АЛГЕБРЫ ИНВАРИАНТОВ И 14-Я ПРОБЛЕМА ГИЛЬБЕРТА

ИВАН В. АРЖАНЦЕВ

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

Занятие 4. Контрпример Нагаты-Стейнберга

В этом разделе основное поле $\mathbb{K}$ предполагается произвольным полем нулевой характеристики. Рассмотрим векторное пространство

$$V := V_2 \oplus V_2 \oplus \cdots \oplus V_2 \qquad (9 \text{ слагаемых}),$$

где каждое V_2 есть двумерное арифметическим пространство $\mathbb{K}^2$ с координатами (x_i, y_i), $1 \le i \le 9$. Тем самым алгебра многочленов $\mathbb{K}[V]$ на пространстве V есть алгебра $\mathbb{K}[x_1, y_1, \ldots, x_9, y_9]$. Пусть $G_a = (\mathbb{K}, +)$ и группа $G_a^9 = G_a \times G_a \times \cdots \times G_a$ (9 множителей) действует на пространстве V как $x_i \to x_i + c_i y_i$, $y_i \to y_i$ для всех $(c_1, \ldots, c_9) \in G_a^9$.

Зафиксируем набор $(a_1, \ldots, a_9)$, где $a_i \in \mathbb{K}$, $a_i \ne a_j$ при $i \ne j$ и $\sum_{i=1}^9 a_i \ne 0$. Рассмотрим в G_a^9 подгруппу $G \cong G_a^6$, заданную условиями

$$\sum_{i=1}^{9} c_i = 0, \quad \sum_{i=1}^{9} a_i c_i = 0, \quad \sum_{i=1}^{9} a_i^3 c_i = 0.$$

Теорема 1. *Алгебра инвариантов $\mathbb{K}[V]^G$ не является конечно порожденной.*

Для доказательства теоремы 1 нам будет удобнее расширить группу G, тем самым уменьшив алгебру инвариантов. Пусть $H = GT$ – расширение группы G при помощи тора $T = T^8 := \{(t_1, \ldots, t_9) : t_1 t_2 \ldots t_9 = 1\}$, который действует в пространстве V по формулам $x_i \to t_i x_i$, $y_i \to t_i y_i$. Указанные действия доставляют реализации групп G и H матрицами 18×18:

$$G = \left\{ \begin{pmatrix} \begin{smallmatrix} 1 & c_1 \\ 0 & 1 \end{smallmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{smallmatrix} 1 & c_9 \\ 0 & 1 \end{smallmatrix} \end{pmatrix} \right\}, \qquad H = \left\{ \begin{pmatrix} \begin{smallmatrix} t_1 & t_1 c_1 \\ 0 & t_1 \end{smallmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{smallmatrix} t_9 & t_9 c_9 \\ 0 & t_9 \end{smallmatrix} \end{pmatrix} \right\}.$$

Теорема 2. *Алгебра инвариантов $\mathbb{K}[V]^H$ не является конечно порожденной.*

Доказательство импликации "теорема 2 $\Rightarrow$ теорема 1". Предположим, что алгебра $\mathbb{K}[V]^G$ конечно порождена. Нетрудно заметить, что действия группы G и тора T на алгебре многочленов перестановочны, откуда $t \cdot f \in \mathbb{K}[V]^G$ для любых $t \in T$ и $f \in \mathbb{K}[V]^G$. Тем самым подалгебра $\mathbb{K}[V]^G \subset \mathbb{K}[V]$ является T-инвариантной и, согласно одной из теорем предыдущего занятия, алгебра инвариантов $(\mathbb{K}[V]^G)^T = \mathbb{K}[V]^H$ конечно порождена. Это противоречит заключению теоремы 2.

Доказательство теоремы 2 мы разобьем на несколько вполне элементарных лемм. Положим $Y := y_1y_2\dots y_9$, а также

$$Z_1 := \sum_{i=1}^{9} x_iy_1\dots\hat{y_i}\dots y_9 = \sum_{i=1}^{9}\frac{x_iY}{y_i},\quad Z_2 := \sum_{i=1}^{9}\frac{a_ix_iY}{y_i},\quad Z_3 := \sum_{i=1}^{9}\frac{a_i^3x_iY}{y_i}.$$

Ясно, что $Y, Z_1, Z_2, Z_3 \in \mathbb{K}[V]$.

Лемма 1. $Y, Z_1, Z_2, Z_3 \in \mathbb{K}[V]^H$.

Доказательство. Достаточно заметить, что

$$Y \to (t_1y_1)(t_2y_2)\dots(t_9y_9) = (t_1t_2\dots t_9)(y_1y_2\dots y_9) = Y;$$

$$Z_1 \to \sum_{i=1}^{9}\frac{(t_ix_i + c_it_iy_i)Y}{t_iy_i} = \sum_{i=1}^{9}\frac{x_iY}{y_i} + (\sum_{i=1}^{9}c_i)Y = Z_1;$$

$$Z_2 \to \sum_{i=1}^{9}\frac{a_i(t_ix_i + c_it_iy_i)Y}{t_iy_i} = \sum_{i=1}^{9}\frac{a_ix_iY}{y_i} + (\sum_{i=1}^{9}a_ic_i)Y = Z_2;$$

$$Z_3 \to \sum_{i=1}^{9}\frac{a_i^3(t_ix_i + c_it_iy_i)Y}{t_iy_i} = \sum_{i=1}^{9}\frac{a_i^3x_iY}{y_i} + (\sum_{i=1}^{9}a_i^3c_i)Y = Z_3.$$

□

Лемма 2. $\mathbb{K}[V]^H = \mathbb{K}[V] \cap \mathbb{K}[Z_1, Z_2, Z_3, Y, Y^{-1}]$.

Доказательство. Группы G и H естественно действуют на алгебре $A := \mathbb{K}[x_1,\dots,x_9,y_1,\dots,y_9,Y^{-1}]$. Положим $W_i := \frac{x_iY}{y_i}$. Тогда $x_i = y_iW_iY^{-1}$, откуда

$$A = \mathbb{K}[W_1, W_2, W_3, x_4,\dots,x_9,y_1,\dots,y_9,Y^{-1}].$$

Далее, $Z_1 = \sum_{i=1}^{9} W_i$, $Z_2 = \sum_{i=1}^{9} a_iW_i$, $Z_3 = \sum_{i=1}^{9} a_i^3W_i$. Перенумеровав элементы $a_1,\dots,a_9$, можно считать, что определитель

$$\begin{vmatrix} 1 & 1 & 1\\ a_1 & a_2 & a_3\\ a_1^3 & a_2^3 & a_3^3 \end{vmatrix} = (a_2 - a_1)(a_3 - a_1)(a_3 - a_2)(a_1 + a_2 + a_3)$$

отличен от нуля. Тогда W_1, W_2 и W_3 можно выразить как линейные функции от $Z_1, Z_2, Z_3, W_4,\dots,W_9$. Это показывает, что

$$A = \mathbb{K}[Z_1, Z_2, Z_3, x_4,\dots,x_9,y_1,\dots,y_9,Y^{-1}]. \qquad (*)$$

Рассмотрим подгруппу $G_4 \subset G$, заданную условиями $c_5 = \dots = c_9 = 0$. Вновь в силу условия на определитель для любого $c_4 \in \mathbb{K}$ найдется ровно один набор (c_1, c_2, c_3) такой, что $(c_1, c_2, c_3, c_4, 0,\dots,0) \in G$. Все образующие (*) алгебры A, за исключением x_4, не изменяются под действием G_4, тогда как $x_4 \to x_4 + c_4y_4$. Это показывает, что элемент $F(Z_1, Z_2, Z_3, x_4,\dots,x_9,y_1,\dots,y_9,Y^{-1}) \in A$ является G_4-инвариантным тогда и только тогда, когда он не зависит от x_4. Рассматривая $G_5,\dots,G_9$, мы покажем, что G-инварианты не зависят также от $x_5,\dots,x_9$. С другой стороны, элементы $Z_1, Z_2, Z_3, y_1,\dots,y_9,Y^{-1}$ являются G-инвариантными, откуда $A^G = \mathbb{K}[Z_1, Z_2, Z_3, y_1,\dots,y_9,Y^{-1}]$. Элемент $(t_1,\dots,t_9) \in T$ умножает одночлен $Z_1^{a_1}Z_2^{a_2}Z_3^{a_3}y_1^{b_1}\dots y_9^{b_9}(Y^{-1})^c$ на $t_1^{b_1-c}\dots t_9^{b_9-c}$. Такой одночлен T-инвариантен в точности тогда, когда $b_1 = \dots = b_9$, откуда $A^H = \mathbb{K}[Z_1, Z_2, Z_3, Y, Y^{-1}]$. Наконец, включение $\mathbb{K}[V] \subset A$ влечет $\mathbb{K}[V]^H = \mathbb{K}[V] \cap A^H$. □

Определение 1. Пусть A – некоторая $\mathbb{K}$-алгебра. Элементы $a_1, \dots, a_s \in A$ называются *алгебраически независимыми*, если для любого ненулевого многочлена $F(X_1, \dots, X_s)$ от формальных переменных $X_1, \dots, X_s$ элемент $F(a_1, \dots, a_s) \in A$ отличен от нуля.

Лемма 3. *Элементы $Z_1, Z_2, Z_3, Y \in \mathbb{K}[V]$ алгебраически независимы.*

Доказательство. Пусть $B := K[x_1, \dots, x_9]$ – алгебра многочленов над полем рациональных дробей $K := \mathbb{K}(y_1, \dots, y_9)$. По построению элементы $x_1, \dots, x_9$ этой алгебры алгебраически независимы. Заметим, что $W_i = \frac{x_i Y}{y_i}$ отличается от x_i на константу $\frac{Y}{y_i} \in K$, откуда $W_1, W_2, W_3, x_4, \dots, x_9$ алгебраически независимы над K. Далее, поскольку наборы $\{W_1, W_2, W_3, x_4, \dots, x_9\}$ и $\{Z_1, Z_2, Z_3, x_4, \dots, x_9\}$ получаются друг из друга обратимой K-линейной заменой, элементы $Z_1, Z_2, Z_3, x_4, \dots, x_9$ (а значит и Z_1, Z_2, Z_3) алгебраически независимы над K.

Пусть теперь $F(Z_1, Z_2, Z_3, Y) = \sum_{I=(i_1,i_2,i_3)} f_I(Y) Z_1^{i_1} Z_2^{i_2} Z_3^{i_3} = 0$. Тогда $f_I(Y)$ являются нулевыми элементами поля K, и потому многочлен F – нулевой. □

Лемма 4. *Имеет место равенство*

$$\mathbb{K}[V]^H = \left\{ \sum_j \frac{f_j(Z_1, Z_2, Z_3)}{Y^{m_j}} \right\},$$

– где f_j – однородный многочлен от Z_1, Z_2, Z_3, который делится на Y^{m_j} в алгебре $\mathbb{K}[V]$.

Доказательство. По лемме 2 любой $F \in \mathbb{K}[V]^H$ имеет вид $\sum \frac{f_j(Z_1,Z_2,Z_3)}{Y^{m_j}}$, где f_j можно считать однородными степени d_j по Z_1, Z_2, Z_3. Нам нужно показать, что $f_j(Z_1, Z_2, Z_3)$ делится на Y^{m_j} в $\mathbb{K}[V]$. Можно считать, что многочлен F является однородным степени d по совокупности переменных $x_1, \dots, x_9, y_1, \dots, y_9$. Стенень выражения $\frac{f_j(Z_1,Z_2,Z_3)}{Y^{m_j}}$ по переменным $x_1, \dots, x_9$ равна d_j, а по переменным $y_1, \dots, y_9$ равна $8d_j - 9m_j$. Отсюда $d = 9(d_j - m_j)$, и значит d_j однозначно определяется по m_j и d. Следовательно, выражение $\frac{f_j(Z_1,Z_2,Z_3)}{Y^{m_j}}$ совпадает с однородной компонентной многочлена F по переменным $x_1, \dots, x_9$, и поэтому принадлежит $\mathbb{K}[V]$. □

Определение 2. Ненулевой многочлен $F(x, y)$ имеет *ноль порядка* $\geq m$ в точке (α, β), если он допускает запись

$$F(x, y) = F_m(x - \alpha, y - \beta) + F_{m+1}(x - \alpha, y - \beta) + \dots,$$

где F_k – некоторый однородный многочлен степени k от двух переменных.

Лемма 5. *Ненулевой однородный многочлен $f(Z_1, Z_2, Z_3)$ степени d от переменных Z_1, Z_2, Z_3 делится на Y^m тогда и только тогда, когда многочлен $\hat{f}(\frac{Z_2}{Z_1}, \frac{Z_3}{Z_1}) := \frac{f(Z_1,Z_2,Z_3)}{Z_1^d}$ имеет в точках $(a_1, a_1^3), \dots, (a_9, a_9^3)$ нули порядка $\geq m$.*

Доказательство. Сделаем замену переменных $Z_1' = Z_1$, $Z_2' = Z_2 - a_1 Z_1$, $Z_3' = Z_3 - a_1^3 Z_1$. После этого точка (a_1, a_1^3) переместится в начало координат. Далее, $Z_1' = x_1 \frac{Y}{y_1} + y_1 U_1$, $Z_2' = y_1 U_2$, $Z_3' = y_1 U_3$, где

$$U_1 = \frac{x_2 Y}{y_1 y_2} + \dots + \frac{x_9 Y}{y_1 y_9}, \quad U_2 = (a_2 - a_1)\frac{x_2 Y}{y_1 y_2} + \dots + (a_9 - a_1)\frac{x_9 Y}{y_1 y_9},$$

$$U_3 = (a_2^3 - a_1^3)\frac{x_2 Y}{y_1 y_2} + \dots + (a_9^3 - a_1^3)\frac{x_9 Y}{y_1 y_9}.$$

Ясно, что многочлены U_1, U_2, U_3 не зависят от y_1. В записи

$$f(Z_1', Z_2', Z_3') = f_m(Z_2', Z_3') Z_1'^{d-m} + f_{m+1}(Z_2', Z_3') Z_1'^{d-m-1} + \dots$$

все члены начиная со второго делятся на y_1^{m+1}, а первый член имеет вид $y_1^m f_m(U_2, U_3)(x_1 \frac{Y}{y_1} + y_1 U_1)^{d-m}$. Условие на определитель (см. доказательство леммы 2) влечет $K(x_2, \dots, x_9) = K(U_2, U_3, x_4, \dots, x_9)$, где $K = \mathbb{K}(y_1, \dots, y_9)$. Значит, U_2 и U_3 алгебраически независимы над K (и над $\mathbb{K}$). Поэтому условие $f_m(Z_2', Z_3') \neq 0$ влечет $f_m(U_2, U_3) \neq 0$ как многочлен от x_i и y_i. Итак, максимальная степень y_1, на которую делится $f(Z_1, Z_2, Z_3)$, равна порядку нуля многочлена $\hat{f}(\frac{Z_2}{Z_1}, \frac{Z_3}{Z_1})$ в точке (a_1, a_1^3). Рассматривая аналогично точки $(a_2, a_2^3), \dots, (a_9, a_9^3)$, получаем утверждение леммы. $\square$

Лемма 6. *Пусть ненулевой многочлен $F(x,y)$ степени $\leq 3m$ имеет нули порядка $\geq m$ в точках $(a_1, a_1^3), \dots, (a_9, a_9^3)$. Тогда $F(x,y) = \lambda(y - x^3)^m$, $\lambda \in \mathbb{K}^\times$.*

Доказательство. Будем рассуждать индукцией по m. В случае $m = 0$ многочлен $F(x,y)$ есть ненулевая константа и утверждение очевидно. При $m > 0$ рассмотрим запись

$$F(x,y) = c_0(x) y^{3m} + c_1(x) y^{3m-1} + \dots + c_{3m}(x).$$

По условию, степень многочлена $c_j(x)$ не превосходит j. Замена $y \to x^3$ приводит к многочлену $F(x, x^3) = c_0 x^{9m} + c_1(x) x^{9m-3} + \dots + c_{3m}(x)$, совпадающему с остатком от деления $F(x,y)$ на $y - x^3$. Многочлен $F(x, x^3)$ делится на $(x - a_i)^m$, поскольку выражение $(x - a_i)^k (y - a_i^3)^p$ после замены $y \to x^3$ делится на $(x - a_i)^{k+p}$. Итак, многочлен $F(x, x^3)$ делится на $(x - a_1)^m \dots (x - a_9)^m$. Сравнивая степени, получаем

$$c_0 x^{9m} + c_1(x) x^{9m-3} + \dots + c_{3m}(x) = c_0 (x - a_1)^m \dots (x - a_9)^m.$$

Коэффициент при x^{9m-1} в левой части равен нулю, тогда как в правой части он равен $-c_0 m \sum_{i=1}^9 a_i$. Отсюда следует, что $c_0 = 0$, и значит $F(x,y)$ делится на $y - x^3$. Поскольку $y - x^3$ имеет в точках (a_i, a_i^3) ноль порядка 1, мы можем применить к частному $\frac{F(x,y)}{y - x^3}$ предположение индукции и получить требуемое. $\square$

Лемма 7. *(а) Векторное пространство многочленов степени $\leq d$ от переменных x и y имеет размерность*

$$\binom{d+2}{2} = \frac{(d+2)(d+1)}{2}.$$

(б) Пусть $d \geq m$. Тогда пространство многочленов степени $\leq d$, имеющих в данной точке P ноль порядка $\geq m$, имеет размерность

$$\binom{d+2}{2} - \binom{m+1}{2}.$$

Доказательство. (а) Надо сосчитать число пар (i,j) с целыми $i, j \geq 0$, $i + j \leq d$. Для этого введем фиктивное слагаемое $k = d - i - j$. Тогда $d = i + j + k$, $i, j, k \geq 0$. Рассмотрим $d + 2$ кружочка, расположенных в ряд. Закрашивание двух из них определяет разбиение d на 3 неотрицательных слагаемых.

(б) После сдвига точки P в начало координат условие на порядок нуля задается обращением в ноль $\binom{m+1}{2}$ коэффициентов многочлена. $\square$

Лемма 8. *Пусть $d \geq 3m$. Тогда пространство многочленов $F(x,y)$ степени $\leq d$, имеющих нули порядка $\geq m$ в точках $(a_1, a_1^3), \dots, (a_9, a_9^3)$, имеет размерность*
$$\binom{d+2}{2} - 9\binom{m+1}{2}.$$

Доказательство. По предыдущей лемме размерность пространства многочленов степени $\leq 3m$ равна $\binom{3m+2}{2} = \frac{9m^2+9m+2}{2}$, тогда как $9\binom{m+1}{2} = \frac{9m^2+9m}{2}$. По лемме 6 пространство многочленов, удовлетворяющих нашим условиям на порядки нулей, одномерно. Следовательно, $9\binom{m+1}{2}$ линейных условий на $F(x,y)$ оказываются линейно независимыми. При $d > 3m$ указанные условия также линейно независимы, поскольку они линейно независимы при ограничении на подпространство многочленов степени $\leq 3m$. $\square$

Лемма 9. *Существует многочлен $F(x,y)$ степени $3m+1$, имеющий в точках $(a_1, a_1^3), \dots, (a_9, a_9^3)$ нули порядка $\geq m$ и не делящийся на $y - x^3$.*

Доказательство. Пространство многочленов степени $\leq 3m+1$, имеющих нули порядка $\geq m$ в точках (a_i, a_i^3), имеет размерность
$$\binom{3m+3}{2} - 9\binom{m+1}{2} = \frac{(3m+3)(3m+2)}{2} - 9\frac{(m+1)m}{2} = 3m+3.$$
Подпространство U многочленов, удовлетворяющих этим условиям и делящихся на $y - x^3$, имеет размерность
$$\binom{3m}{2} - 9\binom{m}{2} = \frac{3m(3m-1)}{2} - 9\frac{m(m-1)}{2} = 3m$$
(это размерность пространства многочленов степени $\leq (3m+1)-3$, имеющих в точках (a_i, a_i^3) нули порядка $\geq m-1$). Тем самым подпространство U является собственным. $\square$

Доказательство теоремы 2. Пусть алгебра $\mathbb{K}[V]^H$ конечно порождена. Лемма 4 позволяет выбрать систему образующих вида
$$S = \left\{ \frac{Z_1^2 Z_3 - Z_2^3}{Y}, \frac{f_1(Z_1, Z_2, Z_3)}{Y^{m_1}}, \dots, \frac{f_r(Z_1, Z_2, Z_3)}{Y^{m_r}} \right\},$$
где $f_j(Z_1, Z_2, Z_3)$ делится Y^{m_j} в $\mathbb{K}[V]$. Можно считать, что $f_j(Z_1, Z_2, Z_3)$ не делятся на $Z_1^2 Z_3 - Z_2^3$, иначе заменим образующую $\frac{f_j(Z_1,Z_2,Z_3)}{Y^{m_j}}$ на $\frac{f_j(Z_1,Z_2,Z_3)}{(Z_1^2 Z_3 - Z_2^3) Y^{m_j - 1}}$. Пусть d_j – это степень f_j относительно Z_1, Z_2, Z_3. Согласно леммы 6, для всех $m_j > 0$ выполнено неравенство $d_j > 3m_j$. Легко видеть, что это неравенство выполнено и при $m_j \leq 0$, поскольку мы можем считать, что S не содержит констант.

Зафиксируем число $m > \max(m_1, \dots, m_r)$. Лемма 9 обеспечивает существование многочлена $F(x,y)$ степени $3m+1$, имеющего нули порядка $\geq m$ в точках (a_i, a_i^3) и не делящегося на $y - x^3$. Пусть $f(Z_1, Z_2, Z_3) := F(\frac{Z_2}{Z_1}, \frac{Z_3}{Z_1}) Z_1^{3m+1}$. По лемме 5 выражение $\frac{f(Z_1,Z_2,Z_3)}{Y^m}$ определяет элемент алгебры $\mathbb{K}[V]^H$. Покажем, что он не выражается через элементы множества S. В самом деле, если такое выражение существует, его можно считать однородным по переменным Z_1, Z_2, Z_3 и по переменной Y (здесь используется лемма 3). Поскольку f не делится на $Z_1^2 Z_3 - Z_2^3$, в данном выражении имеется член, не включающий $\frac{Z_1^2 Z_3 - Z_2^3}{Y}$. Пусть это $\lambda \prod (\frac{f_j(Z_1,Z_2,Z_3)}{Y^{m_j}})^{e_j}$, $\lambda \in \mathbb{K}^\times$. Приравнивая степени по Z_1, Z_2, Z_3 и по Y, получаем

$$(1) \qquad \sum d_j e_j = 3m+1; \qquad (2) \qquad \sum m_j e_j = m.$$

Тогда рассмотрим (1)−3(2) и получим $\sum(d_j-3m_j)e_j=1$. Поскольку $d_j-3m_j>0$, мы заключаем, что ровно одно e_j, скажем e_{j_0}, равно 1, а прочие e_j равны нулю. Из (2) следует, что $m=m_{j_0}$, что противоречит выбору m. Полученное противоречие завершает доказательство теоремы 2.

Задачи к занятию 4

Задача 1. Пусть группа G_a^9 действует на V по формулам $x_i \to x_i + c_i y_i$, $y_i \to y_i$ для всех $(c_1,\ldots,c_9)\in G_a^9$. Докажите, что алгебра инвариантов $\mathbb{K}[x_1,y_1,\ldots,x_9,y_9]^{G_a^9}$ совпадает с подалгеброй $\mathbb{K}[y_1,\ldots,y_9]$.

Задача 2. Найдите в доказательстве теоремы 2 как можно больше мест, где существенно используется тот факт, что число точек (a_i,a_i^3) равно 9.

Задача 3. Пусть $A=\oplus_{(a,b)\in\mathbb{Z}^2}A_{(a,b)}$ — $\mathbb{Z}^2$-градуированная алгебра, удовлетворяющая следующим условиям:

- $A_{(a,b)}\neq 0 \Rightarrow a\geq 0,\ a\geq 3b$;
- $\dim A_{(3b,b)}=1$ при всех $b\geq 0$;
- $A_{(3b+1,b)}\neq A_{(3b-2,b-1)}A_{(3,1)}$ при всех $b\geq 1$.

Докажите, что алгебра A не является конечно порожденной.

Литература

[1] R. Steinberg, Nagata's example. In: "Algebraic Groups Lie Groups", Austral. Math. Soc. Lect. Series **9**, Cambr. University Press (1997), 375–384.

кафедра высшей алгебры МГУ им. М.В. Ломоносова, Ленинские Горы, Москва 119992

E-mail address: `arjantse@mccme.ru`