Краткие сообщения по физике ФИАН *номер 3-4, 1997 г.*

УДК 530.1

О ПРИКЛАДНЫХ АСПЕКТАХ ТЕОРИИ КОЛЕЦ

Р. А. Захеди

Рассмотрены возможности использования теории колец, содержащей, в отличие от группового подхода, не одну, а две бинарных операции. Развит метод нахождения элементов конкретных колец с помощью этих операций. На примере приложения метода в теории диофантовых уравнений показана его эффективность.

Математические модели физических процессов охватывают определенные классы математических объектов и отношения между этими объектами. К наиболее общеупотребительным моделям такого рода относятся группы, кольца, поля, векторные пространства и линейные алгебры. Группа – это множество G с одной бинарной операцией (умножение) $a \cdot b = c$; $a, b, c \in G$, подчиняющейся известным условиям [1]. Группы отображают свойства симметрии физических объектов.

Кольцо представляет собой множество элементов R, где определены уже две бинарные операции – сложение и умножение. Причем по сложению это множество – группа, а умножение связано со сложением законами дистрибутивности

$$a \cdot (b + c) = a \cdot b + a \cdot c, \ (b + c) \cdot a = b \cdot a + c \cdot a, \tag{1}$$

где $a, b, c \in R$. Кольца отображают структурные свойства множества R. В отличие от групповых моделей модели, связанные с кольцами, не получили сколько-нибудь значительного распространения, хотя в физике широко используются различные алгебры матриц, алгебры гиперкомплексных чисел, алгебры Грассмана, Клиффорда и др. Это в значительной мере обусловлено сложностью нахождения взаимосвязи бинарных соотношений сложения и умножения с элементами кольца.

Настоящая работа посвящена развитию достаточно простого метода установления такой взаимосвязи и анализу на этой основе конкретных задач. Представим систему бинарных соотношений кольца в виде

$$\begin{cases} f(M) \oplus f(N) = f(M \oplus N) \oplus h_1(M,N), \\ f(M) \otimes f(N) = f(M \otimes N) \oplus h_2(M,N), \end{cases} \tag{2}$$

где f, h_1, h_2 – функции: $f : D_f \to R$, $h_1 : D_f^2 \to R$, $h_2 : D_f^2 \to R$; $(D_f, \oplus\otimes)$ и $(R, \oplus\otimes)$ – коммутативные кольца с единицей и кольца, коммутативные относительно сложения.

Принципиальный момент предлагаемой формы записи заключается в разделении стандартных бинарных соотношений, характерных для полей действительных, комплексных и некоторых других чисел и функций h_1 и h_2, связанных со спецификой конкретных множеств.

Перейдем к исследованию системы (2). При наложении определенных условий (свойства коммутативности, ассоциативности и дистрибутивности) имеем

$$\begin{gathered} \forall M, N \in D_f : \{f(0) = h_1(M,0),\ f(M) \oplus f(-M) = f(0) \oplus h_1(M,-M), \\ f(M) \oplus f(N) = f(N) \oplus f(M) \Rightarrow [h_1(M,N) = h_1(N,M)],\ f(M) \oplus \\ \oplus [f(N) \oplus f(P)] = [f(M) \oplus f(N)] \oplus f(P) \Rightarrow \\ \Rightarrow [h_1(M, N \oplus P) \oplus h_1(N,P) = h_1(M,N) \oplus h_1(M \oplus N, P)]\}, \end{gathered} \tag{3}$$

$$\begin{gathered} \forall M, N, P \in D_f : \{f(M) \otimes f(N) = f(N) \otimes f(M) \Rightarrow \\ \Rightarrow [h_2(M,N) = h_2(N,M)],\ f(M) \otimes [f(N) \otimes f(P)] = \\ = [f(M) \otimes f(N)] \otimes f(P) \Rightarrow h_2(M, N \otimes P) \oplus [f(M) \otimes \\ \otimes h_2(N,P)] = h_2(M \otimes N, P) \oplus [f(P) \otimes h_2(M,N)]\}, \end{gathered} \tag{4}$$

$$\begin{gathered} \forall M, N, P \in D_f : \{f(M) \otimes [f(N) \oplus f(P)] = \\ = [f(M) \otimes f(N)] \oplus [f(M) \otimes f(P)] \Rightarrow f(M) \otimes f(N \oplus P) \oplus \\ \oplus [f(M) \otimes h_1(N,P)] = f(M \otimes N) \oplus h_2(M,N) \oplus f(M \otimes P) \oplus \\ \oplus h_2(M,P) \Rightarrow f(M \otimes N) \oplus f(M \otimes P) \oplus [-h_1(M \otimes N, M \otimes P)] \oplus \\ \oplus h_2(M, N \oplus P) \oplus [f(M) \otimes h_1(N,P)] = f(M \otimes N) \oplus h_2(M,N) \oplus \\ \oplus f(M \otimes P) \oplus h_2(M,P)\} \Rightarrow \end{gathered}$$

$$f(M)\otimes h_1(N,P)=h_2(M,N)\oplus h_2(M,P)\oplus[-h_2(M,N\oplus P)]\oplus$$
$$\oplus h_1(M\otimes N,M\otimes P)\}. \tag{5}$$

(Если предположим, что $h_1(N,P)\otimes h_1^{-1}(N,P)=1$, $h_1(N,P)\neq 0$, тогда из (1) следует

$$\{f(M)=[h_2(M,N)\oplus h_2(M,P)\oplus[-h_2(M,N\oplus P)]\oplus$$
$$\oplus h_1(M\otimes N,M\otimes P)]\otimes h_1^{-1}(N,P)\}). \tag{6}$$

Таким образом, получаем решение для функции $f(M)$, т.е. находим выражение элементов кольца через специфические, задаваемые нами, функции h_1 и h_2. И, с другой стороны, кольцевых свойств h_1, h_2, т.е. формул (3) – (5), достаточно для того, чтобы показать соответствие решения (6) системе (2).

Для функций h_1 и h_2 кроме кольцевых свойств имеют место некоторые свойства симметрии

$$\forall M,N,\exists M_1,N_1,M_2,N_2: h_1(M,N)=h_1(M_1N_1),\ h_2(M,N)=h_2(M_2N_2),$$
$$\exists P_1,Q_1,\exists P_2,Q_2: h_1(P_1,Q_1)=h_2(P_2,Q_2)\ \text{и т.п.} \tag{7}$$

Пусть для некоторых аргументов h_1 и h_2 задаются некоторые значения – аналоги начальных условий. Будем называть соотношения типа

$$\forall M_1,...,M_s,\ \exists N_1,...,N_s,\ \forall P_1,...,P_r,\ \exists Q_1,...,Q_r:$$
$$\sum_s f(M_s)=\sum_s f(N_s),\ \prod_r f(P_r)=\prod_r f(Q_r), \tag{8}$$

получаемые только с помощью кольцевых и симметрических свойств функций h_1 и h_2 (т.е. без обращения к значениям h_1 и h_2), симметрическими свойствами функции f, и обозначим их $[c,c]_f$[1].

Приведем конкретный пример. Система (2) при $f: Z_k^2\to Z_k$, где Z_k – кольца целых элементов поля K и $h_1(m,n;k,l)=-2(mk+nl)$, $h_2(m,n;k,l)=-2(\alpha+1)mnkl+n^2l^2(1-$

---

[1] В общем случае формулы (7) и (8) можно обобщить: $\forall M_1,...,M_s,N_1,...,N_t,\ \exists M_1',...,M_r',N_1',...,N_u'$: $H_i[h_1(M_1),...,h_1(M_s),h_1(M_1'),...,h_1(M_r'),h_2(N_1),...,h_2(N_t),h_2(N_1'),...,h_2(N_u')] = 0$, $\forall R_1,...,R_k$, $\exists R_1',...,R_1'\ :\ F_i[f(R_1),...,f(R_k),f(R_1'),...,f(R_1')]=0$, где H_i, F_i – функции, которые только строятся как композиции кольцевых операций, и $\forall i: Fi(0)=Hi(0)=0$.

$\alpha^2 k^2$), имеет вид

$$\left\{\begin{array}{r} f(m,n)+f(k,l)=f(m+k,n+l)+h_1(m,n;k,l), \\ f(m,n)\times f(k,l)=f(mk+\alpha nl,ml+nk)+h_2(m,n;k,l). \end{array}\right. \tag{9}$$

Используя соотношение (6), получим решение $f(m,n)=m^2+n^2$.

Из свойств функций h_1 и h_2, т.е. $\forall m,n;k,l:\ f(0,0)=0,\ f(1,0)=1$,

$$h_1(m,n;k,l)=h_1(\pm k,n;\pm m,l)=h_1(m,\pm l;k,\pm n),$$

$$h_2(m,n;k,l)=h_2(\pm k,n;\pm m,l)=h_2(m,\pm l;k,\pm n), \tag{10}$$

при $\alpha=1:\ h_2(m,n;k,l)=h_1(mk,ml;nl,nk)$, и системы (9) непосредственно следует $[c,c]_f$:

$$f(m,n)=f(n,m)=f(-m,n), f(m,n)+f(k,l)=f(k,n)+f(m,l),$$

$$f(m,n)\times f(k,l)=f(n,m)\times f(l,k),\ \text{и т.д.} \tag{11}$$

Общая схема применения метода состоит в следующем. В системе (2) рассмотрим функциональные уравнения

$$\exists M,N:\ f(M)=f(N). \tag{12}$$

Сначала будем ограничивать все алгебраические операции, применяя кольцевые и симметрические свойства данной системы (т.е. абстрактно используя только формулы (3) – (8) без прямого обращения к значениям функций h_1, h_2 или f) для того, чтобы получить достаточные условия для решения уравнения (12). Затем приведем точные решения.

Рассмотрим некоторые примеры. В системе (9) исследуем уравнение

$$f(a,b)=f(c,o), \tag{13}$$

(которое при обычном написании имеет вид $a^2+b^2=c^2$). Используя $[c,c]_f$, получим

$$\forall m,n;k,l: f(m,n)\times f(k,l)=f(mk,ml)+f(nl,nk) \tag{14}$$

$$\Rightarrow f(m,n)\times f(a,b)=f(ma,mb)+f(nb,na)=f(mc,nc). \tag{15}$$

Из уравнения (15) вытекает: $f(na,ma)+f(mb,-nb)=f(cm,cn)$ и, следовательно,

$$f(na+mb,ma-nb)+h_1(na,ma;+mb,-nb)=f(mc,nc). \tag{16}$$

Сопоставляя уравнение (16) с симметрическим соотношением $f(m,n)=f(n,m)=f(-m,n)$, имеем

$$f(na+mb,ma-nb)=f(mc,nc)\Rightarrow\{na+mb=cm,\ ma-nb=cn\}. \tag{17}$$

Из системы линейных уравнений (17) следует $a^2 + b^2 = c^2$, $a(m^2 + n^2) = c(2mn)$, $b(m^2 + n^2) = c(m^2 + n^2)$. Таким образом, решение уравнения (13) имеет вид

$$a = 2mn,\ b = m^2 - n^2,\ c = m^2 + n^2. \tag{18}$$

Как известно [4], (18) является общим решением уравнения (13). Аналогично, для решения уравнения

$$f(a, b) = f(c, d) \tag{19}$$

в системе (9) при функции $f(m, n) = m^2 + n^2$ (т.е. уравнения $a^2 + b^2 = c^2 + d^2$) имеем следующие выражения:

$$f(m, n) \times f(a, b) = f(m, n) \times f(c, d),\ f(k, l) \times f(a, b) = f(k, l) \times f(c, d). \tag{20}$$

Используя $[c, c]_f$ в качестве одного из вариантов, имеем

$$\begin{gathered} f(am + bn, an - bm) + f(ao + bp, ap - bo) = \\ = f(cm + dn, -cn + dm) + f(co - dp, cp - do) \\ \Rightarrow \{am + bn = cm + dn, an - bm = \\ = -cn + dm, ao + bp = co - dp, ap - bo = cp - do\}, \end{gathered} \tag{21}$$

откуда следует

$$\{a^2 + b^2 = c^2 + d^2, a = mo - pn, b = on + mp, c = mo + ph, d = on - mp\}; \tag{22}$$

(22) является общим решением [4].

Система (9) при $h_1(m, n, k, l) = -2(2m^3k + 2mk^3 + 3m^2k^2 + 2n^3l + 2nl^3 + 3n^2l^2$ и $h_2(m, n, k, l) = (1 - \alpha^4)n^4l^4 - 2mnkl(2m^2k^2\alpha + 2\alpha^3n^2l^2 + 2m^2l^2 + 2n^2k^2 + 3\alpha^2mnkl + 3mnkl)$ имеет решение $f(m, n) = m^4 + n^4$. Используя $[c, c]_f$, удовлетворяющее (11), имеем уравнения

$$\begin{gathered} f(mk, ml) + f(\alpha nl, nk) = f(nk, mk) + f(\alpha nl, -ml) \Rightarrow \\ \Rightarrow f(mk + \alpha nl, ml + nk) = f(nk + \alpha nl, mk - ml) \\ h_1(mk, ml; \alpha nl, nk) = h_1(nk, mk; \alpha nl, -ml). \end{gathered} \tag{23}$$

Из них следует частное решение для уравнения

$$f(a, b) = f(c, d),$$

т.е. $a^4 + b^4 = c^4 + d^4$ (см. [3]):

$$f(m^7 + m^5n^2 - 2m^3n^4 + 3m^2n^5 + mn^6, m^6n - 3m^5n^2 - 2m^4n^3 + m^2n^5 + n^7) =$$

$$= f(m^7 + m^5n^2 - 2m^3n^4 - 3m^2n^5 + mn^6, m^6n + 3m^5n^2 - 2m^4n^3 + m^2n^5 + n^7). \tag{24}$$

Аналогичным путем для уравнения $f(a,b) = f(c,d)$ при функции $f(m,n) = m^3 - n^2$ из уравнения $f(mk + \alpha nl, ml + nk) = f(mk - \alpha nl, ml - nk)$ легко получить решение (ср. [3])

$$\forall h,k,l,m : \{a = (2l)^2km(1+h), b = (2l)^3l + (2l)^2k^2m^3h(h^2+3),$$

$$c = (2l)^2km(1-h), d = k(2l)^3l - (2l)^2k^2m^3h(h^2+3)\}. \tag{25}$$

Для уравнения $f(a,b) = f(c,d)$ с функцией $f(m,n) = m^3 + n^3$ аналогично (19) можно получить

$$\forall m_1, n_1; m_2, n_2; m_3, n_3; m_4, n_4; m_5, 0 :$$

$$f(am_1 + bm_1, am_2 + bn_2) + f(am_3 + bm_5, am_4 + bm_2) + f(am_5 + bm_3, an_1 + bn_1) +$$

$$+ f(an_2 + bm_4, an_3 + bn_3) + f(an_4 + bn_4, 0) = f(cn_1 + dn_1, cm_2 + dm_1) + \tag{26}$$

$$+ f(cm_4 + dm_2, cn_3 + dn_4) + f(cn_2 + dm_4, cm_2 + dn_2) +$$

$$+ f(cn_4 + dn_3, cm_3 + dm_3) + f(cm_5 + dm_5, 0).$$

Из (26) также следует система линейных уравнений, из которой получаем общее решение для $a^3 + b^3 = c^3 + d^3$ (ср. [4]): $a = n_1n_2 - m_1^2$, $b = m_1^2 - n_1m_2$, $c = m_1n_2 - n_1^2$, $d = n_1^2 - n_1m_2$ при условиях $m_2^2 + n_2m_2 + n_2^2 = 3m_1n_1$, $m_4 = -(m_2 + n_2)$, $n_4 = -2m_1$, $m_5 = -2n_1$, $n_3 = m_1$, $m_3 = n_1$.

Как видно из приведенных примеров для колец Z_k, в отличие от других методов, мы получаем возможность сведения решения нелинейных диофантовых уравнений к решению некоторых линейных уравнений, которые с помощью кольцевых операций точно решаются. Здесь мы имеем своеобразную аналогию с обратной задачей теории рассеяния, позволяющей свести нелинейные дифференциальные уравнения к системе линейных [5]. Таким образом, предлагаемый подход позволяет сформулировать систематический способ исследования ряда функциональных уравнений в конкретных кольцах (в частности, колец целых элементов).

В заключение выражаю благодарность профессорам В. Я. Файнбергу и Л. А. Шелепину за помощь при подготовке статьи.

ЛИТЕРАТУРА

[1] Любарский Г. Я. Применение теории групп в физике. М., Гостехиздат, 1957.
[2] Уизем Дж. Линейные и нелинейные волны. М., Мир, 1977.
[3] Захеди Р. А. Препринты ФИАН N 31 и N 36, М., 1996.
[4] Dickson L. E. History of the Theory of Numbers, **2, 3**, New York, 1966.
[5] Боревич З. И., Шафаревич И. Р. Теория чисел. М., Наука, 1985.

Поступила в редакцию 14 февраля 1997 г.