Кольца с наибольшим общим делителем

А. Н. КОРЮКИН
Институт математики им. С. Л. Соболева, Новосибирск
e-mail: koryukin@math.nsc.ru

А. М. СЕБЕЛЬДИН
Нижегородский государственный педагогический университет
e-mail: amseb@mail.ru

А. Л. СИЛЛА
Конакрийский государственный университет, Гвинея
e-mail: alfalaminesylla@yahoo.fr

УДК 512.711

Ключевые слова: область целостности, факториальное кольцо, почти факториальное кольцо, простые элементы, неразложимые элементы.

Аннотация

Найден класс колец, лежащий строго между классом ассоциативно коммутативных факториальных колец и классом областей целостности. Это класс НОД-колец, или почти факториальных колец, т. е. областей целостности, где любые два элемента имеют наибольший общий делитель.

Abstract

A. N. Koryukin, A. M. Sebeldin, A. L. Sylla, Rings with the greatest common divisor, Fundamentalnaya i prikladnaya matematika, vol. 16 (2010), no. 7, pp. 69—74.

We have found some class between the class of associative commutative factorial rings and the class of domains of integrity. It is the class of GCD-rings or almost factorial rings, i.e., domains of integrity where any two elements have a greatest common divisor.

Мы рассматриваем только ассоциативные коммутативные кольца с единицей, отличной от нуля. Ненулевой необратимый элемент кольца назовём неразложимым или неприводимым, если любой его делитель тривиален, т. е. обратим, или делится на этот элемент, в противном случае элемент будем называть приводимым. Пусть A — кольцо. Тогда имеем разбиение

$$A = OA \cup UA \cup IA \cup RA,$$

где $OA = \{0_A\}$, UA, IA, RA — все обратимые элементы, все неразложимые элементы, все приводимые элементы из A соответственно. Кольцо A называется целостным или областью целостности, если для любых $a, b \in A$ из $ab = 0$ следует $a = 0$ или $b = 0$. Говорим, что кольцо A факториальное, если A является областью целостности и выполнены следующие два условия:

Фундаментальная и прикладная математика, 2010, том 16, № 7, с. 69—74.

1) для любого элемента a кольца A, такого что $a \notin OA \cup UA$, найдутся элементы $p_1, \ldots, p_k \in IA$, для которых

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_k;$$

2) это разложение единственно в следующем смысле: если $a = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ (где $q_1, q_2, \ldots, q_s \in IA$), то $s = k$ и существует перестановка $\alpha \in \mathrm{S}_k$, такая что $p_i \sim q_{\alpha(i)}$ (т. е. p_i делится на $q_{\alpha(i)}$ и $q_{\alpha(i)}$ делится на p_i, в этом случае говорят, что элементы p_i и $q_{\alpha(i)}$ ассоциированные).

Совокупность всех общих делителей двух элементов a, b кольца A будем обозначать через $\mathrm{D}(a, b)$, множество всех наибольших общих делителей, т. е. таких элементов из $\mathrm{D}(a, b)$, которые делятся на все элементы из $\mathrm{D}(a, b)$, обозначим через $\mathrm{NOD}(a, b)$. Положим $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Пример 1 показывает, что существуют области целостности, в которых для некоторых элементов a, b не существует никакого наибольшего общего делителя, т. е. $\mathrm{NOD}(a, b) = \varnothing$. С другой стороны, в факториальных кольцах $\mathrm{NOD}(a, b) \neq \varnothing$ для любой пары элементов (a, b) (см. теорему 2).

Определение 1 [1, 3]. Пусть A — область целостности. Говорим, что A — НОД-кольцо, или почти факториальное кольцо, если $\mathrm{NOD}(a, b) \neq \varnothing$ для всех $a, b \in A$.

Пример 1. Пусть

$$A = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \colon a, b \in \mathbb{Z}\},$$

где $\sqrt{\cdot}$ означает положительный квадратный корень. Покажем, что $\mathbb{Z}[i\sqrt{5}]$ не является НОД-кольцом.

Действительно, если $\alpha = a + bi\sqrt{5},\ \beta = c + di\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$, то $\alpha - \beta \in \mathbb{Z}[i\sqrt{5}]$. Следовательно, $\mathbb{Z}[i\sqrt{5}]$ является кольцом и даже областью целостности (так как $\mathbb{Z}[i\sqrt{5}] \subseteq \mathbb{C}$).

Покажем, что $\mathrm{NOD}\big(9, 3(2 + i\sqrt{5})\big) = \varnothing$. Вначале напомним полезное понятие. Если $x = a + bi \in \mathbb{C}$, то $\mathrm{n}(x) = a^2 + b^2 = |a + b|^2$ — норма числа x. Найдём совокупность $\mathrm{D}_{\mathrm{nt}}(9)$ всех собственных (нетривиальных) делителей для числа 9. Имеем $9 = (a + bi\sqrt{5})(c + di\sqrt{5})$, что влечёт $81 = (a^2 + 5b^2)(c^2 + 5d^2)$, и если $a + bi\sqrt{5},\ c + di\sqrt{5} \in \mathrm{D}_{\mathrm{nt}}(9)$, то $\mathrm{n}(a + bi\sqrt{5}) = \mathrm{n}(c + di\sqrt{5}) = 9$. Поэтому $9 = 3^2 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ и $\mathrm{D}_{\mathrm{nt}}(9) = \{3, 2 + i\sqrt{5}, 2 - i\sqrt{5}\}$. Заметим, что все эти делители неразложимы, т. е. $\mathrm{D}_{\mathrm{nt}}(9) \subseteq I(\mathbb{Z}[i\sqrt{5}])$. Теперь видим, что $\mathrm{NOD}\big(9, 3(2 + i\sqrt{5})\big) = \varnothing$. Таким образом, $\mathbb{Z}[i\sqrt{5}]$ не является НОД-кольцом.

Замечание 1. Кольцо $A = \mathbb{Z}[i\sqrt{5}]$ не является факториальным. Действительно, $9 = 3^2 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

Определение 2. Пусть A — кольцо. Ненулевой необратимый элемент x из A назовём простым, если прост [2] идеал $\langle x \rangle$, порождённый этим элементом, т. е. если $a, b \in A$ и x делит ab, то x делит по крайней мере один из элементов a, b.

Замечание 2. В кольце $A = \mathbb{Z}[i\sqrt{5}]$ неприводимые элементы 3, $2 + i\sqrt{5}$, $2 - i\sqrt{5}$ не являются простыми.

Однако имеет место следующая теорема.

Теорема 1. *Для любого НОД-кольца A элемент $x \in A$ неприводим тогда и только тогда, когда он прост.*

Доказательство. Достаточность. Пусть элемент $x \in A$ простой, т. е. идеал $\langle x \rangle$ прост. Покажем, что $x \in IA$. Предположим, что $x = yz$ для некоторых $y, z \in IA$. Тогда $yz = x \cdot 1_A$. Значит, x делит y или x делит z. Если x делит y, то $y \sim x$, пусть $y = xw$. Имеем $x = yz = xwz$. Таким образом, $x(wz - 1_A) = 0$. Так как x — ненулевой элемент, то $wz = 1_A$ и $w, z \in UA$, т. е. элемент z обратим. Аналогично, если x делит z, то $z \sim x$ и y обратим. Таким образом, сомножители y и z — тривиальные делители x, а это означает, что $x \in IA$.

Необходимость. Предполагаем, что элемент x неразложим, т. е. $x \in IA$. Покажем, что x прост. Предположим, что x делит ab. Допустим, что x не делит a. Так как A является НОД-кольцом, то совокупность $\mathrm{NOD}(x, a) = x \wedge a$ не является пустой.

Покажем, что $\mathrm{NOD}(x, a) = x \wedge a = UA$. Пусть $d \in \mathrm{NOD}(a, x)$. Так как d делит x, то или $d \in UA$, или $d \sim x$. Если $d \sim x$, то x делит d. Но d делит a, откуда следует, что x делит a. Противоречие. Из этого противоречия получаем, что $d \in UA$ и $x \wedge a = UA$.

Пусть $y \in ab \wedge xb$. Тогда y делит ab и y делит xb. Следовательно, существуют $v, w \in A$, такие что $ab = vy$ и $xb = wy$. Но, с другой стороны, $b \in \mathrm{D}(ab, xb)$, где $\mathrm{D}(ab, xb)$ — совокупность всех общих делителей элементов ab и xb. Следовательно, b делит y.

Пусть $bz = y$ для $z \in A$. Тогда $ab = vbz$, $xb = wbz$. Следовательно, $a = vz$, $x = wz$, так как A является областью целостности. Так как $x \wedge a = UA$, то $z \in UA$ и $y \sim b$. С другой стороны, x делит ab и x делит xb. Таким образом, x делит y и b. □

Определение 3. Говорят, что кольцо является кольцом главных идеалов, если любой его идеал главный.

Теорема 2. *Любое факториальное кольцо A является НОД-кольцом.*

Доказательство. Фиксируем во всех классах эквивалентности множества IA единственный элемент и обозначим эту совокупность через $IP(A)$. Обозначим через $P(a)$ множество всех элементов $p \in IP(A)$ из канонического разложения элемента a. Имеем

$$a = u(a) \cdot \prod_{p \in P(a)} p^{\nu(p,a)},$$

где $u(a) \in UA$, $\nu(p, a) \in \mathbb{N}^*$. Пусть $a, b \in A$. Рассмотрим канонические разложения

$$a = u(a) \cdot \prod_{p \in P(a)} p^{\nu(p,a)}, \quad b = u(b) \cdot \prod_{p \in P(b)} p^{\nu(p,b)}$$

элементов a и b. Без ограничения общности можно считать, что $P(a) = P(b)$, $\nu(p,a), \nu(p,b) \in \mathbb{N}$. Тогда

$$\prod_{p \in P(a)} p^{\min(\nu(p,a),\nu(p,b))} \in \mathrm{NOD}(a,b).$$

Таким образом, A является НОД-кольцом. □

Теорема 3. *Любое кольцо главных идеалов является НОД-кольцом.*

Доказательство. Если A — кольцо главных идеалов, то для любых $a, b \in A$ найдётся такой элемент $x \in A$, что $\langle a \rangle + \langle b \rangle = \langle x \rangle$. Тогда найдутся такие элементы $x_1, x_2 \in A$, что $x_1 a + x_2 b = x$. Так как $a, b \in \langle x \rangle$, видим, что x делит a и x делит b. Значит, $x \in \mathrm{D}(a,b)$. Для $y \in \mathrm{D}(a,b)$ очевидно, что y делит x. Следовательно, $x \in \mathrm{NOD}(a,b)$. □

Теорема 4. *Любое нётерово НОД-кольцо факториально.*

Доказательство. Пусть A — нётерово НОД-кольцо. Предположим, что существует такой элемент $a \in A$, что $a \notin OA \cup UA$ и a не разложим в конечное произведение неприводимых элементов. Рассмотрим главный идеал $\langle a \rangle = aA$. Так как a разложим, найдутся такие $b, c \in A$, что $a = bc$, и это разложение не тривиально, т. е. $b, c \notin OA \cup UA$. В силу выбора элемента $a \in A$ получаем, что по крайней мере один из элементов b или c принадлежит RA. Будем считать, что $b \in RA$. Тогда найдутся такие $b_1, c_1 \in A$, что $b_1, c_1 \notin OA \cup UA$ и $b = b_1 c_1$.

Если, например, $b_1 \in RA$, то найдутся такие $b_2, c_2 \in A$, что $b_2, c_2 \notin OA \cup UA$ и $b_1 = b_2 c_2$, где, например, $b_2 \in RA$, и т. д. Имеем бесконечный ряд $a, b_1, b_2, b_3, \ldots$, где $b_i \in RA$ и b_{i+1} делит b_i. Таким образом, имеем бесконечную строго возрастающую цепочку идеалов $\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle \subset \langle b_3 \rangle \subset \ldots$. Однако кольцо A нётерово. Противоречие. Следовательно, существует разложение элемента a в конечное произведение неразложимых элементов. Так как A является НОД-кольцом, произвольный элемент неразложим тогда и только тогда, когда он прост (теорема 1).

Пусть $a = p_1 p_2 \cdots p_k$, где элементы $p_1, p_2, \ldots, p_k$ просты. Покажем, что это разложение единственно. Если элемент a прост, это очевидно.

Предположим, что единственность имеет место для k элементов, и покажем, что она имеет место также для $k+1$. Пусть

$$a = p_1 \cdot \ldots \cdot p_k \cdot p_{k+1} = q_1 \cdot \ldots \cdot q_s \cdot q_{s+1} -$$

два разложения элемента a в произведение неприводимых элементов. Тогда элемент p_{k+1} делит по крайней мере один из сомножителей $q_1, \ldots, q_s, q_{s+1}$. Можно считать, что p_{k+1} делит q_{s+1}. Значит, существует такой элемент $u \in UA$, что $u \cdot p_{k+1} = q_{s+1}$. Имеем

$$a = p_1 \cdot \ldots \cdot p_k \cdot p_k + 1 = q_1 \cdot \ldots \cdot q_s \cdot u \cdot p_{k+1}.$$

Отсюда следует, что

$$a = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_s \cdot u.$$

Применяя индукцию, закончим доказательство. □

Из теоремы 4 и того, что любое кольцо главных идеалов нётерово, незамедлительно вытекает следующий хорошо известный результат.

Теорема 5. *Любое кольцо главных идеалов факториально.*

Теорема 6. *Класс факториальных колец является собственным подклассом класса НОД-колец.*

Доказательство. Напомним сначала, что класс НОД-колец содержит класс факториальных колец. Нужно показать, что класс НОД-колец строго содержит класс факториальных колец, т. е. что существует нефакториальное НОД-кольцо.

Рассмотрим кольцо $\mathbb{Q}[x_1]$ многочленов над полем $\mathbb{Q}$ рациональных чисел. Рассмотрим также кольца $\mathbb{Q}[x_1][x2] = \mathbb{Q}[x_1, x_2]$, где $x_1 = x_2^2$, $\mathbb{Q}[x_1, x_2, x_3]$, где $x_2 = x_3^2, \ldots$, $\mathbb{Q}[x_1, x_2, \ldots, x_k]$, где $x_{k-1} = x_k^2$. Полагая $\mathbb{Q}_k = \mathbb{Q}_{k-1}[x_k]$ ($\mathbb{Q}_1 = \mathbb{Q}[x_1]$) и продолжая процесс до бесконечности, имеем

$$\mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \mathbb{Q}_3 \subset \ldots \subset \mathbb{Q}_k \subset \ldots .$$

Обозначим через $\mathbb{Q}^+$ объединение возрастающей цепочки этих колец. Очевидно, что кольцо $\mathbb{Q}^+$ ассоциативно, коммутативно и является областью целостности.

Покажем, что $\mathbb{Q}^+$ является НОД-кольцом. Покажем сначала, что x_i — необратимые в $\mathbb{Q}^+$ элементы для всех $i \in \mathbb{N}^*$. Действительно, предположим, что x_1 обратим. Тогда существует элемент $y_1 \in \mathbb{Q}^+$, такой что $x_1 y_1 = 1$. Свойство $y_1 \in \mathbb{Q}^+$ означает, что существует $s \in \mathbb{N}^*$, для которого $y_1 \in \mathbb{Q}_s$ и $x_1 y_1 = 1$ в $\mathbb{Q}_s$.

Тогда $x_1 y_1 \in \mathbb{Q}$, так как единственные обратимые элементы в $\mathbb{Q}_s$ — это обратимые элементы из $\mathbb{Q}$. Но это невозможно, так как любой элемент из $\mathbb{Q}$ является алгебраическим над $\mathbb{Q}$, в то время как элемент x_1 трансцендентный. Из этого следует, что элементы x_i для всех $i = 1, 2, 3, \ldots$ необратимы.

Покажем теперь, что $\mathbb{Q}^+$ является НОД-кольцом. Пусть α и β — два произвольных элемента из $\mathbb{Q}^+$. Существует целое положительное число k, такое что $\alpha, \beta \in \mathbb{Q}_k$. Значит, $\alpha = \alpha(x_k)$ и $\beta = \beta(x_k)$. Так как α и β являются многочленами от одной переменной, в кольце $\mathbb{Q}_k$ существует их наибольший общий делитель. Пусть $\mathrm{NOD}(\alpha, \beta) = \gamma \in \mathbb{Q}_k$. По теореме Безу в $\mathbb{Q}_k$ существуют два многочлена $u(x_k)$ и $v(x_k)$, такие что

$$u(x_k)\alpha(x_k) + v(x_k)\beta(x_k) = \gamma(x_k).$$

Покажем, что γ также является наибольшим общим делителем элементов α, β в $\mathbb{Q}^+$. Для этого достаточно показать, что произвольный общий делитель δ многочленов α, β также делит в $\mathbb{Q}^+$ элемент γ. Учитывая последнее равенство, видим, что если δ делит α и β, то δ делит γ. Таким образом, $\mathbb{Q}^+$ является НОД-кольцом.

Покажем, наконец, что кольцо $\mathbb{Q}^+$ не является факториальным. Для этого достаточно показать, что x_1 не разложим в конечное произведение неприводимых сомножителей. Мы уже знаем, что x_1 не является единицей кольца $\mathbb{Q}^+$ и для любого $m \geqslant 2$ он не является неприводимым в $\mathbb{Q}_m$, так как $x_1 = x_m^{\nu(m)}$, где $\nu(m) = 2^{m-1}$.

Предположим теперь, что A факториально и

$$x_1 = p_1 \cdot p_2 \cdot \ldots \cdot p_t,$$

где p_j $(1 \leqslant j \leqslant t)$ неразложимы в $\mathbb{Q}^+$. Тогда существует число $m \in \mathbb{N}^*$, такое что $p_1, p_2, \ldots, p_t \in \mathbb{Q}_m$. Ясно, что $p_1, p_2, \ldots, p_t \in I\mathbb{Q}_m$.

Равенство $x_1 = x_m^{\nu(m)}$ показывает, что тогда $\nu(m) = t$ and $p_j = q_j x_m$, где q_j — ненулевой элемент из $\mathbb{Q}$. Так как элементы p_j неприводимы в $\mathbb{Q}^+$, они также неприводимы в $\mathbb{Q}_{m+1}$. Но в $\mathbb{Q}_{m+1}$ $x_m = x_{m+1}^2$. Значит, элементы p_j являются приводимыми. Противоречие. Таким образом, НОД-кольцо $\mathbb{Q}^+$ не является факториальным. □

Литература

[1] Корюкин А. Н., Себельдин А. М., Sylla A. L. Почти факториальные кольца // Материалы Всероссийского симпозиума по абелевым группам. — Бийск: РИО БГПУ им. В. М. Шукшина, 2006. — С. 29—30.

[2] Мельников О. В., Ремесленников В. Н., Романьков В. А., Скорняков Л. А., Шестаков И. П. Общая алгебра. Т. 1. — М.: Наука, 1990.

[3] Fofana S. L., Sebeldin A. M., Sylla A. L. Algèbre. Introduction a la théorie des anneaux. — Conakry: Édit. Univ., 2004.