4. Пылин, В.В. Генерация параметров асимметричной криптосистемы на эллиптических кривых [Текст] /В.В Пылин; //Новые информационные технологии в научных исследованиях и в образовании (НИТ-2006): тезисы докладов XI Всерос. науч.-техн. конф. студентов, молодых ученых и специалистов, Фед. агентство по образованию, науки и молодеж. политики, Адм. Рязан. обл., Рязан. гос. радиотехн., университет. Рязань: Рязан. гос. радиотехн. университет, 2006, С. 149–150.
5. Пылин, В.В. Условия эффективной реализации алгоритма Чуфа для расчета числа точек эллиптической кривой над конечным полем [Текст] / В.В. Пылин; Труды международных научно-технических конференций «Интеллектуальные системы» (AIS'06) и «Интеллектуальные САПР» (CAD–2006): в 3 т., М.: Физматлит, 2006, Т.2, С. 163–167.
6. Dewaghe, L. Remarks on the Schoof–Elkies–Atkin algorithm [Текст] / Dewaghe. L; Mathematics of Computation, 1998, Vol. 67(223), P. 1247–1252.
7. Shanks, D. Class number, a theory of factorization and genera [Текст] / Shanks. D.; Proc. Symp. Pure Math, 1971, Vol.20, P. 415–440.
8. Csirik, J. A. An exposition of the SEA algorithm, preprint [Текст] / Csirik. J. A; t, 2000
9. Mueller, V. On the generation of Cryptographically Strong Elliptic Curves [Текст] /Mueller, V. //Technical Report, Technical University of Darmstadt, 1997.

ФУНКЦИИ МОЛИНА ДЛЯ ПРЕДСТАВЛЕНИЙ ЧЕТЫРЕХМЕРНЫХ ТОЧЕЧНЫХ ГРУПП

MOLIN FUNCTIONS FOR REPRESENTATIONS OF FOUR-DIMENSIONAL POINT GROUPS

Кужукеев Ж.М.
Костанайский инженерно-экономический университет им.М.Дулатова, г.Костанай, Казахстан

Построены функции Молина для представлений 4-мерной точечной группы K_{384} и для некоторых магнитных точечных групп.

Функции Молина или производящие функции полиномиальных инвариантов для 3-мерных точечных групп приводятся в работах [1,2]. Разработана теория построения функций Молина для 3-мерных пространственных групп [3]. Непосредственное приложение к физическим проблемам прослеживается в [4,5].

Целью настоящей работы было: 1) вычислить функции Молина для представлений 4-мерной точечной группы K_{384} из списка [6]; 2) используя редукционные соотношения между представлениями группы K_{384} и ее подгруппами [7], построить функции Молина для магнитных точечных групп.

Показано, что информация, содержащаяся в них, облегчает процедуру построения целых рациональных базисов тензорных инвариантов. Так как полезность ЦРБИ для конструирования термодинамического потенциала в теории фазовых переходов несомненна, то можно надеяться на дальнейшее физическое приложение полученных результатов.

I. Степени главных инвариантов группы K_{384}

Опираясь на теорему Шевалле [8], найдем главные инварианты группы K_{384}, так как степени главных инвариантов входят составной частью в формулу функции Молина.

Теорема. Пусть G – конечная, порожденная отражениями, группа в ***n*** – мерном пространстве V над полем К характеристики нуль. Тогда К – алгебра I инвариантов группы G генерируется ***n*** алгебраически независимыми однородными элементами $I_1, I_2, \ldots, I_n$ со степенями $m_1+1, m_2+1, \ldots, m_n+1$, такими, что

$$\prod_{i=1}^{n}(m_l+1)=|G|, \tag{1}$$

где $|G|$ - порядок группы.

Числа m_i для всех групп, порожденных отражениями, затабулированы в справочнике $[9]$. Среди них можно найти и группу K_{384}. В обозначениях Коксетера она запишется $[3,3,4]$ и мы имеем $m_1=1$, $m_2=3$, $m_3=5$, $m_4=7$. Формула (1) получается из более общего выражения:

$$\prod_{i=1}^{n}(m_l\lambda+1)=\sum_{k=0}^{n}B_k\lambda^k\ , \tag{2}$$

если положить $\lambda=1$.

Коэффициент B_k есть число изометрий из групп, представимых в виде произведения k отражений. Для каждой такой изометрии существует вполне инвариантное $(n-k)$-мерное пространство, а именно пересечение kзеркал.

Например, для нашей группы имеем

$$(1+\lambda)(1+3\lambda)(1+5\lambda)(1+7\lambda)=1+16\lambda+86\lambda^2+176\lambda^3+105\lambda^4 \tag{3}$$

Таким образом, в группе K_{384}, кроме тождественного элемента, имеется 16 плоскостей отражения, 86 чистых поворотов в одной плоскости, 176 поворотов с отражениями и 105 поворотов во взаимно перпендикулярных плоскостях.

Согласно теореме, степени главных инвариантов группы K_{384} будут равны 2, 4, 6, 8.

Нетрудно выписать их явный вид:

$$\begin{aligned}
I_1 &= x^2+y^2+z^2+t^2\\
I_2 &= x^2y^2+x^2z^2+y^2z^2+(x^2+y^2+z^2)t^2\\
I_3 &= x^2y^2(z^2+t^2)+z^2t^2(x^2+y^2)\\
I_4 &= x^2y^2z^2t^2
\end{aligned} \tag{4}$$

Если исключить 4-ю размерность, т.е. положить $t=0$, то получим инварианты для трехмерной группы $m3m$.

И наконец, кольцо полиномов, инвариантное относительно преобразований группы K_{384}, имеет вид $P_0(I_1, I_2, I_3, I_4)$.

2. Функции Молина для представлений группы K_{384}

В предыдущем пункте мы нашли инвариантные базисные функции, преобразующиеся только по единичному представлению группы. Для этого представления производящая функция полиномиальных инвариантов типа P_0 имеет вид

$$P_0(t)=1/\prod_{i=1}^{n}\left(1-t^{q_i}\right)\ =1+\sum_{k=1}^{\infty}a_kt^k\ , \tag{5}$$

где q_i - степени главных инвариантов, a_k - число независимых инвариантов степени k.

В общем случае для представлений Γ_j имеем следующее выражение функции Молина

$$P_0(\Gamma_j;t)=\frac{1}{|G|}\sum_s\frac{g_s\chi(\Gamma_{s_j})}{\det(I-tA_s)}, \tag{6}$$

где q_s - число элементов в классе s, $\chi(\Gamma_{s_j})$ - характер представления Γ_j, A_s - матрица 4-го порядка векторного представления, I - матрица для тождественного элемента.

Функцию Молина можно представить в виде отношения двух конечных полиномов

$$P_0(\Gamma_j;t)=\frac{N_j(t)}{D(t)}\ , \tag{7}$$

где $N_j(t)=\sum_p k_pt^p$ нумератор, $D(t)=\prod_{i=1}^{n}\left(1-t^{q_i}\right)$- денумератор.

Необходимые данные для вычисления функции (6) можно найти в $[6,7]$.

Таким образом, для $P_0(\Gamma_1;t)$ получим выражение

$$P_0(\Gamma_1;t)=\frac{1}{384}\left[\frac{1}{(1-t^4)}+\frac{4}{(1-t)^2(1-t^2)}+\ldots+\frac{48}{1+t^4}\right]=\frac{1}{(1-t^2)(1-t^4)(1-t^6)(1-t^8)}$$

В табл. 1 даны функции Молина для всех представлений группы $К_{384}$.

Выписаны только нумераторы, так как денумератор для всех представлений будет одинаков. В табл.2 даны разложения функций Молина в степенной ряд. Коэффициенты при t^k есть числа однородных полиномов степени *k*, образующих базисные инварианты для представления Γ_j.

Таблица 1. Функции Молина для неприводимых представлений группы $К_{384}$

Представления	Функции Молина	Представления	Функции Молина
$Г_1$	1	$Г_{11}$	$t+t^3+t^5+t^7$
$Г_2$	$t^2+t^4+t^6$	$Г_{12}$	$t^3+2t^5+2t^7+2t^9+t^{11}$
$Г_3$	t^4+t^8	$Г_{13}$	$t^7+t^9+t^{11}+e^{13}$
$Г_4$	$t^6+t^8+t^{10}$	$Г_{14}$	$t^2+t^4+2t^6+t^8+t^{10}$
$Г_5$	t^{12}	$Г_{15}$	$t^4+t^6+2t^8+t^{10}+t^{12}$
$Г_6$	t^4	$Г_{16}$	$t^4+t^6+2t^8+t^{10}+t^{12}$
$Г_7$	$t^6+t^8+t^{10}$	$Г_{17}$	$t^6+t^8+2t^{10}+t^{12}+e^{14}$
$Г_8$	t^8+t^{12}	$Г_{18}$	$t^3+t^5+t^7+t^9$
$Г_9$	$t^{10}+t^{12}+t^{14}$	$Г_{19}$	$t^3+2t^5+2t^7+2t^9+t^{11}$
$Г_{10}$	t^{16}	$Г_{20}$	$t^9+t^{11}+e^{13}+e^{15}$

Таблица 2. Полиномиальный ряд инвариантов для представлений группы $К_{384}$

Представления	Полиномиальный ряд
$Г_1$	$1+t^2+2t^4+3t^6+5t^8+6t^{10}+9t^{12}+10t^{14}+\ldots$
$Г_2$	$t^2+2t^4+4t^6+6t^8+10t^{10}+14t^{12}+20t^{14}+25t^{16}+\ldots$
$Г_3$	$t^4+t^6+3t^8+4t^{10}+7t^{12}+9t^{14}+14t^{16}+16t^{18}\ldots$
$Г_4$	$t^6+2t^8+4t^{10}+6t^{12}+10t^{14}+14t^{16}+20t^{18}+25t^{20}\ldots$
$Г_5$	$t^{12}+t^{14}+2t^{16}+3t^{18}+5t^{20}+6t^{22}+9t^{24}+10t^{26}+\ldots$
$Г_6$	$t^4+t^6+2t^8+3t^{10}+5t^{12}+6t^{14}+9t^{16}+10t^{18}\ldots$
$Г_7$	$t^6+2t^8+4t^{10}+6t^{12}+10t^{14}+14t^{16}+20t^{18}+25t^{20}\ldots$
$Г_8$	$t^8+t^{10}+3t^{12}+4t^{14}+7t^{16}+9t^{18}+14t^{20}+16t^{22}\ldots$
$Г_9$	$t^{10}+2t^{12}+4t^{14}+6t^{16}+10t^{18}+14t^{20}+20t^{22}+25t^{24}\ldots$
$Г_{10}$	$t^{16}+t^{18}+2t^{20}+3t^{22}+5t^{24}+16^{26}+9t^{28}+10t^{30}\ldots$
$Г_{11}$	$t+2t^3+4t^5+7t^7+11t^9+16t^{11}+23t^{13}+30t^{15}+\ldots$
$Г_{12}$	$t^3+3t^5+6t^7+11t^9+18t^{11}+27t^{13}+39t^{15}+53t^{17}+\ldots$
$Г_{13}$	$t^7+2t^9+4t^{11}+7t^{13}+11t^{15}+16t^{17}+23t^{19}+30t^{21}+\ldots$
$Г_{14}$	$t^2+2t^4+5t^6+8t^8+14t^{10}+20t^{12}+30t^{14}+39t^{16}+\ldots$
$Г_{15}$	$t^4+2t^6+5t^8+8t^{10}+14t^{12}+20t^{14}+30t^{16}+39t^{18}\ldots$
$Г_{16}$	$t^4+2t^6+5t^8+8t^{10}+14t^{12}+20t^{14}+30t^{16}+39t^{18}\ldots$
$Г_{17}$	$t^6+2t^8+5t^{10}+8t^{12}+14t^{14}+20t^{16}+30t^{18}+39t^{20}\ldots$
$Г_{18}$	$t^3+2t^5+4t^7+7t^9+11t^{11}+16t^{13}+23t^{15}+30t^{17}+\ldots$
$Г_{19}$	$t^3+3t^5+6t^7+11t^9+18t^{11}+27t^{13}+39t^{15}+53t^{17}+\ldots$
$Г_{20}$	$t^9+2t^{11}+4t^{13}+7t^{15}+11t^{17}+16t^{19}+23t^{21}+30t^{23}+\ldots$

3. Функции Молина для магнитных групп

Пусть H – подгруппа группы G. Тогда для представления группы G можно написать редукционное соотношение

$$\Gamma_j = \sum_m c_m \Gamma_m^n , \qquad (8)$$

где c_m – кратность вхождения представления Γ_m^n подгруппы H в представление Γ_j.

В работе [7] даны таблицы редукции типа (8) в цепочке групп $K_{384} \supset M$, где M – группа магнитной симметрии.

Нетрудно построить функции Молина для групп M, пользуясь (8) и табл.1. С этой целью необходимо для представления Γ_m^n подгруппы M найти ее активные представления в группе K_{384}. Это будут те представления, которые при редукции (8) дадут Γ_m^n. Например, для представления Γ_2^+ магнитной группы $m'3m$ активными будут представления $\Gamma_4, \Gamma_5, \Gamma_6, \Gamma_7$ группы K_{384}.

Зная функции Молина для последних представлений из табл.1 получим, что функция Молина для представления Γ_2^+ будет равна сумме этих функций. В табл.3 представлены порождающие функции полиномиальных инвариантов для четырех кубических групп $m3m$, $m'3m'$, $m'3m$, $m3m'$.

Известно, что целые рациональные базисы для инвариантов содержат два типа базисных тензоров: I^q и E^p. I^q – главные инварианты – целиком определяются денумератором Молина. E^p – ковarианты представлений – определяются нумератором.

ЦРБ для данного представления Γ_j имеет вид

$$P_0(I_1; I_2; \ldots I_n) + \sum E^p(\Gamma_j; t) P_0\,(I_1; I_2; \ldots I_n),$$

где сумма распространяется на все однородные члены, определенные нумератором.

Таблица 3. Функции Молина для представлений магнитных групп

Представления	Функции Молина
а) $m'3m'$	
Γ_1^+	$1 + t^2 + t^4 + t^6 + t^{10} + t^{12} + t^{14} + t^{16}$
Γ_2^+	$t^4 + 2t^6 + 2t^8 + 2t^{10} + t^{12}$
Γ_3^+	$t^2 + 2t^4 + 3t^6 + 4t^8 + 3t^{10} + 2t^{12} + t^{14}$
Γ_4^+	$t^2 + 3t^4 + 5t^6 + 6t^8 + 5t^{10} + 3t^{12} + t^{14}$
Γ_5^+	$t^2 + 3t^4 + 5t^6 + 6t^8 + 5t^{10} + 3t^{12} + t^{14}$
Γ_1^-	$t + t^3 + t^5 + t^7 + t^9 + t^{11} + t^{13} + t^{15}$
Γ_2^-	$t^3 + t^5 + 2t^7 + 2t^9 + t^{11} + t^{13}$
Γ_3^-	$2t^3 + 4t^5 + 4t^7 + 4t^9 + 2t^{11}$
Γ_4^-	$t + 3t^3 + 5t^5 + 5t^7 + 5t^9 + 3t^{11} + t^{13} + t^{15}$
Γ_5^-	$3t^3 + 5t^5 + 6t^7 + 6t^9 + 3t^{11} + t^{13}$
б) $m3m'$	
Γ_1^+	$1 + t^2 + t^4 + t^6 + t^7 + t^9 + t^{11} + t^{13}$
Γ_2^+	$t^6 + t^8 + t^{10} + t^{12}$

Γ_3^+	$t^2+t^3+2t^4+2t^5+2t^6+2t^7+2t^8+2t^9+t^{10}+t^{11}$
Γ_4^+	$2t^3+t^4+3t^5+2t^6+3t^7+3t^8+3t^9+3t^{10}+t^{11}+2t^{12}+t^{13}$
Γ_5^+	$t^2+t^3+2t^4+2t^5+3t^6+2t^7+3t^8+3t^9+2t^{10}+2t^{11}+t^{12}+t^{13}+$
Γ_1^-	$t^4+t^6+t^8+t^9+t^{10}+t^{11}+t^{13}+t^{15}$
Γ_2^-	$t+2t^3+2t^5+2t^7+t^9+t^{10}+t^{12}+t^{14}+t^{16}$
Γ_3^-	$t^3+2t^5+t^6+3t^7+2t^8+3t^9+2t^{10}+2t^{11}+2t^{12}+t^{13}+t^{14}$
Γ_4^-	$t+2t^3+t^4+3t^5+2t^6+3t^7+3t^8+2t^9+3t^{10}+t^{11}+2t^{12}+t^{13}$
Γ_5^-	$t^2+t^3+2t^4+2t^5+3t^6+2t^7+3t^8+2t^9+2t^{10}+t^{11}+t^{12}$
в) $m'3m$	
Γ_1^+	$1+t^2+2t^4+2t^6+t^8+t^{10}$
Γ_2^+	$t^6+t^8+t^{10}+t^{12}$
Γ_3^+	$t^2+2t^4+3t^6+4t^8+3t^{10}+2t^{12}+t^{14}$
Γ_4^+	$2t^4+4t^6+6t^8+6t^{10}+4t^{12}+4t^{14}$
Γ_5^+	$2t^2+4t^4+6t^6+6t^8+4t^{10}+4t^{14}$
Γ_1^-	$t^7+2t^9+2t^{11}+2t^{13}+t^{15}$
Γ_2^-	$t+2t^3+2t^5+2t^7+t^9$
Γ_3^-	$2t^3+4t^5+4t^7+4t^9+2t^{11}$
Γ_4^-	$t+4t^3+6t^5+6t^7+5t^9+2t^{11}$
Γ_5^-	$2t^3+4t^5+5t^7+6t^9+4t^{11}+2t^{13}+t^{15}$
г) $m3m$	
Γ_1^+	$1+t+t^2+t^3+t^4+t^5+t^6+t^7$
Γ_2^+	$t^6+t^7+t^8+t^9+t^{10}+t^{11}+t^{12}+t^{13}$
Γ_3^+	$t^2+t^3+2t^4+2t^5+2t^6+2t^7+2t^8+2t^9+t^{10}+t^{11}$
Γ_4^+	$t^3+t^4+2t^5+2t^6+2t^7+3t^8+3t^9+3t^{10}+2t^{11}+2t^{12}+t^{13}+t^{14}$
Γ_5^+	$t^2+2t^3+2t^4+3t^5+3t^6+3t^7+3t^8+3t^9+2t^{10}+t^{11}+t^{12}$
Γ_1^-	$t^9+t^{10}+t^{11}+t^{12}+t^{13}+t^{14}+t^{15}+t^{16}$
Γ_2^-	$t^3+t^4+t^5+t^6+t^7+t^8+t^9+t^{10}$
Γ_3^-	$t^3+2t^5+t^6+2t^7+2t^8+2t^9+2t^{10}+t^{11}+2t^{12}+t^{14}$
Γ_4^-	$t+t^2+2t^3+3t^4+3t^5+3t^6+3t^7+3t^8+2t^9+2t^{10}+t^{11}+t^{12}$
Γ_5^-	$t^3+t^4+2t^5+2t^6+3t^7+3t^8+3t^9+3t^{10}+2t^{11}+2t^{12}+t^{13}+t^{14}$

СПИСОК ЛИТЕРАТУРЫ

1. Patera J., Sharp R.T., Winternitz P. – J.Math.Phys., 1978, 19, p.2362.
2. Desmier P.E., Sharp R.T. – J.Math.Phys., 1979, 20, p.74.
3. Jaric M.V., Birman J.L. – J.Math.Phys., 1977, 18, p.1456.
4. Jaric M.V., Birman J.L. – J.Math.Phys., 1978, 17, p.4368.
5. Kopsky V. – Chtchoslovak J. Phys., 1983, 33, p.845.

6. Brown H., Bulow R., Neubuser J. et.al. Cristallographic Groups of Four Diimensional Space., N.Y., 1978.
7. Кустов Е.Ф., Кужукеев У.М. – Теоретико-групповые методы в физике. М., Наука, 1986, с.608.
8. Chevalley C. – Amer.J.Math., 1955, 77, p.778.
9. Коксеттер Г.С.М., Мозер У.О.Дж. Порождающие элементы и определяющие соотношения дискретных групп. М. Наука, 1980.
10. Голубятников Г.Н., Лохин В.В. – ДАН СССР, 1969, 187, с.249.

ТЕРБЕЛМЕЛІ ФУНКЦИЯЛАР КЛАСЫНА ТОЛЫҚТЫРУ

TO SUPPLEMENT TO CLASSES VIBRATING FUNCTIONS

Мұстафаев А.П., Өмірбаева Ә.М.
Шәкәрім атындағы Семей мемлекеттік университеті, Семей қ.,Қазақстан

Лапласс теңдеуі мен тербелмелі функциялар математикалық физикада ерекше орынға ие екендігі белгілі. Мысалы, зарядтардан бос облыстағы электрлік өрістің потенциалы және электр тогынсыз облыстағы стационар магниттік өрістегі скаляр потенциалдар тербелмелі функциялар арқылы сипатталады. Гидродинамикада потенциалдар жылдамдығы мен қысылмайтын идеалды сұйықтың құйынсыз жазық ағыны тогының функциясы қандай да бір анықталған облыстарда тербелмелі функциялар болады.

Аналитикалық функциялардың тербелмелілігі де математикалық есептеулер мен оның қолданыс аясын кеңейтуде. Олардың арасындағы байланыстар негізінен аналитикалық функциялардың физикалық қолданыстарында жиі кездеседі.

Сондықтан біз бұл жұмысымызда комплекс айнымалы функциялар теориясын негізге ала отырып, комплекс айнымалылы функцияларды түйіндес аргумент бойынша дифференциалдау [3] ережесіне сәйкес, тербелмелі функциялардың тағы бір топтамасын анықтаймыз.

Комплекс айнымалыны:

$$\omega = f(z) = u(x,y) + iv(x,y) \tag{1}$$

функциясының диференциалын анықтау барысында

$$\frac{\partial f}{\partial z} = \frac{1}{2}\left(u_x + v_y\right) + \frac{i}{2}\left(v_x - u_y\right) \tag{2}$$

$$\frac{\partial f}{\partial \bar{z}} = \frac{1}{2}\left(u_x - vy\right) + \frac{i}{2}\left(v_x + u_y\right) \tag{3}$$

теңдігінен:

$$\frac{\partial f}{\partial \bar{z}} = 0 \tag{4}$$

өрнегін нолге теңестіру арқылы Коши-Риман шартын алдық. Осы арқылы аналитикалық функциялар негізі қаланды.

Екінші жағынан z және $\bar{z}$ айнымалылары өзара сызықты тәуелсіз айнымалылар. Дегенмен, комплекс айнымалылы функциялар теориясында z айнымалысына тәуелді функциялар толық көлемде зерттелінгенімен,

$$\omega = f(\bar{z}) \tag{1'}$$

болғанда мәлімет жоқтың қасы.

Сонымен қатар, $f(z) = \bar{z}$ болғанда, оның дифференциалданбайтындығы, ал

$$\frac{df(z)}{d\bar{z}} = 1$$

дәлелдеуді қажет етпейтіндігі белгілі.