АЛГЕБРЫ ИНВАРИАНТОВ И 14-Я ПРОБЛЕМА ГИЛЬБЕРТА

ИВАН В. АРЖАНЦЕВ

Летняя школа "Современная математика", Дубна, 19-25 июля 2007 года

Занятие 2. Инварианты конечных групп. Формулировка и история 14-й проблемы Гильберта

Пусть $\mathbb{K}$ – некоторое поле и $\mathbb{K}[x_1, \dots, x_n]$ – алгебра многочленов над полем $\mathbb{K}$. Рассмотрим линейное преобразование переменных S:

$$S(x_1) = a_{11}x_1 + \dots + a_{n1}x_n, \ \dots, \ S(x_n) = a_{1n}x_1 + \dots + a_{nn}x_n.$$

Будем считать, что преобразование S *обратимо*, т.е. существует линейное преобразование S^{-1} такое, что композиции $S \circ S^{-1}$ и $S^{-1} \circ S$ определяют тождественное преобразование. Ясно, что множество обратимых линейных преобразований переменных $x_1, \dots, x_n$ образует группу относительно операции композиции. Более того, сопоставление преобразованию S матрицы (a_{ij}) позволяет отождествить группу обратимых линейных преобразований с группой обратимых матриц $\mathrm{GL}_n(\mathbb{K})$.

Определение 1. Будем говорить, что многочлен $F(x_1, \dots, x_n)$ *инвариантен* относительно преобразования S, если $F(S(x_1), \dots, S(x_n)) = F(x_1, \dots, x_n)$.

Пример 1. Рассмотрим преобразование $S(x_1) = x_2, S(x_2) = x_3, \dots, S(x_{n-1}) = x_n, S(x_n) = x_1$. Тогда многочлен $x_1 + x_2 + \dots + x_n$ инвариантен относительно S, а $x_1 + x_2^2 + \dots + x_n^n$ – нет.

Можно также рассматривать множество обратимых линейных преобразование $C = \{S_\omega : \omega \in \Omega\}$, где Ω – некоторое множество индексов, и множество всех многочленов $\mathbb{K}[x_1, \dots, x_n]^C$, инвариантных относительно преобразований из C. Ясно, что $\mathbb{K}[x_1, \dots, x_n]^C$ содержит константы и замкнуто относительно сложения и умножения многочленов, т.е. $\mathbb{K}[x_1, \dots, x_n]^C$ – подалгебра в $\mathbb{K}[x_1, \dots, x_n]$. Более того, если G – подгруппа в $\mathrm{GL}_n(\mathbb{K})$, порожденная элементами множества C, то $\mathbb{K}[x_1, \dots, x_n]^G = \mathbb{K}[x_1, \dots, x_n]^C$. Эти наблюдения служат мотивировкой для следующей задачи.

Основная задача теории инвариантов. Пусть G – подгруппа в $\mathrm{GL}_n(\mathbb{K})$. Опишите алгебру инвариантов $\mathbb{K}[x_1, \dots, x_n]^G$.

Пример 2. Пусть $G = S_n$ – группа перестановок, действующая линейными преобразованиями переменных $x_1, \dots, x_n$ по формуле $\tau(x_i) = x_{\tau(i)}$ для каждой перестановки $\tau \in S_n$. Напомним, что многочлен $F(x_1, \dots, x_n)$ называется *симметрическим*, если $F(x_{\tau(1)}, \dots, x_{\tau(n)}) = F(x_1, \dots, x_n)$ для каждой $\tau \in S_n$, или, другими словами, $F(x_1, \dots, x_n)$ является S_n-инвариантом. Рассмотрим набор многочленов

$$\sigma_1 = x_1 + x_2 + \dots + x_n, \ \ \sigma_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n, \ \ \dots, \ \ \sigma_n = x_1x_2 \dots x_n.$$

Ясно, что эти многочлены являются симметрическими. Их называют *элементарными* симметрическими многочленами.

Основная теорема о симметрических многочленах. Для каждого симметрического многочлена $F(x_1, \dots, x_n)$ существует единственный многочлен $H(y_1, \dots, y_n)$ такой, что $F(x_1, \dots, x_n) = H(\sigma_1, \dots, \sigma_n)$.

Тем самым, алгебра $\mathbb{K}[x_1, \dots, x_n]^{S_n}$ порождается элементарными симметрическими многочленами.

Пример 3. Пусть G – группа порядка 2, состоящая из тождественного преобразования и преобразования $x_1 \to -x_1, \dots, x_n \to -x_n$. Под действием такого преобразования одночлен $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ умножается на $(-1)^{i_1+i_2+\dots+i_n}$. Поэтому многочлен $F(x_1, \dots, x_n)$ инвариантен тогда и только тогда, когда сумма показателей степеней каждого входящего в него члена четна. Это доказывает, что алгебра инвариантов порождается $x_1^2, x_2^2, \dots, x_n^2, x_1x_2, x_1x_3, \dots, x_{n-1}x_n$.

Замечание 1. В предыдущем примере мы неявно предполагали, что $-1 \neq 1$ в поле $\mathbb{K}$. Это условие выполнено не всегда. Заметим, что согласно определению поле $\mathbb{K}$ содержит элемент 1, а значит и элементы $1 + \dots + 1$. Говорят, что поле $\mathbb{K}$ имеет *нулевую характеристику*, если $1 + \dots + 1$ (n раз) не равно нулю для любого натурального n. Это условие равносильно тому, что подполе в $\mathbb{K}$, порожденное 1, можно отождествить с полем рациональных чисел. Например, поля $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ имеют нулевую характеристику. Всюду далее мы предполагаем, что $\mathbb{K}$ – поле нулевой характеристики.

Теорема 1. *Пусть $G \subset GL_n(\mathbb{K})$ – конечная подгруппа. Тогда алгебра инвариантов $\mathbb{K}[x_1, \dots, x_n]^G$ конечно порождена.*

Мы приведем два различных доказательства теоремы 1. Первое восходит к Давиду Гильберту и выводит конечную порожденность алгебры инвариантов из конечной порожденности некоторого идеала. Второе доказательство принадлежит Эмме Нетер. Оно основано на основной теореме о симметрических многочленах и доставляет эффективную оценку сверху на степени порождающих.

Доказательство 1. Рассмотрим отображение $P : \mathbb{K}[x_1, \dots, x_n] \to \mathbb{K}[x_1, \dots, x_n]$:

$$P(F(x_1, \dots, x_n)) = \frac{1}{|G|} \sum_{S \in G} F(S(x_1), \dots, S(x_n)).$$

Несложно проверить, что для любых $F, H \in \mathbb{K}[x_1, \dots, x_n]$ и $f \in \mathbb{K}[x_1, \dots, x_n]^G$ выполнены следующие свойства:

$$P(F + H) = P(F) + P(H),\ P(F) \in \mathbb{K}[x_1, \dots, x_n]^G,\ P(f) = f,\ P(fF) = fP(F).$$

В частности, P проектирует $\mathbb{K}[x_1, \dots, x_n]$ на $\mathbb{K}[x_1, \dots, x_n]^G$. В силу линейности преобразований из группы G если многочлен $f(x_1, \dots, x_n)$ инвариантен, то инвариантна и каждая его однородная компонента. Пусть I – идеал в $\mathbb{K}[x_1, \dots, x_n]$, порожденный всеми однородными инвариантами положительной степени. Как и каждый идеал в $\mathbb{K}[x_1, \dots, x_n]$, идеал I порожден конечным числом многочленов $f_1, \dots, f_s$. Эти многочлены можно считать однородными инвариантами.

Утверждается, что многочлены $f_1, \dots, f_s$ порождают алгебру инвариантов. Для этого достаточно доказать, что каждый однородный инвариант f выражается через $f_1, \dots, f_s$. Проведем индукцию по степени m инварианта f. В случае $m = 0$ многочлен f является константой и наше утверждение справедливо. При $m > 0$ многочлен f принадлежит I и значит имеет место представление $f = h_1f_1 + \dots + h_sf_s$, $h_1 \dots, h_s \in \mathbb{K}[x_1, \dots, x_n]$. Применив проектор P к обеим частям представления, получим $f = P(f) = P(h_1)f_1 + \dots + P(h_s)f_s$.

Поскольку степени f_i положительны, степени однородных инвариантов $P(h_i)$ меньше m и, по предположению индукции, $P(h_i)$ выражаются через $f_1, \dots, f_s$. Значит, и f выражается через $f_1, \dots, f_s$.

Доказательство 2. Здесь для упрощения изложения мы будем предполагать, что $\mathbb{K} = \mathbb{C}$. Нам потребуется вспомогательное

Предложение 1. *Пусть $f(x_1, \dots, x_n)$ – однородный многочлен степени m с комплексными коэффициентами. Тогда для некоторого натурального k найдутся такие линейные многочлены $L_j = \sum_{i=1}^{n} a_{ij} x_i$, $j = 1, \dots, k$, $a_{ij} \in \mathbb{C}$, что*

$$f(x_1, \dots, x_n) = L_1^m + \dots + L_k^m.$$

Доказательство. Рассмотрим случай $n = 2$. Вычисляя коэффициенты при помощи бинома Ньютона и используя определитель Вандермонда, легко показать, что многочлены $x_1^m, (x_1 + x_2)^m, \dots, (x_1 + mx_2)^m$ линейно независимы и, следовательно, образуют базис пространства однородных многочленов степени m от переменных x_1 и x_2. Это означает, что для произвольного однородного многочлена $f(x_1, x_2)$ степени m найдутся комплексные числа $\alpha_0, \dots, \alpha_m$ такие, что

$$f(x_1, x_2) = \alpha_0 x_1^m + \dots + \alpha_m (x_1 + mx_2)^m = (\beta_0 x_1)^m + \dots + (\beta_k (x_1 + mx_2))^m,$$

где $\beta_i^m = \alpha_i$.

Для $n > 2$ будем вести индукцию по n. Достаточно доказать, что любой одночлен $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ степени m представим в нужном нам виде. Можно считать, что $i_1 \geq 1$. По предположению индукции одночлен $x_2^{i_2} \dots x_n^{i_n}$ представим в виде $M_1^{m-i_1} + \dots + M_k^{m-i_1}$, где M_j — линейные многочлены от $x_2, \dots, x_n$. Остается заметить, что, вновь по предположению индукции, многочлен $x_1^{i_1} M_j^{m-i_1}$ представим в виде суммы m-х степеней линейных многочленов от x_1 и M_j. □

Пусть теперь $f(x_1, \dots, x_n) = L_1^m + \dots + L_k^m$ – указанное представление однородного инварианта f. Применяя к этому представлению отображение P, мы получаем, что f есть сумма выражений вида

$$L^{(m)}(x_1, \dots, x_n) := \frac{1}{|G|} \sum_{S \in G} L(S(x_1), \dots, S(x_n))^m,$$

где L – линейный многочлен.

Поскольку многочлен $Y_1^m + \dots + Y_s^m$ ($s = |G|$) является симметрическим многочленом от $Y_1, \dots, Y_s$, его можно выразить через элементарные симметрические многочлены от $Y_1, \dots, Y_s$. Это показывает, что $L^{(m)}(x_1, \dots, x_n)$ выражается через элементарные симметрические многочлены от $L(S(x_1), \dots, S(x_n))$, которые являются однородными инвариантами степени не выше $|G|$. Пространство многочленов от $x_1, \dots, x_n$ степени $\leq |G|$ конечномерно, и любой базис подпространства инвариантов в этом пространстве является конечной системой порождающих для $\mathbb{C}[x_1, \dots, x_n]^G$.

Следствие 1. *Пусть $G \subset GL_n(\mathbb{C})$ – конечная подгруппа. Тогда $\mathbb{C}[x_1, \dots, x_n]^G$ порождается инвариантами степени не выше $|G|$.*

Отметим, что данное следствие позволяет получить простой (но часто очень трудоемкий) алгоритм для построения конечной системы порождающих алгебры инвариантов конечной группы G: нужно взять все одночлены от $x_1, \dots, x_n$ степени $\leq |G|$ и применить к ним проектор P.

Теперь мы переходим к обсуждению основной проблемы, рассматриваемой в данном курсе.

14-я проблема Гильберта. Пусть G – подгруппа группы $\mathrm{GL}_n(\mathbb{K})$. Верно ли, что алгебра инвариантов $\mathbb{K}[x_1, \ldots, x_n]^G$ конечно порождена ?

История этой проблемы весьма драматична[1] . На Втором Международном конгрессе математиков, проходившем в августе 1900 года в Париже, Д. Гильберт поставил несколько проблем, решение которых, по его мнению, должно было определить основные направления развития математики в XX веке. В самом докладе Гильберт предложил 10 проблем, и интересующая нас проблема там не фигурировала. Однако в опубликованном тексте доклада проблем было уже 23, и проблема о конечной порожденности алгебры инвариантов имела номер 14. На самом деле, при постановке этой проблемы Гильберт ссылается на работу Маурера (L. Maurer) 1899 года, в которой конечная порожденность алгебры инвариантов была доказана для любой подгруппы $G \subset \mathrm{GL}_n(\mathbb{K})$, и ставит более общий вопрос.

- Пусть $K \subset \mathbb{K}(x_1, \ldots, x_n)$ – некоторое подполе, содержащее поле $\mathbb{K}$. Верно ли, что алгебра $\mathbb{K}[x_1, \ldots, x_n] \cap K$ является конечно порожденной ? [2]

Однако, как вскоре выяснилось, работа Маурера содержала ошибку, и с тех пор четырнадцатая проблема Гильберта рассматривается именно как проблема о конечной порожденности алгебры инвариантов. В первой половине XX века было получено несколько положительных результатов в этом направлении. (Некоторые из них мы рассматриваем в этом курсе.) Однако в 1958 г. на конгрессе в Эдинбурге М. Нагата – весьма неожиданно – привел пример группы, для которой алгебра инвариантов не допускает конечного числа порождающих, см. например [2]. Достаточно недавно Р. Стейнбергу удалось упростить аргументы Нагаты и заменить в его контрпримере тонкие соображения из алгебраической геометрии плоских кривых вполне элементарными рассуждениями [3]. Эти рассуждения мы приведем на последнем занятии.

В настоящее время 14-ю проблему естественно формулировать так: охарактеризовать те подгруппы $G \subset \mathrm{GL}_n(\mathbb{K})$, для которых алгебра инвариантов $\mathbb{K}[x_1, \ldots, x_n]^G$ конечно порождена. В такой формулировке проблема еще очень далека от окончательного решения.

Литература

[1] Д. Гильберт, Избранные труды, тома 1-2. М.: Факториал, 1998.
[2] M. Nagata, Lectures on the Fourteenth problem of Hilbert. Tata Institute, 1965.
[3] R. Steinberg, Nagata's example. In: "Algebraic Groups Lie Groups", Austral. Math. Soc. Lect. Series **9**, Cambr. University Press (1997), 375–384.

[1] Приведенные здесь сведения заимствованы из комментариев к книге [1]

[2] Вопрос о конечной порожденности алгебры инвариантов является частным случаем этого вопроса: достаточно рассмотреть в качестве подполя K подполе, состоящее из рациональных функций, инвариантных относительно действия группы G.