\simeq k^{m+1}$, к ней применима лемма 2, т. е. $F=k(\omega)$. Рассмотрим тогда идеал I, определенный подпространством $V\subset F$ с базисом $[1, \omega]$ (см. лемму 1). Поскольку $\dim F=m+1$, элементы $\{1, \omega, \omega^2, \ldots, \omega^m\}$ линейно независимы, поэтому при $n<m$ базисом подпространства V^n является $[1, \omega, \omega^2, \ldots, \omega^n]$, причем $\omega^{n+1}\notin V^n$. Предположим, что $\alpha V^n\subset V^n$ для некоторого $\alpha\in F$. Тогда, так как $1\in V^n$, $\alpha\in V^n$, т. е. $\alpha=c_0+c_1\omega+\ldots+c_n\omega^n$. Следовательно, $\alpha\omega=c_0\omega+c_1\omega^2+\ldots+c_n\omega^{n+1}$ и если $\alpha\omega\in V^n$, то $c_n=0$. Аналогично из $\alpha^2\omega\in V^n$ получаем $c_{n-1}=0$ и т. д. Окончательно $\alpha=c_0\in k$, т. е. V^n — точное подпространство, а I^n — точный A-идеал. Поскольку $\mu_A(I^n)=\dim V^n=n+1$, I^n — не главный, а потому и необратимый A-идеал.

Остается рассмотреть случай $F\simeq k^{m+1}$. Выберем в k различные элементы $c_1, \ldots, c_m$ и рассмотрим в F порождающее подпространство V с базисом $[\alpha, \beta]$, где $\alpha=(c_1, c_2, \ldots, c_m, 1)$, $\beta=(1, 1, \ldots, 1, 0)$. Аналогично тому, как было сделано выше, несложно убедиться, что V^n — точное подпространство в F при любом $n<m$, причем $\dim V^n=n+1$. Следовательно, идеал I, определенный подпространством V, таков, что I^n необратим при $n<m$, и теорема 1 полностью доказана.

Замечание. Ограничение на поле k во второй части теоремы 1 существенно, как показывает следующий пример. Пусть k — поле из q элементов, A — такое локальное кольцо с полем вычетов k, что $pA_0=p$ и $F=A_0/p\simeq k^{m+1}$, где $m>q$. Учитывая, что $c^{q-1}=1$ для любого ненулевого $c\in k$, нетрудно проверить, что если V — порождающее подпространство в F, то V^q — подалгебра в F. Отсюда очевидно, что I^q обратим для любого идеала I. Отметим, что в качестве A здесь можно выбрать даже локализацию некоторого кольца алгебраических чисел. Аналогичные примеры можно построить и для более сложных фактор-алгебр F. Однако из доказательства теоремы 1 видно, что, имея информацию о фактор-алгебре F, условия на поле k иногда можно ослабить.

Говорят, что два идеала, I и J, принадлежат одному классу, если они изоморфны как модули [6, 7]. Как мы уже отмечали, всякий A_0-идеал является главным (напомним, что кольцо A предполагается локальным). Если поле вычетов k конечно, отсюда очевидной индукцией по надкольцам (и, например, с использованием леммы 1) выводится, что число классов идеалов кольца A конечно. Однако если k бесконечно, это уже не так (см. [3], теорему 4). Установим следующий критерий конечности числа классов.

Теорема 2. *Число классов идеалов кольца A конечно тогда и только тогда, когда либо поле вычетов k конечно, либо выполнены следующие условия:*

1) $m=\mu_A(A_0/A)\leqslant 2$;

2) $m_1=\mu_A(A+pA_0/A)\leqslant 1$.

Замечание. Очевидно, $A+pA_0/A$ — это радикал A-модуля A_0/A (т. е. пересечение его максимальных подмодулей). Поэтому условия 1) и 2) в точности совпадают с условиями из критерия конечности числа неразложимых A-решеток (конечнопорожденных A-модулей без кручения), полученного в [8]. Таким образом, имеет место следствие.

Следствие. *Пусть поле вычетов k бесконечно. Тогда если A имеет бесконечно много неизоморфных неразложимых решеток, то число классов идеалов кольца A также бесконечно.*

Доказательство теоремы 2. Пусть поле вычетов k бесконечно. Из [3] (теорема 4) следует, что тогда неравенство $m \leqslant 2$ является необходимым условием конечности числа классов идеалов. С другой стороны, $m_1 = \mu_A(A + pA_0) - 1 \leqslant m$, а при выполнении условий 1) и 2) конечность числа классов следует из [8] (и, кроме того, может быть несложно доказана непосредственно). Поэтому остается проверить, что при $m = m_1 = 2$ число классов идеалов бесконечно.* Обозначим $A_1 = A + pA_0$; $A_2 = A + pA_1$. Как мы уже отмечали, A_1 — локальное кольцо с максимальным идеалом pA_0 и полем вычетов k. Аналогично, поскольку $A_2/pA_1 \simeq A/(A \cap pA_1) = A/p = k$, A_2 — также локальное кольцо с максимальным идеалом pA_1 и полем вычетов k. При этом $\mu_{A_2}(A_0) = \mu_A(A_0)$ и $\mu_{A_2}(A_1) = \mu_A(A_1)$. Поэтому можно считать, что $A = A_2$, т. е. $A' = O(p) = A_1$. Тогда $A'/p = F$ — локальная алгебра размерности 3 над полем k с радикалом $R = pA_0/p$. Но $p = pA_1 \supset p^2 A_0 = (pA_0)^2$, поэтому $R^2 = 0$ и для алгебры F есть одна возможность: F есть алгебра с базисом $[1, r_1, r_2]$ и таблицей умножения $r_i r_j = 0$ при любых i, j. В этом случае подпространства V_c с базисом $[1, r_1 + cr_2]$ $(c \in k)$ являются подалгебрами в F, различными при разных c. Поэтому соответствующие им по лемме 1 идеалы I_c являются различными надкольцами A и, следовательно, неизоморфны, что и доказывает теорему 2.

Замечание. По аналогии с теоремой 4 работы [3] теорему 2 можно уточнить для случая конечного поля вычетов. Именно, если обозначить $A^{(n)}$ неразветвленное расширение степени n кольца A, то при нарушении условий 1) и 2) число классов идеалов колец $A^{(n)}$ стремится к бесконечности при $n \to \infty$. В то же время из результатов [8] и совпадения целого замыкания $A^{(n)}$ с $A_0 \otimes A^{(n)}$ следует, что при выполнении условий 1), 2) число классов идеалов колец $A^{(n)}$ остается ограниченным при $n \to \infty$.

Аналогичное соображение справедливо и для теоремы 1: если k — конечное поле из $q < m$ элементов, то даже если для всех A-идеалов I идеалы I^{m-1} обратимы, у колец $A^{(n)}$ при достаточно больших n найдутся такие идеалы J, что J^{m-1} необратимы. В то же время примеры показывают, что от условия $[(m+1)/2]$-совершенности таким образом избавиться невозможно.

Очевидно, результаты теорем 1 и 2 можно «глобализировать» на произвольные нетеровы одномерные кольца без ниль-потентов, подобно тому как это сделано в [3]. Однако мы предпочтем провести глобализацию в более общей ситуации. При этом идеалы нужно заменить дивизорами.

§ 2. Дивизоры

Для дальнейшего нам будет удобно ослабить ограничения на кольцо A и вместо нетеровости наложить следующие два условия:

I) для всякого простого идеала p высоты 1 кольцо A_p нетерово;

* Из [3] (теорема 3) следует, что в этом случае у всякого надкольца A (в том числе и у самого A) не более двух точных идеалов!

II) всякий элемент $a \in A$, не являющийся делителем нуля, содержится только в конечном числе простых идеалов высоты.

Напомним, что простые идеалы высоты 1 — это идеалы, минимальные во множестве $(\operatorname{Spec} A)\setminus M$, где M — множество минимальных простых идеалов кольца A. Множество всех простых идеалов высоты 1 кольца A обозначим $P=P(A)$. Кроме того, мы по-прежнему будем предполагать, что A — редуцированное кольцо, т. е. не содержит нильпотентов. Очевидно, нетеровы кольца всегда удовлетворяют условиям I) и II) [4]. Кольца, удовлетворяющие этим условиям, мы будем называть псевдонетеровыми; в дальнейшем все кольца будут считаться псевдонетеровыми и редуцированными.

Пусть Q — полное кольцо частных A. Дробным идеалом кольца A будем называть такой A-подмодуль $I \subset Q$, что $aA \subset I \subset bA$ для некоторых обратимых элементов a, $b \in Q$. На множестве $I(A)$ дробных идеалов кольца A введем отношение предпорядка $\prec$, считая $I \prec J$, если $Ip \supset Jp$ для всех $p \in P$. Фактор-множество $D(A)$ множества $I(A)$ по ассоциированному с $\prec$ отношению эквивалентности «$I \prec J$ и $J \prec I$» (или, что то же, $I_p = J_p$ для всех $p \in P$) назовем множеством дивизоров кольца A, а его элементы — дивизорами. Элемент $\operatorname{div} I$, соответствующий идеалу $I \in I(A)$, будем называть дивизором идеала I. Если $I = aA$ — главный идеал (a — обратимый элемент Q), то его дивизор мы будем обозначать $\operatorname{div}(a)$ и называть дивизором элемента a. Дивизоры вида $\operatorname{div}(a)$ назовем главными дивизорами. Порядок, индуцированный на $D(A)$ отношением $\prec$, будем обозначать $\leqslant$. Два идеала, I и J, такие, что $\operatorname{div} I = \operatorname{div} J$, назовем псевдоравными.* Поскольку предпорядок $\prec$, очевидно, согласован с обычными операциями над идеалами, все эти операции переносятся на множество дивизоров $D(A)$. В частности, имеет место следующее предложение.

Предложение 1. *$D(A)$ является структурно упорядоченной коммутативной полугруппой относительно порядка $\leqslant$ и операции умножения*: **

$$(\operatorname{div} I)(\operatorname{div} J) = \operatorname{div}(IJ).$$

При этом роль верхней грани играет пересечение дивизоров $(\operatorname{div} I)\cap(\operatorname{div} J) = \operatorname{div}(I\cap J)$, а роль нижней грани — сумма дивизоров $(\operatorname{div} I)+(\operatorname{div} J) = \operatorname{div}(I+J)$. Дивизор $\operatorname{div} A$ является единицей полугруппы $D(A)$.

Если S — конечное подмножество в P, то для любого A-модуля M можно построить модуль частных $M_S = \bar{S}^{-1}M$, где $\bar{S} = \bigcup_{p\in S} p$. Если $S \supset T$, то определен канонический гомоморфизм $f_S^T : M_S \to M_T$ (см. [4], гл. II, § 2). Обозначим $\tilde{M} = \varprojlim M_S$ (предел берется по всем конечным частям $S \subset P$ относительно гомоморфизмов f_S^T). Если A — целостное кольцо и I — идеал в A, то, как легко заметить, $I_S = \bigcap_{p\in S} I_p$, а $\tilde{I} = \bigcap_{p\in P} I_p$. В общем случае определен

* Если A — кольцо Крулля, то эти определения равносильны определениям [4]. Однако в общем случае это не так. Например, если A — нетерово одномерное кольцо, то при наших определениях $D(A)=I(A)$, в то время как при определениях [4] это не так, если только A не горенштейново в смысле [9].

** В отличие от [4] нам удобнее записывать эту операцию мультипликативно, а не аддитивно.

мономорфизм $\tilde{I} \to Q$, при помощи которого $\tilde{I}$ можно отождествить с A-подмодулем в Q, содержащим I. Очевидно, $\tilde{I}_p = I_p$, т. е. $I \prec J$ означает, что $\tilde{I} \supset \tilde{J}$. В частности, $\tilde{A}_p = A_p$, значит, $\tilde{A}$ — также псевдонетерово кольцо. Заметим, что если A^0 — целое замыкание A в Q, то A_p^0 — целое замыкание A_p в Q_p (см. [4], гл. V, § 1) и, следовательно, A_p^0 — прямая сумма конечного числа дедекиндовых колец. Поэтому A^0 — также псевдонетерово кольцо, причем $\tilde{A}^0 = A^0$, а значит, $\tilde{A} \subset A^0$, т. е. $\tilde{A}$ цело над A и для всякого $p \in P(A)$ найдется $\tilde{p} \in P(\tilde{A})$, такой, что $\tilde{p} \cap A = p$ (см. [4], гл. V, § 2) и $\tilde{A}_p = \tilde{A}_{\tilde{p}}$. Очевидно, для любого $I \in I(A)$ модуль $\tilde{I}$ является дробным идеалом кольца $\tilde{A}$. В частности, определено отображение $\delta : D(A) \to D(\tilde{A})$, которое является, как легко видеть, гомоморфизмом (и даже мономорфизмом) структурно упорядоченных полугрупп.

Следующий стандартный результат является основным инструментом для переноса локальных результатов на полугруппу дивизоров.

Предложение 2. *Предположим, что для каждого $p \in P$ задан дробный идеал $I(p)$ кольца A_p, причем для всех p, кроме конечного числа, $I(p) = J_p$, где J — некоторый дробный идеал кольца A. Тогда существует дробный идеал $I = I(A)$, такой, что $I_p = I(p)$ для всех $p \in P$.*

Доказательство. Пусть $p_1, \ldots, p_n$ — все те простые $p \in P$, для которых $I(p) \neq J_p$. Заметим прежде всего, что, заменяя J на $a^{-1}J$, где a — неделитель нуля из A, можно добиться того, чтобы $I(p) \subset J_p$ для всех $p \in P$. Мы будем предполагать, что это условие выполнено, и будем вести доказательство индукцией по n. Если $n = 1$, рассмотрим канонический гомоморфизм $\varphi : J \to J_{p_1}$ и положим $I = \varphi^{-1}(I(p_1))$. Тогда $J/I \simeq I(p_1) + \mathrm{Jm}\,\varphi / I(p_1)$, откуда сразу следует, что $I_p = J_p$ при $p \neq p_1$ и $I_{p_1} = I(p_1)$, что и требовалось получить. Для любого n, применив эту конструкцию, мы получим идеал J', такой, что $J'_p = J_p \supset I(p)$ при $p \neq p_1$ и $J'_{p_1} = I(p_1)$, т. е. $J'_p \neq I(p)$ только для $p = p_2, \ldots, p_n$ и можно применить индукционное предположение.

Из условия II) вытекает, что для любого $I \in I(A)$ локализации I_p и A_p различаются лишь для конечного числа $p \in P$.

Следствие 1. $D(A) \simeq \bigoplus_{p \in P} D(A_p)$.

Здесь под прямой суммой полугрупп с единицами понимается подмножество их прямого произведения, состоящее из таких наборов, у которых все координаты, кроме конечного числа, равны единицам. Отметим еще, что $D(A_p) = I(A_p)$ для $p \in P$.

Следствие 2. *Гомоморфизм $\delta : D(A) \to D(\tilde{A})$ является изоморфизмом. Таким образом, при изучении дивизоров можно ограничиться дивизориальными кольцами, т. е. такими, что $A = \bigcap_{p \in P} A_p$.**

Для любого идеала I дивизориального кольца $\tilde{I}$ также будет идеалом, причем $\operatorname{div} I = \operatorname{div} \tilde{I}$. Идеалы вида $\tilde{I}$ назовем дивизориальными. В частности, главные идеалы дивизориального кольца являются дивизориальными и вообще если I — дивизориальный идеал, то и aI — дивизориальный идеал для любого обратимого элемента $a \in Q$.

* Автору неизвестно, будет ли кольцо $\tilde{A}$ нетеровым для нетерова кольца A. Конечно, это будет так в важном частном случае, когда A^0 — конечно порожденный A-модуль.

Главные дивизоры образуют подгруппу в $D(A)$, поэтому можно ввести отношение эквивалентности дивизоров, считая $\operatorname{div} I \sim \operatorname{div} J$, если $\operatorname{div} J = (\operatorname{div} I)(\operatorname{div}(a)) = \operatorname{div}(aI)$ для некоторого обратимого элемента $a \in Q$. Очевидно, это равенство эквивалентно тому, что $\tilde{J} = a\tilde{I}$. Фактор-полугруппу $C(A)$ полугруппы $D(A)$ по этому отношению эквивалентности назовем полугруппой классов дивизоров кольца A.

Надкольцом кольца A назовем всякий дробный идеал B, который является подкольцом в Q. Очевидно, тогда $(\operatorname{div} B)^2 = \operatorname{div} B$, т. е. $\operatorname{div} B$ — идемпотент полугруппы $D(A)$. Наоборот, пусть $(\operatorname{div} I)^2 = \operatorname{div} I$. Тогда $I_p^2 = I_p$ для всех $p \in P$, откуда, как обычно, следует, что I_p — надкольцо A_p (см., например, [7]). Рассмотрим в Q подмножество $B = I : I = \{\alpha \in Q \mid \alpha I \in I\}$. Если $aA \subset I \subset bA$, то $A \subset B \subset a^{-1}bA$, т. е. B — дробный идеал. В то же время B, конечно, является подкольцом в Q и $B_p = I_p : I_p = I_p$ (равенство $(I : J)_p = I_p : J_p$ для любых I, J следует, например, из канонического отождествления $I : J$ с модулем $\operatorname{Hom}_A(J, I)$ и результатов [4], гл. II, § 2). Отсюда вытекает следующее предложение.

Предложение 3. *Всякий идемпотент полугруппы $D(A)$ имеет вид $\operatorname{div} B$ для некоторого надкольца B кольца A. Кроме того, если для любого $p \in P$ задано надкольцо $B(p)$ кольца A_p, причем $B(p) = A_p$ для всех p, кроме конечного числа, то существует такое надкольцо B кольца A, что $B_p = B(p)$ для всех $p \in P$.*

Дивизор $\operatorname{div}(I : J)$ назовем частным дивизоров $\operatorname{div} I$ и $\operatorname{div} J$ и обозначим $(\operatorname{div} I) : (\operatorname{div} J)$. Дивизор $O(\operatorname{div} I) = \operatorname{div} I : \operatorname{div} I$ назовем дивизором множителей дивизора I. Поскольку $O(\operatorname{div} I) = \operatorname{div}(I : I)$, дивизор множителей является идемпотентом в $D(A)$. Если $O(\operatorname{div} I) = \operatorname{div} A$, назовем дивизор $\operatorname{div} I$ точным.

Будем говорить, что дивизор $\operatorname{div} J$ делит дивизор $\operatorname{div} I$, если $\operatorname{div} I = (\operatorname{div} J)(\operatorname{div} J')$ для некоторого J'. Ввиду предложения 2 это равносильно тому, что идеал J_p делит I_p для всех $p \in P$. Тогда в качестве J', очевидно, можно взять $I : J$. Дивизор $\operatorname{div} I$ назовем обратимым, если он делит свой дивизор множителей. Это вновь равносильно тому, что идеал I_p обратим для всех $p \in P$ в смысле [3] (§ 2), т. е. ввиду локальности A_p тому, что I_p — главный идеал своего кольца множителей. Поэтому имеет место следующее предложение.

Предложение 4. *Для любых дробных идеалов I и J следующие условия равносильны:*

1) $\operatorname{div} J = (\operatorname{div} I)(\operatorname{div} I')$ *для некоторого обратимого дивизора* $\operatorname{div} I'$;
2) $I_p \simeq J_p$ *для всех* $p \in P$.

Если I и J удовлетворяют равносильным условиям предложения 4, то будем говорить, что дивизоры $\operatorname{div} I$ и $\operatorname{div} J$ принадлежат одному роду и писать $(\operatorname{div} I) \vee (\operatorname{div} J)$ (см. [7] для одномерного случая). Очевидно, принадлежность одному роду — это отношение эквивалентности, согласованное с умножением дивизоров. Поэтому можно рассмотреть фактор-полугруппу $G(A)$ полугруппы $D(A)$ по этому отношению эквивалентности. Назовем $G(A)$ полугруппой родов дивизоров кольца A. Из предложения 2 тогда вытекает следствие 3.

Следствие 3. $G(A) \simeq \bigoplus_{p \in P} C(A_p)$.

Заметим, что ограничение естественного эпиморфизма $D(A) \to G(A)$ на полугруппу идемпотентов $E(A) = \{\operatorname{div} B \mid B$ — надкольцо $A\}$ является мономорфизмом, так что $E(A)$ можно рассматривать и как подполугруппу в $G(A)$, а также в $C(A)$. При этом, конечно, $E(A) \simeq \bigoplus_{p \in P} E(A_p)$. Кроме того, $E(A)$ является структурой, в которой роль верхней грани играет пересечение, а роль нижней грани — произведение.

Отметим, наконец, следующие результаты, которые дают возможность вычислять полугруппу классов.

Предложение 5. *Пусть* $g \in G(A)$, $\operatorname{div} I$ — *какой-либо представитель рода* g, C_g — *прообраз* g *при естественном эпиморфизме* $C(A) \to G(A)$, B — *такое надкольцо* A, *что* $\operatorname{div} B = O(\operatorname{div} I)$ (*например*, $B = I : I$). *Обозначим* $\mathcal{J}$ *группу иделей кольца* B, *т. е. подмножество прямого произведения* $\prod_{p \in P} Q_p^*$ (Q_p^* — *группа обратимых элементов* Q_p), *состоящее из таких наборов* (a_p), *что* $a_p \in B_p^*$ *для всех* $p \in B$, *кроме конечного числа*; $\mathcal{J}_B$ — *группу* B-*единичных иделей, т. е. подгруппу* $\prod_{p \in P} B_p^* \subset \mathcal{J}$; Δ — *образ естественного диагонального гомоморфизма* $Q^* \to \mathcal{J}$. *Тогда существует взаимно-однозначное соответствие между* C_g *и фактор-группой* $\mathcal{J}/\Delta\mathcal{J}_B$.

Доказательство немедленно следует из предложения 2 аналогично [7] или [4] (гл. VII, § 4): иделю (a_p) нужно сопоставить класс дивизора $\operatorname{div} J$, где $J_p = a_p I_p$ для всех $p \in P$.

Следствие 4. *В обозначениях предложения 5 существует взаимно-однозначное соответствие между* C_g *и* $C_{O(g)}$, *где* $O(g)$ — *род, содержащий* $\operatorname{div} B$ (*главный род кольца* B).

Заметим, что если g — главный род кольца B, то $O(\operatorname{div} I) = \operatorname{div} B$ для любого $\operatorname{div} I \in g$ и, кроме того, всякий дивизор из g обратим. Поэтому C_g — подгруппа в $C(A)$.

Предложение 6. *Пусть* B *и* B' — *два надкольца* A, *такие, что* $\operatorname{div} B' \leqslant \operatorname{div} B$ (*т. е.* $B_p \subset B'_p$ *для всех* $p \in P$); g *и* g' — *соответственно главные рода колец* B *и* B'; $\varphi : C_g \to C_{g'}$ — *гомоморфизм, переводящий класс дивизора* $\operatorname{div} I$ *в класс дивизора* $\operatorname{div} I'$, *где* $I' = IB'$ (*т. е. гомоморфизм умножения на* $\operatorname{div} B'$). *Обозначим* $S = \{p \in P / B_p \neq B'_p\}$ (*это конечное подмножество в* P). *Тогда* $\operatorname{Ker} \varphi \simeq \prod_{p \in S} B_p'^* / \Delta_S \prod_{p \in S} B_p^*$, *где* Δ_S — *образ естественного диагонального гомоморфизма* $\widehat{B}'^* \to \prod_{p \in S} B_p'^*$.

Доказательство. В силу предложения 5 φ можно отождествить с естественным эпиморфизмом $\mathcal{J}/\Delta\mathcal{J}_B \to \mathcal{J}/\Delta\mathcal{J}_{B'}$. Поэтому $\operatorname{Ker}\varphi \simeq \Delta\mathcal{J}_{B'}/\Delta\mathcal{J}_B \simeq \mathcal{J}_{B'}/\mathcal{J}_{B'} \cap \Delta\mathcal{J}_B$. Но $\mathcal{J}_{B'} \cap \Delta\mathcal{J}_B = \Delta'\mathcal{J}_B$, где Δ' — образ диагонального отображения $\widehat{B}'^* \to \mathcal{J}_{B'}$. Учитывая, наконец, что $B_p^* = B_p'^*$ при $p \notin S$, мы получаем требуемый результат.

Замечание. Поскольку B'_p — конечнопорожденный B_p-модуль, B_p содержит некоторый идеал F_p кольца B'_p и, следовательно, B_p^* содержит «конгруэнц-подгруппу» $1 + F_p$. Поэтому в предложении 6 $P_p'^*$ можно заменить на $(B'_p/F_p)^*$ с соответствующей заменой остальных членов, после чего вычисление $\operatorname{Ker}\varphi$ сводится к вычислениям в некотором артиновом кольце.

§ 3. Глобализация локальных теорем

Мы сохраняем все определения и обозначения предыдущего параграфа. В частности, A будет обозначать псевдонетерово редуцированное кольцо, A^0 — его целое замыкание в $Q=Q(A)$. Идеал $p\in P$ назовем критическим, если $A_p\neq A_p^0$. Положим $m_p=\mu_{A_p}(A_p^0/A_p)$; $m=m(A)=\sup\{m_p\mid p\in P\}$. Если $m=m_p$, назовем идеал $p\in P$ строго критическим. Обозначим также $k_p=A_p/pA_p$.

Теорема 3. *Если $m<\infty$, то дивизор $(\operatorname{div} I)^m$ обратим для любого дивизора $\operatorname{div} I\in D(A)$. Если, кроме того, для некоторого строго критического идеала p поле k_p содержит не менее m элементов и $[(m+1)/2]$-совершенно, то найдется такой дивизор $\operatorname{div} I$, что $(\operatorname{div} I)^n$ необратим ни при каком $n<m$. Наконец, если $m=\infty$, а все поля k_p для критических p бесконечны и совершенны, то для любого натурального n найдется такой дивизор $\operatorname{div} I_n$, что $(\operatorname{div} I_n)^n$ необратим.*

В частности, при $m=1$, получаем такое следствие.

Следствие. *Всякий дивизор кольца A обратим тогда и только тогда, когда $m(A)\leqslant 1$.*

Доказательство немедленно следует из теоремы 1 и предложения 2. Отметим, что если p — немаксимальный идеал, то поле k_p заведомо бесконечно. Поэтому, например, второе и третье утверждения теоремы 3 заведомо выполняются для кольца регулярных функций на аффинном алгебраическом многообразии X над полем характеристики 0, если все неприводимые компоненты X имеют размерность не меньше 2.

Числу $m(A)$ можно также придать «глобальный» смысл, подобно тому как в одномерном случае это сделано в [3]. Именно, назовем элементы $a_1, \ldots, a_n$ поля Q системой образующих дивизора $\operatorname{div} I$, если $\operatorname{div} I=$ $=\operatorname{div}(a_1,\ldots,a_n)=\sum_{i=1}^{n}\operatorname{div}(a_i)$. Обозначим $\mu_A(\operatorname{div} I)$ наименьшее число элементов во всевозможных системах образующих дивизора $\operatorname{div} I$.*

Предложение 7. *У всякого дивизора $\operatorname{div} I$ есть конечная система образующих, причем если I — точный обратимый дивизор, то $\mu_A(\operatorname{div} I)\leqslant 2$, а в противном случае $\mu_A(\operatorname{div} I)=\sup\{\mu_{A_p}(I_p)\mid p\in P\}$. Учитывая, что $\mu_{A_p}(I_p)\leqslant m_p+1$ [3], получаем отсюда следствие.*

Следствие. *Если $A\neq A^0$, то для любого дивизора $\operatorname{div} I$ $\mu_A(\operatorname{div} I)\leqslant$ $\leqslant\sup\{m_p+1\mid p\in P$ и $I_p\not\cong A_p\}\leqslant m(A)+1$.*

Доказательство основывается на следующей лемме.

Лемма 3. *Пусть $S=\{p_1,\ldots,p_t\}$ — конечное множество простых идеалов кольца A, причем $p_i\not\subset p_j$ при $i\neq j$; M — произвольный A-модуль и x_i — некоторый элемент из M_{p_i} для каждого $i=1,\ldots,t$. Тогда существует элемент $x\in M$, такой, что $xA_{p_i}+p_iM_{p_i}=x_iA_{p_i}+p_iM_{p_i}$ для всех $i=1,\ldots,t$.*

Доказательство. Обозначим $\mathfrak{a}_i=\prod_{j\neq i}p_j$. Тогда $\mathfrak{a}_i\not\subset p_i$, значит, идеал $\mathfrak{a}=\sum_{i=1}^{t}\mathfrak{a}_i$ не содержится ни в каком из p_i, а следовательно, $\mathfrak{a}\not\subset$

* Обратим внимание, что, даже если идеал I дивизориален и конечнопорожден, а кольцо A нетерово, возможно $\mu_A(\operatorname{div} I)\neq\mu_A(I)$.

$\not\subset \bigcup\limits_{i=1}^{t} p_i$ (см. [4], гл. II, § 1). Поэтому найдутся элементы $a_i \in \mathfrak{a}_i$, такие, что $\sum\limits_{i=1}^{t} a_i \notin \bigcup\limits_{i=1}^{t} p_i$.

Пусть $x_i = y_i/z_i$, где $y_i \in M$, $z_i \in A \setminus p_i$. Положим $x = \sum\limits_{i=1}^{t} a_i y_i$. Поскольку $a_j \in p_i$ при $j \neq i$, $xA_{p_i} + p_i A_{p_i} = a_i y_i A_{p_i} + p_i A_{p_i} = x_i A_{p_i} + p_i A_{p_i}$, так как $a_i \notin p_i$ и, значит, $a_i/z_i \in A^*_{p_i}$.

Доказательство предложения 7. Положим $S = \{p_1, \ldots, p_s\}$ — множество всех тех $p \in P$, для которых $I_p \not\simeq A_p$. Для каждого p_i выберем элемент $x_i \in I_{p_i} \setminus p_i I_{p_i}$, и пусть $x \in I$ — такой элемент, что $xA_{p_i} + p_i I_{p_i} = x_i I_{p_i} + p_i I_{p_i}$ для всех $i = 1, \ldots, s$ (если $S = \varnothing$, в качестве x возьмем любой элемент из I, обратимый в Q). Добавляя к x элементы из $p_1 p_2 \ldots p_t I$, можно сделать x обратимым в Q. Рассмотрим модуль $M = I \mid xA$. Обозначим $T = \{p_1, \ldots, p_t\}$ $(t \geqslant s)$ множество всех тех $p \in P$, для которых $M_p \neq 0$ (оно конечно, так как I и xA — дробные идеалы). Поскольку $x \notin p_i I_{p_i}$ $(i = 1, \ldots, s)$, из леммы Накаяма следует, что $\mu_{A_{p_i}}(M_{p_i}) = \mu_{A_{p_i}}(I_{p_i}) - 1$ при $i = 1, \ldots, s$. С другой стороны, при $i = s + 1, \ldots, t$ модуль I_{p_i}, а значит, и M_{p_i} цикличен. Пусть $n = \sup \{\mu_{A_{p_i}}(I_{p_i}) \mid i = 1, \ldots, s\}$ (или $n = 2$, если $S = \varnothing$). Тогда для любого $i = 1, \ldots, t$ в модуле M_{p_i} можно выбрать систему из $n - 1$ образующих $\{b_{i2}, \ldots, b_{in}\}$. Пользуясь леммой 3, построим в M элементы $b_2, \ldots, b_n$, такие, что $b_j A_{p_i} + p_i M_{p_i} = b_{ij} A_{p_i} + p_i M_{p_i}$. По лемме Накаяма, тогда $\sum\limits_{j=2}^{n} b_j A_{p_i} = M_{p_i}$ для всех $i = 1, \ldots, t$. Следовательно, полагая $a_1 = x$, a_j — прообраз b_j в I $(j = 2, \ldots, t)$, мы видим, что если J — идеал, порожденный $a_1, \ldots, a_n$, то $J_p = I_p$ для всех p, т. е. $\operatorname{div} I = \operatorname{div} J = \operatorname{div}(a_1, \ldots, a_n)$, что и требовалось доказать.

Замечание. Если число критических простых идеалов конечно, т. е. A^0 является дробным A-идеалом, то, очевидно, $m(A) = \mu_A(\operatorname{div} A^0) - 1$. Для одномерных нетеровых колец предложение 7 было доказано в [9].

Аналогично из теоремы 2 и следствия 3 выводится следующая теорема.

Теорема 4. *Полугруппа родов $G(A)$ конечна тогда и только тогда, когда у A есть лишь конечное число критических простых идеалов $p \in P$ и для тех критических p, для которых поля k_p бесконечны,* выполнены условия:*

1) $m_p \leqslant 2$;

2) $\mu_{A_p}(A_p + pA^0_p / A_p) \leqslant 1$.

В частности, если все поля k_p для строго критических p бесконечны, эти условия можно переписать так: $m(A) \leqslant 2$ и $\mu_A(\operatorname{div} A^1) \leqslant 2$, где $\operatorname{div} A^1$ — верхняя грань (т. е. пересечение) минимальных дивизоров, содержащих $\operatorname{div} A^0$ и содержащихся в $\operatorname{div} A$.

Наконец, выясним условия, при которых будет конечной полугруппа классов дивизоров $C(A)$. Тривиально необходимыми условиями для этого являются конечность $G(A)$ и $C(A^0)$. Если все поля k_p для критических

---

* В частности, для немаксимальных критических p.

$p \in P$ конечны, из предложения 6 следует, что данные условия и достаточны. В общем случае это уже не так. Например, имеет место следующее предложение.

Предложение 8. *Предположим, что у кольца A есть критический простой идеал $p \in P$ с бесконечным полем k_p, а фактор-группа $A^{0*}/\bar{A}^*$ конечно порождена.*** *Тогда $C(A)$ бесконечна.*

Доказательство. Поскольку идеал p — критический, $\bar{B} = O(p) \neq A$ [3]. Применяя предложение 6 к паре колец A и B, мы видим, что достаточно установить бесконечность фактор-группы $B_p^* | \varphi(\widetilde{B}^*) A_p^*$, где $\varphi: \widetilde{B} \to B_p$ — канонический гомоморфизм. Учитывая, что $pB_p = pA_p$, эту фактор-группу можно заменить на $F^*/\pi(\widetilde{B}^*) k^*$, где $k = k_p$, $F = B_p/pB_p$, $\pi: \widetilde{B} \to F$ — композиция φ с проекцией $B_p \to F$. Но F^*/k^* — линейная алгебраическая группа над полем k, а $\pi(\widetilde{B}^*) k^*/k^* \simeq \pi(\widetilde{B}^*)/\pi(\widetilde{B}^*) \cap k^* = \pi(\widetilde{B}^*)/\pi(\bar{A}^*)$ — конечно порожденная подгруппа в F^*/k^*. Проводя в F^*/k^* композиционный ряд и учитывая, что ни в мультипликативной, ни в аддитивной группе бесконечного поля k нет конечно порожденных подгрупп конечного индекса, мы видим, что фактор-группа $F^*/\pi(\widetilde{B}^*) k^*$ бесконечна, что и требовалось доказать.

По-видимому, вопрос о конечности $C(A)$, даже в предположении конечности $C(A^0)$ (что само по себе весьма нетривиально), является довольно сложным и тонким, несмотря на то, что предложение 6 дает достаточно удобный подход к решению этой задачи.

Литература

1. Dade E. C., Taussky O., Zassenhaus H. On the theory of orders, in particular on the semigroup of idealclasses and genera of an order in an algebraic number field.— Math. Ann., 1962, Bd 148, N 1, S. 31—64.
2. Фаддеев Д. К. К теории кубических Z-колец.— Тр. Мат. ин-та АН СССР, 1965, т. 80, с. 183—187.
3. Дрозд Ю. А. Идеалы коммутативных колец.— Мат. сб., 1976, т. 101, № 3, с. 22—34.
4. Бурбаки Н. Коммутативная алгебра. М., 1971. 707 с.
5. Джекобсон Н. Теория колец. М., 1947. 287 с.
6. Боревич З. И., Шафаревич И. Р. Теория чисел. М., 1972. 495 с.
7. Фаддеев Д. К. Введение в мультипликативную теорию модулей целочисленных представлений.— Тр. Мат. ин-та АН СССР, 1965, т. 80, с. 145—182.
8. Дрозд Ю. А., Ройтер А. В. Коммутативные кольца с конечным числом целочисленных неразложимых представлений.— Изв. АН СССР. Сер. мат., 1976, т. 31, № 4, с. 783—798.
9. Bass H. On the ubiquity of Gorenstein rings.— Math. Z., 1963, Bd 82, N 1, S. 8—28.

** Эти условия, как правило, выполняются в «геометрической» ситуации, когда A — кольцо регулярных функций на аффинном многообразии.