УДК 512.552.3

П. А. Фрейдман, И. Л. Хмельницкий

О КОЛЬЦАХ, В КОТОРЫХ ПОДКОЛЬЦА МОНОГЕННЫХ ПОДКОЛЕЦ МОНОГЕННЫ

1. *A*-кольца простой характеристики

Все рассматриваемые кольца предполагаются ассоциативными. Известно, что во всякой группе любая подгруппа моногенной подгруппы сама моногенна. Аналогичное утверждение для колец несправедливо. Поэтому естественно изучить кольца со свойством, указанным в заглавии. Такие кольца будем для краткости называть *A-кольцами.* Очевидно, что во всяком A-кольце любое моногенное подкольцо является D_1-кольцом, т. е. кольцом, в котором всякое конечно порожденное подкольцо моногенно. Отметим, что D_1-кольца были изучены в работах [1] и [2]. Приведем необходимые для дальнейшего сведения о строении D_1-колец.

Предложение 1.1. *Кольцо R простой характеристики p тогда и только тогда является D_1-кольцом без нильпотентных элементов, отличных от нуля, когда R изоморфно прямой сумме колец F_i $(i = 1, \ldots, n)$, каждое из которых есть либо конечное поле, либо объединение возрастающей последовательности конечных полей, причем $n \leq p - 1$.*

Предложение 1.2. *Кольцо R простой характеристики тогда и только тогда является D_1-нилькольцом, когда $R = \langle r \mid r^3 = 0\rangle$.*

Предложение 1.3. *Кольцо R без кручения тогда и только тогда является D_1-кольцом, когда R изоморфно либо кольцу с нулевым умножением и аддитивной группой ранга 1, либо ненулевому подкольцу поля рациональных чисел.*

Следующая лемма очевидна.

Лемма 1.1. *Всякое конечное D_1-кольцо является A-кольцом.*

Теорема 1.1. *Кольцо R простой характеристики p является A-нилькольцом тогда и только тогда, когда оно удовлетворяет тождеству $x^3 = 0$.*

Доказательство. Пусть $a \in R$. Тогда подкольцо $\langle a \rangle$ является D_1-кольцом. Поэтому из описания D_1-нильколец простой характеристики (см. предложение 1.2) следует, что $a^3 = 0$.

Обратное утверждение вытекает из леммы 1.1 и предложения 1.2.

Лемма 1.2. *Полная прямая сумма простых полей характеристики p является A-кольцом.*

Доказательство. Пусть $R = \prod\limits_{i \in S} F_i$, где всякое F_i – простое поле характеристики p с единицей e_i. Пусть $a \in R$ и $a(i) = \alpha_i e_i$, где $\alpha_i \in \{0, 1, \ldots, p-1\}$, $i \in S$. Обозначим $S_j = \{i \in S | \alpha_i = j\}$ $(j = 1, \ldots, p-1)$. Обозначим далее через u_j такой элемент из R, для которого

$$u_j(i) = \begin{cases} e_i, & \text{если } i \in S_j, \\ 0, & \text{если } i \notin S_j. \end{cases}$$

Легко видеть, что элементы $u_1, \ldots, u_{p-1}$ образуют ортогональную систему идемпотентов в кольце R, причем $a = \sum\limits_{j=1}^{p-1} j u_j$. Поэтому

$$\langle a \rangle \subset \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \cdots \oplus \langle u_{p-1} \rangle,$$

так что $\langle a \rangle$ есть подкольцо прямой суммы k простых полей характеристики p и $k \leq p - 1$. Из предложения 1.1 следует, что $\langle a \rangle$ есть D_1-кольцо. Значит, $\langle a \rangle$ является конечным D_1-кольцом и в силу леммы 1.1 R является A-кольцом.

Лемма 1.3. *Кольцо $R = F_1 \oplus F_2 \oplus \cdots \oplus F_p$, где F_j $(j = 1, 2, \ldots, p)$ – конечные поля характеристики p, хотя бы одно из которых непростое, не является A-кольцом.*

Доказательство. Пусть для определенности F_1 – непростое поле и $F_1 = \langle a_1 \rangle$, где a_1 – корень неприводимого по модулю p многочлена $f(x)$.

Положим

$$a = a_1 + \alpha_2 e_2 + \cdots + \alpha_p e_p, \tag{1}$$

где α_i – попарно различные числа из множества $\{1, \ldots, p-1\}$, а e_j – единицы полей F_j $(j = 2, \ldots, p)$. Тогда

$$\begin{aligned} f(a) &= f(a_1) + f(a_2 e_2) + \cdots + f(\alpha_p e_p) = \\ &= f(\alpha_2 e_2) + \cdots + f(\alpha_p e_p) = f(\alpha_2) e_2 + \cdots + f(\alpha_p) e_p. \end{aligned}$$

Так как $f(x)$ – неприводимый по модулю p многочлен степени выше первой, то $f(\alpha_j) \neq 0$ для каждого α_j. Поэтому по теореме Ферма

$$f^{p-1}(a) = e_2 + \cdots + e_p \tag{2}$$

и, следовательно,

$$af^{p-1}(a) = \alpha_2 e_2 + \cdots + \alpha_p e_p. \tag{3}$$

Покажем, что $e_j \in \langle a \rangle$ для всякого $j \geq 2$. Обозначим $f^{p-1}(a)$ через e и $af^{p-1}(a)$ через b. Из равенств (2) и (3) следует, что $e, b \in \langle a \rangle$. Тогда

$$b - \alpha_j e = \sum_{i=2}^{p} (\alpha_i - \alpha_j) e_i.$$

Так как $\alpha_i - \alpha_j \neq 0$ для всякого $i \neq j$, то $(b - \alpha_j e)^{p-1} = (\sum\limits_{i=2}^{p} e_i) - e_j$ и поэтому $e - (b - \alpha_j e)^{p-1} = e_j$. Значит, $e_j \in \langle a \rangle$. Но тогда, как следует из равенства (1), $a_1 \in \langle a \rangle$. Таким образом, $\langle a \rangle = F_1 \oplus \langle e_2 \rangle \oplus \cdots \oplus \langle e_p \rangle$. Из предложения 1.1 следует, что $\langle a \rangle$ – не D_1-кольцо, поэтому R не является A-кольцом.

Теорема 1.2. *Кольцо R простой характеристики p является A-кольцом без ненулевых нильпотентных элементов тогда и только тогда, когда R есть кольцо одного из следующих типов:*

1) *подпрямая сумма конечных простых полей;*

2) *прямая сумма $F_1 \oplus F_2 \oplus \cdots \oplus F_k$, где $k \leq p-1$, F_j $(j = 1, \ldots, k)$ – конечные поля или объединения возрастающей последовательности конечных полей, причем хотя бы одно из F_j не является простым полем.*

Доказательство. Пусть R есть A-кольцо простой характеристики p без нильпотентных элементов, отличных от нуля. Так как R – алгебраическое кольцо, то R является алгебраической алгеброй над конечным простым полем и поэтому коммутативно. Следовательно, R, будучи коммутативным полупростым кольцом, есть подпрямая сумма алгебраических полей F_j характеристики p. При этом легко проверяется, что F_j является конечным полем или объединением возрастающей последовательности конечных полей.

Если все F_j – простые поля, то R будет кольцом первого из указанных в формулировке теоремы типов.

Пусть существует такое j, для которого поле F_j не является простым. В этом случае поле F_j содержит подкольцо S, являющееся конечным непростым полем. Тогда $S = \langle b \rangle$, где b – корень неприводимого по модулю p многочлена $f(x)$ степени $n > 1$. Пусть a – такой элемент из кольца R, что $a(j) = b$. Так как R – алгебраическое кольцо, то $\langle a \rangle$ конечно и поэтому

$$\langle a \rangle = S_1 \oplus S_2 \oplus \cdots \oplus S_m,$$

где $S_i \quad (i = 1, \ldots, m)$ – конечные поля. Предположим, что все S_i – простые поля. Тогда $a^p = a$ и поэтому $b^p = b$. Так как b является корнем неприводимого многочлена $f(x)$, то 1 делится на n. Полученное противоречие показывает, что среди подколец S_i имеется хотя бы одно непростое поле.

Пусть P – подкольцо кольца R, являющееся конечным непростым полем и $P = \langle c \rangle$. Предположим, что кольцо R содержит p ортогональных идемпотентов e_i, отличных от нуля. Пусть $M = \langle c, e_1, \ldots, e_p \rangle$. Так как R – коммутативное алгебраическое кольцо, то M конечно и, следовательно,

$$M = T_1 \oplus \cdots \oplus T_l,$$

где $T_j \ (j = 1, \ldots, l)$ – конечные поля. Из ортогональности идемпотентов $e_1, \ldots, e_l$ вытекает, что $l \geq p$. Кроме того, из равенства $P = \langle c \rangle$ следует, что хотя бы одно T_j – непростое поле. Получили противоречие с леммой 3.1.

Таким образом, мы установили, что всякая ортогональная система ненулевых идемпотентов кольца R состоит из не более чем $p - 1$ идемпотентов. Поэтому $R = F_1 \oplus \cdots \oplus F_k$, где $k \leq p - 1$, $F_i \ (i = 1, \ldots, k)$ – конечные поля или объединения возрастающей последовательности конечных полей. Действительно, пусть $u_1, \ldots, u_k$ – ортогональная система ненулевых идемпотентов кольца R наибольшей мощности. Согласно предыдущему, $k \leq p - 1$. Тогда, применяя пирсовское разложение кольца R по этим идемпотентам, получаем

$$R = u_1 R \oplus u_2 R \oplus \cdots \oplus u_k R \oplus (1 - u)R,$$

где $u = u_1 + \cdots + u_k$. При этом $(1 - u)R = 0$, так как иначе в $(1 - u)R$ существует ненулевой идемпотент, ортогональный к идемпотентам $u_1, \ldots, u_k$. Кроме того, u_j – единственный ненулевой идемпотент в кольце $u_j R$. В самом деле, если e – ненулевой идемпотент из $u_j R$ и $e \neq u_j$, то e и $u_j - e$ суть ненулевые ортогональные идемпотенты, ортогональные ко всем идемпотентам u_i, где $i \neq j$. Таким образом, $u_j R$ – коммутативное алгебраическое кольцо, содержащее единственный ненулевой идемпотент. Поэтому $u_j R$ есть конечное поле или объединение возрастающей последовательности конечных полей. При этом, как следует из предыдущего, хотя бы одно из колец $u_j R$, где $j = 1, \ldots, k$, не является простым полем.

Обратно, если R – подпрямая сумма конечных простых полей характеристики p, то оно является A – кольцом по лемме 2.1. Если же R есть кольцо второго типа из формулировки теоремы, то оно является D_1-кольцом по предложению 1.1 и поэтому для всякого $a \in R$ подкольцо $\langle a \rangle$ есть конечное D_1-кольцо. Следовательно, по лемме 1.1 и в этом случае R является A-кольцом.

2. *A*-кольца без кручения

Теорема 2.1. *Кольцо без кручения является A-нилькольцом тогда и только тогда, когда оно удовлетворяет тождеству $x^2 = 0$.*

Доказательство. Пусть R есть A-нилькольцо без кручения и $a \in R$. Тогда подкольцо $\langle a \rangle$ является D_1-кольцом. Поэтому из описания D_1-нильколец без кручения (см. предложение 1.3) следует, что $a^2 = 0$.

Обратное утверждение теоремы очевидно.

Замечание. Отметим, что если кольцо R без кручения удовлетворяет тождеству $x^2 = 0$, то $R^3 = 0$. В самом деле, так как R удовлетворяет тождеству $x^2 = 0$, то R антикоммутативно. Пусть $a, b, c \in R$. Тогда

$$a(bc) = a(-cb) = -(ac)b = (ca)b = c(ab) = -(ab)c,$$

откуда, учитывая, что R – кольцо без кручения, получим $abc = 0$.

Лемма 2.1. *Пусть R есть A-кольцо без кручения, a – ненулевой элемент из R, причем $a^2 = \alpha a$ для некоторого целого α. Тогда для всякого нильпотентного элемента $r \in R$ имеет место равенство*

$$ar + ra = \alpha r. \tag{4}$$

Доказательство. Так как $\langle r \rangle$ есть A-нилькольцо без кручения, то по предыдущей теореме $r^2 = 0$. Подкольцо $\langle a + r \rangle$ является D_1-кольцом. Поэтому из предложения 1.3 следует, что возможны два случая.

1. $(a + r)^2 = 0$. Тогда

$$\alpha a + ar + ra = 0. \tag{5}$$

Пусть $\alpha \neq 0$. Умножив равенство (5) справа на r, получим

$$\alpha ar + rar = 0. \tag{6}$$

Умножив равенство (6) слева на r, получим $\alpha rar = 0$ и, значит, $rar = 0$. Поэтому из равенства (6) следует, что $\alpha ar = 0$, откуда $ar = 0$. Аналогично показывается, что и $ra = 0$. Но тогда из равенства (5) вытекает, что $\alpha a = 0$, в противоречии с предположением. Значит, $\alpha = 0$ и из (5) получим $ar + ra = 0$. Таким образом, в рассматриваемом случае равенство (4) доказано.

2. $\beta(a + r)^2 = \gamma(a + r)$, где $a + r \neq 0$, β и γ – ненулевые взаимно простые числа. Тогда

$$\beta\alpha a + \beta ar + \beta ra = \gamma a + \gamma r. \tag{7}$$

Умножая равенство (7) справа на r, получаем

$$\beta\alpha ar + \beta rar = \gamma ar. \tag{8}$$

Умножая равенство (8) на r слева, будем иметь

$$(\beta\alpha - \gamma)rar = 0. \tag{9}$$

Предположим, что $\beta\alpha-\gamma \neq 0$; тогда из равенства (9) следует, что $rar = 0$, и поэтому из равенства (8) получим $ar = 0$. Аналогично можно получить, что в этом случае $ra = 0$. Тогда из равенства (7) вытекает, что

$$(\beta\alpha - \gamma)a = \gamma r. \tag{10}$$

Если $\alpha = 0$, то из (10) вытекает, что $\gamma(a + r) = 0$, и поэтому $a + r = 0$ в противоречии с рассматриваемым случаем. Если же $\alpha \neq 0$, то, умножив равенство (10) на a, получим $\alpha(\beta\alpha - \gamma) = 0$, что также невозможно. Значит, $\beta\alpha-\gamma = 0$, при этом очевидно, что $\alpha \neq 0$. Так как числа β и γ взаимно просты, можно считать, что $\beta = 1$ и, следовательно, $\alpha = \gamma$. Поэтому из равенства (7) следует, что $ar + ra = \alpha r$. Лемма доказана.

Из леммы 2.1 легко вытекает следующая

Лемма 2.2. *Пусть R есть A-кольцо без кручения, $b \in R$. Тогда для всякого нильпотентного элемента $r \in R$ имеет место равенство $rbr = 0$.*

Доказательство. Пусть b – нильпотентный элемент. Тогда $b^2 = 0$ и по лемме 2.1 $br + rb = 0$. Умножив это равенство на r, получим $rbr = 0$.

Пусть b – ненильпотентный элемент. Тогда $\beta b^2 = \gamma b$, где β и γ – ненулевые числа. Положив $a = \beta b$, получим $a^2 = \beta^2 b^2 = \beta\gamma b = \gamma a$. Поэтому, снова по лемме 2.1, $rar = 0$, т. е. $\beta rbr = 0$, откуда $rbr = 0$.

Лемма 2.3. *Пусть R есть A-кольцо без кручения, не являющееся нилькольцом. Тогда множество $N(R)$ всех нильпотентных элементов кольца R является двусторонним идеалом в R, причем $(N(R))^2 = 0$.*

Доказательство. Пусть $r_1, r_2 \in N(R)$. По лемме 2.2 $r_1r_2r_1 = r_2r_1r_2 = 0$. Поэтому $(r_1 - r_2)^3 = 0$, так что $r_1 - r_2 \in N(R)$. Кроме того, для любого $a \in R$ и любого $r \in N(R)$ выполняется равенство $rar = 0$. Поэтому $(ar)^2 = (ra)^2 = 0$ и $ar, ra \in N(R)$. Значит, $N(R)$ – двусторонний идеал кольца R.

Докажем, что $(N(R))^2 = 0$. Так как R не является нилькольцом, то в нем имеется ненулевой элемент a, для которого $a^2 = \alpha a$, где $\alpha \neq 0$. Отметим, что идеал $N(R)$ удовлетворяет тождеству $x^2 = 0$, значит, он антикоммутативен. Пусть r_1, r_2 – произвольные элементы из $N(R)$ и $r = r_1r_2$. Тогда

$$ar = (ar_1)r_2 = -r_2(ar_1) = -(r_2a)r_1 = r_1r_2a = ra,$$

и, так как для элементов a и r выполняется равенство (4), имеем $2ar = \alpha r$. Умножив это равенство слева на a, получим $2\alpha ar = \alpha ar$, т. е. $\alpha ar = 0$ и $ar = 0$. Поэтому $\alpha r = 0$. Следовательно, $r = r_1r_2 = 0$.

Теорема 2.2. *Кольцо K без кручения, не являющееся нилькольцом, есть A-кольцо тогда и только тогда, когда $K = S + R$, где S изоморфно некоторому подкольцу Q_1 поля $\mathbb{Q}$ рациональных чисел, R – идеал с нулевым умножением, причем для всякого $r \in R$ $\; ar + ra = \alpha r$, где α – наименьшее натуральное число в Q_1, a – ненулевой элемент из S, для которого $a^2 = \alpha a$.*

Доказательство. Пусть K есть A-кольцо без кручения и $K \neq N(K)$. По лемме 2.3 $N(K)$ – идеал в K, причем $(N(K))^2 = 0$. Рассмотрим фактор-кольцо $\overline{K} = K/N(K)$. Очевидно, что $\overline{K}$ – кольцо без кручения, не содержащее ненулевых нильпотентных элементов. Пусть $\overline{b} = b + N(K)$ – ненулевой элемент из $\overline{K}$, т. е. b – ненильпотентный элемент из K. Так как $\langle b\rangle$ является D_1-кольцом без кручения, то $\beta b^2 = \gamma b$, где β и γ – отличные от нуля целые числа. Следовательно, для всякого ненулевого элемента $\overline{b} \in \overline{K}$ имеет место $\beta \overline{b}^2 = \gamma \overline{b}$. Поэтому $\overline{K}$, как всякое кольцо без кручения, удовлетворяющее указанному условию, изоморфно некоторому подкольцу Q_1 поля $\mathbb{Q}$.

Пусть α – наименьшее натуральное число в Q_1, $p_i (i \in I)$ – все различные простые числа, входящие в разложение знаменателей несократимых дробей из Q_1. Ясно, что Q_1 порождается числами $\frac{\alpha}{p_i} (i \in I)$, причем α взаимно просто с каждым p_i. Пусть $\overline{a} = a + N(K)$ – ненулевой элемент из $\overline{K}$, для которого $\overline{a}^2 = \alpha \overline{a}$. Очевидно, что $a^2 \neq 0$, поэтому $\beta a^2 = \gamma a$, где β, γ – ненулевые целые числа. Тогда $\beta \overline{a}^2 = \gamma \overline{a}$, т. е. $\beta \alpha \overline{a} = \gamma \overline{a}$ и, значит, $\beta\alpha = \gamma$. Поэтому $\beta a^2 = \beta \alpha a$, откуда следует, что
$$a^2 = \alpha a. \tag{11}$$

Далее, пусть $p_i \overline{b_i} = \overline{a}$ и $\overline{b_i} = b_i + N(K) \quad (i \in I)$, тогда
$$p_i b_i = a + r_i, \tag{12}$$
где $r_i \in N(K)$. Следовательно, $p_i b_i r_i = a r_i$ и $p_i r_i b_i = r_i a$. Сложив эти равенства почленно, с учетом леммы 2.1 получим $p_1(b_1 r_1 + r_1 b_1) = a r_1 + r_1 a = \alpha r_1$. Обозначим $b_i r_i + r_i b_i = s_i$. Тогда
$$p_i s_i = \alpha r_i. \tag{13}$$
Умножим равенство (12) на α и, учитывая (13), получим $\alpha p_i b_i = \alpha a + p_i s_i$, откуда $p_i(\alpha b_i - s_i) = \alpha a$. Обозначим $\alpha b_i - s_i = t_i$. Тогда
$$p_i t_i = \alpha a. \tag{14}$$

Пусть S – подкольцо, порожденное множеством $M = \{a\} \cup \{t_i \in I\}$. Докажем, что S изоморфно некоторому подкольцу поля $\mathbb{Q}$.

Пусть c – элемент из S и $c = \sum\limits_{j=1}^{n} \mu_j c_j$, где каждое c_j – произведение элементов из M. Из равенств (11) и (14) следует, что для всякого $j \in \{1, \ldots, n\}$

найдется такое $k_j \in N$, что $k_j c_j = m_j a$, и поэтому для некоторого натурального n имеет место равенство $nc = \delta a$, причем ясно, что $\delta \neq 0$. Тогда $n^2c^2 = \delta^2 \alpha a = \delta\alpha(ca) = \delta\alpha nc$ и, значит, $nc^2 = \delta\alpha c$. Таким образом, S – кольцо без кручения, в котором каждый ненулевой элемент является корнем некоторого многочлена $\alpha_2 x^2 - \alpha_1 x$, где α_1 и α_2 – ненулевые целые числа. Поэтому S изоморфно некоторому подкольцу поля $\mathbb{Q}$. Покажем, что $K = S + N(K)$. Отметим, что, как легко видеть, Q_1 порождается множеством $\{\alpha\} \cup \left\{\frac{\alpha^2}{p_i} | i \in I\right\}$. Поэтому изоморфное ему кольцо $\overline{K}$ порождается множеством элементов $\{\overline{a}\} \cup \left\{\alpha\overline{b_i} | i \in I\right\}$. При этом $\alpha\overline{b_i} = \overline{t_i}$, так как $\alpha b_i = s_i = t_i$ и $s_i \in N(K)$. Таким образом, $\overline{K}$ порождается множеством $\{\overline{a}\} \cup \left\{\overline{t_i} | i \in I\right\}$.

Пусть теперь $k \in K$. Тогда $k = s + t$, где $s \in S = \langle M \rangle$, $t \in N(K)$. Поэтому $K = S + N(K)$. Заметим, что из равенства $S \cap N(K) = 0$ вытекает, что $\overline{K} = K/N(K) \cong S$, откуда α – наименьшее натуральное число в S. Из леммы 2.1 следует, что $ar + ra = \alpha r$ для всякого $r \in N(R)$.

Обратно, покажем, что кольцо K, удовлетворяющее условиям теоремы, будет A-кольцом. Пусть $k \in K$, где $K = S + R$. Если $k \in R$, то $k^2 = 0$. Пусть $k \notin R$. Тогда найдутся такие ненулевые целые числа β и γ, что $\gamma k = \beta a + r$, где $r \in R$. Поэтому $(\gamma k)^2 = \beta^2 a^2 + \beta(ar + ra)$. Следовательно,

$$\gamma^2 k^2 = \beta^2 \alpha a + \beta\alpha r = \beta\alpha(\beta a + r) = \beta\alpha\gamma k,$$

откуда вытекает, что $\gamma k^2 = (\alpha\beta)k$. Значит, $\langle k \rangle$ изоморфно подкольцу поля $\mathbb{Q}$, порожденному $\frac{\alpha\beta}{\gamma}$. Так как множество простых чисел, входящих в разложение знаменателей несократимых дробей моногенного подкольца в $\mathbb{Q}$, конечно, то всякое его подкольцо также моногенно. Теорема доказана.

Литература

1. Создаева Г. С., Фрейдман П. А. О локально циклических кольцах // Учен. зап. Свердл. пед. ин-та. 1969. Т. 78. С. 83–94.

2. Создаева Г. С., Фрейдман П. А. Локально циклические кольца. II // Там же. 1970. Т. 124. С. 56–73.

Статья поступила 21.02.2005 г.