Math-Net.Ru

Общероссийский математический портал

А. В. Акишин, Несовместимые преобразования колец главных идеалов, *Дискрет. матем.*, 2007, том 19, выпуск 1, 50–59

DOI: <https://doi.org/10.4213/dm7>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.81.137.203

26 апреля 2023 г., 10:40:15

Несовместимые преобразования колец главных идеалов

© 2007 г. А. В. Акишин

В работе рассматриваются вопросы о преобразованиях колец главных идеалов, несовместимых с некоторым эпиморфизмом данного кольца. Вводится понятие максимально несовместимого преобразования. Получено описание всех максимально несовместимых преобразований кольца главных идеалов A относительно гомоморфизма $A \rightarrow A/\mathfrak{m}$, где $\mathfrak{m}$ — некоторый идеал кольца A .

1. Несовместимые преобразования

1.1. Определение несовместимых преобразований

Понятие совместимого преобразования появилось в математической литературе довольно давно. Например, в монографии [3] П. Кон рассматривал отображения универсальных алгебр, совместимые с некоторой сигнатурной операцией. Совместимые преобразования колец вычетов рассматривал В. С. Анашин в работах [1, 2], посвященных исследованию преобразований колец целых p -адических чисел.

Введем понятие несовместимого преобразования. Пусть X, Y — два непустых множества. Обозначим через $F(X, Y) = \{X \rightarrow Y\}$ множество всех функций на X со значениями в Y ; положим $F(X) = F(X, X)$. Пусть $\alpha: X \rightarrow Y$ — некоторое сюръективное отображение. Через $X_y = \alpha^{-1}(y)$, $y \in Y$, обозначим множество всех прообразов элемента $y \in Y$. Отображение α определяет разбиение множества X на непересекающиеся классы, то есть задает на X отношение эквивалентности. Далее, определим

$$\Psi = \{\psi: Y \rightarrow X \mid \psi(y) \in X_y\},$$

множество функций выбора, сопоставляющих каждому элементу $y \in Y$ некоторый элемент $x_y \in X_y$. Множество $\psi(Y)$ представителей всех классов эквивалентности будем называть полной системой представителей. Отметим, что задание полной системы представителей эквивалентно заданию функции выбора.

Зафиксируем отображение $\alpha: X \rightarrow Y$. Пусть $\psi \in \Psi$. Пара отображений (α, ψ) индуцирует отображение $F(X) \rightarrow F(Y)$, сопоставляя каждой функции $f \in F(X)$ функцию $f_\psi \in F(Y)$, определяемую следующим образом:

$$f_\psi = \alpha f \psi.$$

Если для функции $\pi \in F(Y)$ существует функция выбора $\psi \in \Psi$ такая, что $f_\psi = \pi$, то мы говорим, что функция f реализует функцию π . Через

$$F_f(Y) = \{f_\psi \mid \psi \in \Psi\}$$

будем обозначать множество всех отображений множества Y в себя, реализуемых функцией $f \in F(X)$. При этом, если $\text{card } F_f(Y) = 1$, мы говорим, что функция f является совместимой с отображением α или, кратко, α -совместимой. Кроме того, будем говорить, что функции $f, g \in F(X)$ являются α -эквивалентными, если $f_\psi = g_\psi$ для любого $\psi \in \Psi$.

В данной работе рассматриваются преобразования, несовместимые с отображением α , характеризующиеся свойством $\text{card } F_f(Y) > 1$. Такие функции будем называть также α -несовместимыми. Простейшим примером такой функции является указанное А. А. Нечаевым преобразование кольца целых чисел $\mathbf{Z}$, задаваемое многочленом $(x^2 - x)/2$, которое, как легко видеть, является несовместимым с гомоморфизмом $\mathbf{Z} \rightarrow \mathbf{Z}/(2)$.

Тот факт, что структура функций, реализуемых несовместимым преобразованием f , зависит от выбора полной системы представителей, приводит к идее использовать полную систему представителей в качестве ключа криптоалгоритма. Однако перед построением реальных криптоалгоритмов необходимо знать свойства, которыми обладают несовместимые преобразования, в частности, насколько широко множество $F_f(Y)$ и какие типы функций оно содержит.

В данной работе рассматриваются полиномиальные несовместимые преобразования колец главных идеалов. Вводится понятие максимально несовместимого преобразования и определяются условия существования и общий вид таких преобразований.

Пользуясь случаем, автор выражает благодарность М. В. Ларину за помощь в выборе темы работы.

1.2. Максимально несовместимые преобразования

Если $F_f(Y) = F(Y)$, то функцию f будем называть максимально α -несовместимой; если функция f максимально α -несовместима, то при подходящем выборе полной системы представителей она реализует любое отображение $Y \rightarrow Y$.

Установим условия существования максимально несовместимых функций. Прежде всего, докажем следующую теорему.

Теорема 1. *Функция $f \in F(X)$ является максимально несовместимой с отображением $\alpha: X \rightarrow Y$ тогда и только тогда, когда для любых $i, j \in Y$ существует функция выбора ψ такая, что $f_\psi(i) = j$. Другими словами, функция f максимально α -несовместима тогда и только тогда, когда множество $F_f(Y)$ транзитивно на множестве Y .*

Доказательство. В самом деле, если функция f максимально α -несовместима, то очевидно, что функция выбора ψ с нужными свойствами существует.

Обратно, пусть условия теоремы выполнены. Положим

$$X_{ij}^f = \{x \in X_i \mid f(x) \in X_j\}.$$

Если для любых $i, j \in Y$ существует функция выбора ψ такая, что $f_\psi(i) = j$, то $f(x_i) \in X_j$ для некоторого $x_i \in X_i$. Это означает, что каждое множество X_{ij}^f непусто.

Зададим произвольное отображение $\pi: Y \rightarrow Y$ и построим функцию выбора $\varphi \in \Psi$ так, чтобы выполнялось равенство $f_\varphi = \pi$. Определение функции φ будем проводить

следующим образом: если $i \in Y$ и $\pi(i) = j$, то полагаем $\varphi(i) = x_i$, где $x_i \in X_{ij}^f$ выбираем произвольно (это всегда можно сделать в силу непустоты множества X_{ij}^f). Тогда для любого $i \in Y$

$$f_\varphi(i) = (\alpha f \varphi)(i) = (\alpha f)(x_i) = \alpha(x_j) = j,$$

то есть, действительно, $f_\varphi = \pi$.

Для выполнения равенства $F_f(Y) = F(Y)$, как легко видеть из доказательства теоремы 1, необходимо и достаточно, чтобы каждое множество X_{ij}^f было непусто. Это возможно только если $\text{card } X_i \geq \text{card } Y$ для любого $i \in Y$. Это условие является и достаточным, и имеет место следующая теорема.

Теорема 2. *Максимально α -несовместимые функции существуют тогда и только тогда, когда $\text{card } X_i \geq \text{card } Y$ для любого $i \in Y$.*

Доказательство. Необходимость указанного условия была отмечены выше. Докажем его достаточность.

Так как $\text{card } X_i \geq \text{card } Y$, для каждого $i \in Y$ можно определить сюръективное отображение $\eta_i: X_i \rightarrow Y$. Если обозначить через $X_{ij} = \eta_i^{-1}(j)$ полный прообраз элемента $j \in Y$, то окажется, что каждое множество X_{ij} непусто. Построим теперь функцию $f \in F(X)$ следующим образом: положим $f(x) = y$, где $y \in X_j$, как только $x \in X_{ij}$. Очевидно, что так определенная функция f является максимально α -несовместимой.

Пример 1. Пусть, например, $X = \mathbf{Z}$, $Y = \mathbf{Z}_p = \{0, 1, \dots, p-1\}$, где p — произвольное простое число, и пусть $\sigma: \mathbf{Z} \rightarrow \mathbf{Z}_p$ — гомоморфизм колец, так что $X_i = i + p\mathbf{Z}$. Определим функцию $f \in F(\mathbf{Z})$ равенством

$$f(x) = \frac{x(x+1)\dots(x+p-1)}{p}$$

и покажем, что $F_f(\mathbf{Z}_p) = F(\mathbf{Z}_p)$.

Рассмотрим смежный класс $a + p\mathbf{Z}$. Преобразование f запишем в виде

$$F(x) = g(x) \frac{x + p - a}{p},$$

где

$$g(x) = x(x+1)\dots(x+p-a-1)(x+p-a+1)\dots(x+p-1).$$

Очевидно, что $g(x) \equiv g(x') \pmod{p}$ для любых $x, x' \in a + p\mathbf{Z}$, при этом, $g(x) \not\equiv 0 \pmod{p}$ для любого $x \in a + p\mathbf{Z}$. Покажем, что можно выбрать элемент $x \in a + p\mathbf{Z}$ так, чтобы $f(x) \in b + p\mathbf{Z}$ для любого $b \in \mathbf{Z}_p$. Из определения функции f следует, что

$$f(kp + a) \equiv g(a) \frac{kp + a + p - a}{p} \equiv g(a)(k+1) \pmod{p}.$$

Так как $(g(a), p) = 1$, достаточно положить $k = bs(a) - 1$, где $s(a)g(a) \equiv 1 \pmod{p}$, чтобы $f(kp + a) \equiv b \pmod{p}$. Таким образом, действительно, $F_f(\mathbf{Z}_p) = F(\mathbf{Z}_p)$.

2. Максимально несовместимые многочлены

Пусть A — кольцо главных идеалов, $\mathfrak{m}$ — идеал кольца A и

$$\alpha: A \rightarrow \bar{A} = A/\mathfrak{m}$$

— гомоморфизм колец. Так как идеал $\mathfrak{m}$ полностью определяет гомоморфизм α , вместо приставки α - будем использовать приставку $\mathfrak{m}$ -. Образ элемента $a \in A$ при гомоморфизме α будем обозначать через a^α . Гомоморфизм α индуцирует гомоморфизм (который мы обозначаем той же буквой) $\alpha: A[x] \rightarrow \bar{A}[x]$. Образ многочлена $f(x) \in A[x]$ при гомоморфизме α будем обозначать через $\bar{f}(x)$.

Легко показать, что справедливо следующее утверждение.

Лемма 1. *Любой $\mathfrak{m}$ -несовместимый многочлен $F(x)$ с коэффициентами из целостного расширения B кольца A лежит в кольце $\Omega[x]$, где Ω — поле частных кольца главных идеалов A .*

2.1. Случай максимального идеала

Пусть вначале $\mathfrak{m} = \mathfrak{p}$ — максимальный идеал кольца A , так что факторкольцо $A/\mathfrak{p}$ является полем.

Произвольный многочлен $F(x) \in \Omega[x]$ можно записать в виде

$$F(x) = \frac{a}{b} f(x),$$

где $f(x) \in A[x]$ — многочлен с содержанием 1, $a, b \in A$, причем $(a, b) = 1$. Напомним, что содержанием многочлена называется наибольший общий делитель его коэффициентов.

Очевидно, что если $bA + \mathfrak{p} = A$, то многочлен $F(x)$ является $\mathfrak{p}$ -совместимым. Значит, необходимо, чтобы $b \in \mathfrak{p}$. Далее, $F(c) \in A$ для любого $c \in A$, поэтому $f(c) \in \mathfrak{p}$ для любого $c \in A$.

Выясним, какие многочлены $f(x) \in A[x]$ обладают таким свойством. Очевидно, что если $f(x) \in \mathfrak{p}[x]$, то многочлен $f(x)$ указанным свойством обладает. Покажем, что если (и только если) индекс $(A : \mathfrak{p})$ конечен, существуют и другие многочлены положительной степени с таким свойством. Для доказательства этого факта мы воспользуемся следующей очевидной теоремой.

Теорема 3. *Если многочлен $f(x) \in A[x]$ такой, что $f(b) \in \mathfrak{p}^n$ для любого $b \in a + \mathfrak{p}$, то $\bar{f}(x)$ делится на $(x - a^\alpha)^n$.*

Из этой теоремы легко выводится следующее утверждение.

Теорема 4. *Если многочлен $f(x) \in A[x]$ такой, что $f(c) \in \mathfrak{p}^n$ для любого $c \in A$, то*

$$\bar{f}(x) = \bar{g}(x) \prod_{a \in \mathfrak{p}} (x - a^\alpha)^n,$$

в частности,

$$\deg f(x) \geq n(A : \mathfrak{p}).$$

Если индекс $(A : \mathfrak{p})$ бесконечен, то таких многочленов нет.

Вернемся к изучению максимально $\mathfrak{p}$ -несовместимых многочленов. При этом будем считать, что $(A : \mathfrak{p}) = q < \infty$ и $\mathfrak{p} = \mathfrak{p}A$. Сначала докажем следующую лемму.

Лемма 2. Пусть

$$H(x) = \frac{1}{p} \prod_{i=0}^{q-1} (x - a_i) \in \Omega[x],$$

где $a_0, \dots, a_{q-1}$ — представители всех смежных классов кольца A по идеалу $\mathfrak{p}$. Тогда многочлен $H(x)$ является максимально $\mathfrak{p}$ -несовместимым.

Доказательство. Покажем, что для любых $i, j = 0, 1, \dots, q-1$, существует такой элемент $c \in A$, что

$$H(a_i + cp) \equiv a_j \pmod{\mathfrak{p}}.$$

В соответствии с теоремой 1 это как раз и означает, что многочлен $H(x)$ максимально $\mathfrak{p}$ -несовместим. Справедливо равенство

$$H(a_i + cp) = \frac{cp}{p} \prod_{k \neq i} (a_i + cp - a_k) = c \prod_{k \neq i} (a_i + cp - a_k).$$

Переходя к факторкольцу $\bar{A}$, получим, что

$$H(a_i + cp)^\alpha = c^\alpha t,$$

где

$$t = \prod_{k \neq i} (a_i + cp - a_k)^\alpha \neq 0.$$

Осталось выбрать элемент c так, чтобы $c^\alpha = a_j^\alpha t^{-1}$.

Произвольный $\mathfrak{p}$ -несовместимый многочлен $F(x)$ можно записать в виде

$$F(x) = \frac{f(x)}{mp^n},$$

где $f(x) \in A[x]$, $(m, p) = 1$ и содержание многочлена $f(x)$ не лежит в идеале $\mathfrak{p}$. Пусть $mu + p^n v = 1$. Тогда

$$F(x) = \frac{mu + p^n v}{mp^n} f(x) = \frac{uf(x)}{p^n} + \frac{vf(x)}{m}.$$

Так как $f(c) \in \mathfrak{p}^n$ для любого $c \in A$, при гомоморфизме $A \rightarrow A/\mathfrak{p}$ второе слагаемое отображается в нуль. Таким образом, можно сразу считать, что

$$F(x) = \frac{f(x)}{p^n}.$$

В соответствии с теоремой 4 $\deg f(x) \geq nq$. Разложим $f(x)$ по степеням многочлена

$$h(x) = \prod_{i=0}^{q-1} (x - a_i).$$

Пусть

$$F(x) = \frac{u_0(x)h(x)^s + u_1(x)h(x)^{s-1} + \dots + u_{s-1}(x)h(x) + u_s(x)}{p^n},$$

где $u_i(x) \in A[x]$, $i = 0, 1, \dots, s$, и $\deg u_i(x) \leq q-1$. Если здесь $s > n$, то $h(c)^s \equiv 0 \pmod{p^{n+1}}$ для любого $c \in A$. Следовательно, многочлен $F(x)$ можно заменить на p -эквивалентный ему многочлен степени (по $h(x)$) не выше n . Поэтому сразу считаем, что

$$F(x) = \frac{u_0(x)h(x)^n + u_1(x)h(x)^{n-1} + \dots + u_{n-1}(x)h(x) + u_n(x)}{p^n}.$$

Учитывая, что $h(c)^t \equiv 0 \pmod{p^t}$, $h(c)^t \not\equiv 0 \pmod{p^{t+1}}$ для любого $c \in A$, легко получить, что многочлен $F(x)$ имеет вид

$$F(x) = u_0(x)H(x)^n + u_1(x)H(x)^{n-1} + \dots + u_{n-1}(x)H(x) + u_n(x).$$

Выясним теперь, каким условиям должны удовлетворять многочлены $u_i(x)$ для того, чтобы многочлен $F(x)$ был максимально p -несовместимым.

Пусть $b_0, b_1, \dots, b_{q-1} \in a_i + p$ — такие элементы смежного класса $a_i + p$, что $H(b_j)$ лежит в смежном классе $a_j + p$. Многочлен

$$F(x) = u_0(x)H(x)^n + u_1(x)H(x)^{n-1} + \dots + u_{n-1}(x)H(x) + u_n(x)$$

является максимально p -несовместимым тогда и только тогда, когда множество $F(b_0), F(b_1), \dots, F(b_{q-1})$ содержит представители всех смежных классов кольца A по идеалу p . Отсюда следует, что для каждого a_i многочлен

$$F'(y) = u_0(a_i)y^n + u_1(a_i)y^{n-1} + \dots + u_n(a_i) \in \bar{A}[y]$$

определяет подстановку на множестве $\bar{A}$. Очевидно, что это условие является и достаточным.

Отсюда получаем следующий метод построения максимально p -несовместимых многочленов. Выберем q многочленов $F_i(y) \in \bar{A}[y]$, $0 \leq i < q$, которые определяют подстановки на множестве $\bar{A}$. Пусть

$$F_i(y) = f_{i,0}y^{q-1} + f_{i,1}y^{q-2} + \dots + f_{i,q-2}y + f_{i,q-1}.$$

Построим многочлены $u'_i(x) \in \bar{A}[x]$, положив $u'_i(c) = f_{i,i}$ для $c \in a_j + p$, $0 \leq i < q$ (это можно сделать, так как $\bar{A}$ — конечное поле). Выберем теперь многочлены $u_i(x) \in A[x]$ так, чтобы $\bar{u}_i(x) = u'_i(x)$ и положим

$$F(x) = u_0(x)H(x)^{q-1} + u_1(x)H(x)^{q-2} + \dots + u_{q-1}(x).$$

Тогда, в соответствии со сказанным выше, многочлен $F(x)$ максимально p -несовместим. Кроме того, очевидно, что любой многочлен из класса максимально p -несовместимых, можно получить таким образом.

В качестве примера применим полученные результаты в случае, когда $A = \mathbf{Z}$ — кольцо целых чисел и $p = 5\mathbf{Z}$ — максимальный идеал, порожденный простым числом 5.

Пример 2. Сначала построим максимально $5\mathbf{Z}$ -несовместимый многочлен $F(x)$ вида

$$F(x) = a_0H(x)^4 + a_1H(x)^3 + a_2H(x)^2 + a_3H(x) + a_4,$$

где $a_0, a_1, \dots, a_4$ — целые числа. Коэффициенты многочлена выбираем так, чтобы многочлен $a_0y^4 + \dots + a_4$ определял подстановку на $\mathbf{Z}_5$. В качестве такого многочлена можно взять многочлен $2y^3 + 2y^2 + 4y + 1$, который определяет подстановку $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 0 & 2 \end{pmatrix}$. Получаем многочлен

$$F_1(x) = 2H(x)^3 + 2H(x)^2 + 4H(x) + 1,$$

который является максимально $5\mathbf{Z}$ -несовместимым.

Пример 3. Построим теперь максимально $5\mathbb{Z}$ -несовместимый многочлен общего вида. Пусть

$$\begin{aligned} g_0(y) &= 3y^3 + 4, & g_1(y) &= y + 1, & g_2(y) &= 2y^3 + 2y^2 + 4y + 1, \\ g_3(y) &= y + 2, & g_4(y) &= 3y + 1 \end{aligned}$$

— многочлены, определяющие подстановки на множестве $\mathbb{Z}_5$. Строим многочлены $u_i(x)$ так, чтобы $u_i(c) = g_{c,i}$, $0 \leq c < 5$, где $g_{c,i}$ — коэффициент многочлена $g(y)$ при y^{4-i} . Получаем, что

$$\begin{aligned} u_0(x) &= 0, \\ u_1(x) &= x^3 + 2x^2 + 4x + 3, & u_2(x) &= 3x^4 + x^3 + 2x^2 + 4x, \\ u_3(x) &= x^4 + x^3 + x^2 + 3x, & u_4(x) &= x^4 + 2x^3 + x^2 + 3x + 4. \end{aligned}$$

В результате находим максимально $5\mathbb{Z}$ -несовместимый многочлен

$$\begin{aligned} F_2(x) &= (x^3 + 2x^2 + 4x + 3)H(x)^3 + (3x^4 + x^3 + 2x^2 + 4x)H(x)^2 \\ &\quad + (x^4 + x^3 + x^2 + 3x)H(x) + (x^4 + 2x^3 + x^2 + 3x + 4). \end{aligned}$$

2.2. Общий случай

Пусть снова A — кольцо главных идеалов, $\mathfrak{p}$ — его максимальный идеал и $(A : \mathfrak{p}) = q$ — конечное число. Тогда, очевидно, $\mathfrak{p}^n = p^n A$ и $(A : \mathfrak{p}^n) = q^n$.

Докажем следующую лемму.

Лемма 3. Пусть $m, n, t > n$, — натуральные числа. Тогда имеет место импликация

$$a \equiv a' \pmod{\mathfrak{p}^m} \implies H(a) \equiv H(a') \pmod{\mathfrak{p}^n}.$$

Доказательство. В самом деле, пусть $a' = a + sp^m$. Тогда

$$H(a') = H(a) + p^{m-1}g(a),$$

где $g(x) \in A[x]$ — некоторый многочлен. Отсюда сразу следует, что утверждение леммы верно.

Как следствие, получаем следующее утверждение.

Лемма 4. Пусть $m, n, t > n$, — натуральные числа. Тогда для любого $\mathfrak{p}$ -несовместимого многочлена $F(x)$ верна импликация

$$a \equiv a' \pmod{\mathfrak{p}^m} \implies F(a) \equiv F(a') \pmod{\mathfrak{p}^n}.$$

Теперь мы можем доказать следующую теорему.

Теорема 5. Максимально $\mathfrak{p}^n$ -несовместимые многочлены существуют в том и только том случае, когда $n = 1$.

Доказательство. В самом деле, рассмотрим смежный класс $a + \mathfrak{p}^n$. Для того, чтобы многочлен $H(x)$ был максимально $\mathfrak{p}^n$ -несовместимым, необходимо, чтобы среди образов $H(b)$ элементов этого смежного класса встречались представители всех смежных классов кольца A по идеалу $\mathfrak{p}^n$. Однако, очевидно, что число различных образов не более q^{n-1} . Число же смежных классов равно q^n . Таким образом, многочлен $H(x)$ не является максимально $\mathfrak{p}^n$ -несовместимым при $n > 1$.

Любой $\mathfrak{p}^n$ -несовместимый многочлен $F(x) \in \Omega[x]$ можно записать в виде

$$F(x) = a_0(x)H(x)^s + a_1(x)H(x)^{s-1} + \dots + a_s(x),$$

где $a_i(x) \in A[x]$, $s \geq 1$. Очевидно, что если $H(x)$ не является максимально $\mathfrak{p}^n$ -несовместимым, то и многочлен $F(x)$ не будет таковым. Утверждение теоремы теперь следует из того, что $H(x)$ максимально $\mathfrak{p}^n$ -несовместим, только если $n = 1$.

Пусть теперь $\mathfrak{m}$ — произвольный идеал кольца A , и пусть $\mathfrak{m} = \mathfrak{m}_1\mathfrak{m}_2$, $\mathfrak{m}_1 + \mathfrak{m}_2 = A$ — разложение идеала $\mathfrak{m}$ в произведение взаимно простых идеалов $\mathfrak{m}_1$ и $\mathfrak{m}_2$.

Произвольный $\mathfrak{m}$ -несовместимый многочлен $F(x)$ можно записать в виде

$$F(x) = \frac{f(x)}{k_1k_2},$$

где $k_1 \in \mathfrak{m}_1 = m_1A$, $k_2 \in \mathfrak{m}_2 = m_2A$ и $(k_1, k_2) = 1$. Так как m_1 и m_2 взаимно просты, пусть

$$uk_2m_2 + vk_1m_1 = 1.$$

Тогда

$$F(x) = \frac{uk_2m_2 + vk_1m_1}{k_1k_2}f(x) = m_2\frac{f'(x)}{k_1} + m_1\frac{f''(x)}{k_2} = m_2F_1(x) + m_1F_2(x).$$

Теперь мы можем доказать следующую теорему.

Теорема 6. Если многочлен $F(x) \in \Omega[x]$ является максимально $\mathfrak{m}$ -несовместимым, то $F_1(x)$ является максимально $\mathfrak{m}_1$ -несовместимым, а $F_2(x)$ — максимально $\mathfrak{m}_2$ -несовместимым.

Доказательство. Пусть $a_1, a_2, \dots, a_t$ — представители всех смежных классов кольца A по идеалу $\mathfrak{m}$. Так как $F(x)$ максимально $\mathfrak{m}$ -несовместим, по теореме 1 для любых i, j , $1 \leq i, j \leq t$, существует такой элемент $c_{ij} \in a_i + \mathfrak{m}$, что $F(c_{ij}) \in a_j + \mathfrak{m}$. Тогда

$$F(c_{ij}) = m_2F_1(c_{ij}) + m_1F_2(c_{ij}) \equiv m_2F_1(c_{ij}) \equiv a_j \pmod{\mathfrak{m}_1}.$$

Так как $\mathfrak{m}_1 + \mathfrak{m}_2 = A$, очевидно, что многочлен $F_1(x)$ максимально $\mathfrak{m}_1$ -несовместим. Аналогично, многочлен $F_2(x)$ является максимально $\mathfrak{m}_2$ -несовместимым.

Раскладывая идеал $\mathfrak{m}$ в произведение степеней максимальных идеалов

$$\mathfrak{m} = \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_s^{n_s}$$

и используя лемму 4, легко доказать следующую теорему

Теорема 7. Для любого $\mathfrak{m}$ -несовместимого многочлена $F(x)$ верна импликация

$$a \equiv a' \pmod{\mathfrak{m}^2} \implies F(a) \equiv F(a') \pmod{\mathfrak{m}}.$$

Как указано в теореме 6, для того чтобы многочлен

$$F(x) = m_2 F_1(x) + m_1 F_2(x)$$

был максимально $\mathfrak{m}$ -несовместимым, необходимо чтобы $F_1(x)$ был максимально $\mathfrak{m}_1$ -несовместимым и $F_2(x)$ был максимально $\mathfrak{m}_2$ -несовместимым. Докажем, что это условие является и достаточным и справедлива следующая теорема.

Теорема 8. *Многочлен*

$$F(x) = m_2 F_1(x) + m_1 F_2(x)$$

является максимально $\mathfrak{m}$ -несовместимым тогда и только тогда, когда $F_1(x)$ и $F_2(x)$ — соответственно максимально $\mathfrak{m}_1$ -несовместимый и $\mathfrak{m}_2$ -несовместимый многочлены.

Доказательство. Необходимость условия указана выше. Докажем его достаточность. Пусть условия теоремы выполнены. Пусть $a_1, a_2, \dots, a_t$ — представители всех смежных классов кольца A по идеалу $\mathfrak{m}$, и пусть $um_1 + vm_2 = 1$. Тогда

$$a_j = (um_1 + vm_2)a_j = (a_ju)m_1 + (a_jv)m_2.$$

Так как $F_1(x)$ максимально $\mathfrak{m}_1$ -несовместим, по теореме 1 в смежном классе $a_1 + \mathfrak{m}_1$ существует такой элемент $c' = a_1 + b_1m_1$, что

$$F_1(c') = (a_jv) + d_1m_1.$$

Аналогично, в смежном классе $a_1 + \mathfrak{m}_2$ существует такой элемент $c'' = a_1 + b_2m_2$, что

$$F_2(c'') = (a_ju) + d_2m_2.$$

Пусть $c = a_1 + km \in a_1 + \mathfrak{m}$. Используя китайскую теорему об остатках (см., например, [4]), найдем такое k , что

$$km_2 \equiv b_1 \pmod{\mathfrak{m}_1}, \quad km_1 \equiv b_2 \pmod{\mathfrak{m}_2}.$$

Тогда

$$c \equiv c' \pmod{\mathfrak{m}_1^2}, \quad c \equiv c'' \pmod{\mathfrak{m}_2^2}.$$

Отсюда

$$\begin{aligned} F_1(c) &= F_1(c') + d'_1m_1 = (a_jv) + d'_1m_1, \\ F_2(c) &= F_2(c'') + d'_2m_2 = (a_ju) + d'_2m_2. \end{aligned}$$

Тогда

$$F(c) = a_j(vm_2 + um_1) + Dm \in a_j + \mathfrak{m}.$$

Повторяя рассуждения для остальных смежных классов, легко получаем, что для любых $i, j = 1, 2, \dots, t$ существует такой элемент $c \in a_i + \mathfrak{m}$, что $F(c) \in a_j + \mathfrak{m}$. Следовательно, многочлен $F(x)$ является максимально $\mathfrak{m}$ -несовместимым.

Используя теоремы 5 и 8, легко доказать следующую теорему.

Теорема 9. Пусть $\mathfrak{m} = \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_s^{n_s}$ — разложение идеала $\mathfrak{m}$ в произведение степеней максимальных попарно взаимно простых идеалов, причем $\mathfrak{p}_i + \mathfrak{p}_j = A$ при $i \neq j$, $\mathfrak{p}_i = \mathfrak{p}_i A$. Тогда максимально $\mathfrak{m}$ -несовместимые многочлены существуют тогда и только тогда, когда $n_i = 1$ для любого $i = 1, 2, \dots, s$ и эти многочлены имеют вид

$$F(x) = u_1 F_1(x) + u_2 F_2(x) + \dots + u_s F_s(x),$$

где $u_i = p_1 \dots p_{i-1} p_{i+1} \dots p_s$ и $F_i(x)$ — максимально $\mathfrak{p}_i$ -несовместимый многочлен, $i = 1, \dots, s$.

Список литературы

1. Анашин В. С., Равномерно распределенные последовательности целых p -адических чисел. *Дискретная математика* (2004) **14**, №4, 3–64.
2. Анашин В. С., Равномерно распределенные последовательности целых p -адических чисел. *Математические заметки* (1994) **55**, №2, 3–46.
3. Кон П., *Универсальная алгебра*. Мир, Москва, 1968.
4. Ленг С., *Алгебра*. Мир, Москва, 1968.

Статья поступила 28.06.2005

Переработанный вариант поступил 12.01.2006.