2 Курс, Алгебра 3
27.10.2003

Симметрические многочлены

Часть 1. Кольца инвариантов

Пусть G — конечная группа автоморфизмов k-алгебры A (то есть $g(a+b) = ga+gb$, $g(ab) = (ga)(gb)$ и $g\lambda = \lambda$ для всех $g \in G$, $\lambda \in \mathsf{k}$). Например, $A = \mathsf{k}[x_1, \ldots, x_n]$, а $G = \mathfrak{S}_n$ действует на A перестановками переменных.

Алгеброй инвариантов называется множество $A^G = \{\, a \in A \mid ga = a \ \forall g \in G \,\}$. Легко видеть, что A^G является подалгеброй в A. Заметим, что поле k содержится в алгебре инвариантов.

Лемма 1.1. *Расширение колец $A^G \subset A$ целое.*

Доказательство: для всякого $a \in A$ многочлен $f(x) = \prod_{g\in G}(x - ga) \in A[x]$ инвариантен относительно действия группы G, следовательно $f(x) \in A^G[x]$. Кроме того, старший коэффициент $f(x)$ равен 1, и $f(a) = 0$. Значит a цел над A^G. □

Лемма 1.2. *Если алгебра A конечно порождена, то A является конечно порожденным A^G-модулем.*

Доказательство: пусть $x_1, \ldots, x_n$ порождают A над k. Каждый из x_i целый над A^G, то есть $x_i^{d_i} = \sum_{j=0}^{d_i-1} b_{ij} x_i^j$, где $b_{ij} \in A^G$. Следовательно, мономы $\prod_{i=1}^n x_i^{k_i}$, $0 \leqslant k_i < d_i$ порождают A как A^G-модуль. □

Теорема 1.3. *Если алгебра A конечно порождена, то алгебра инвариантов A^G тоже конечно порождена.*

Доказательство: воспользуемся тем же рассуждением, что и при доказательстве теоремы Гильберта о нулях. Пусть $a_1, \ldots, a_n$ порождают A как k-алгебру, а $e_1, \ldots, e_l$ — порождают A как A^G-модуль. Тогда для всех $1 \leqslant i, j \leqslant n$ имеем

$$a_i = \sum_{k=1}^{l} \lambda_{ik} e_k, \qquad e_i e_j = \sum_{k=1}^{l} \mu_{ijk} e_k, \qquad \lambda_{ik}, \mu_{ijk} \in A^G.$$

Пусть $B \subset A^G$ — алгебра, порожденная над k элементами λ_{ik}, μ_{ijk}. Тогда B конечно порождена, следовательно нетерова. Из предыдущих равенств следует, что не только a_i, но и все их произведения представляются в виде линейной комбинации элементов e_i с коэффициентами в B, следовательно элементы $e_1, \ldots, e_l$ порождают A как B-модуль. Значит A — конечно порожденный B-модуль, следовательно A^G — тоже конечно порожденный B-модуль, так как $A^G \subset A$, следовательно A^G — конечно порожденная B-алгебра, следовательно A^G — конечно порожденная k-алгебра. □

В частности, алгебра инвариантов нетерова, если алгебра A конечно порождена, а группа G конечна. Можно однако показать, что алгебра инвариантов нетерова и в более общих предположениях. Всякому идеалу $I \subset A^G$ сопоставим идеал $AI \subset A$, а идеалу $J \subset A$ сопоставим идеал $J \cap A^G \subset A^G$.

Лемма 1.4. *Если порядок группы G взаимно прост с $\operatorname{char} \mathsf{k}$, то $I = AI \cap A^G$.*

Доказательство: вложение $I \subset AI \cap A^G$ очевидно. С другой стороны, всякий элемент идеала AI имеет вид $a = \sum a_k i_k$, где $a_k \in A$, $i_k \in I$. Применяя к нему оператор симметризации, получаем $\frac{1}{|G|}\sum_{g\in G} ga = \sum(\frac{1}{|G|}\sum_{g\in G} ga_k) i_k$, так как $i_k \in I \subset A^G$. Теперь, если $a \in AI \cap A^G$, то левая часть равна a, а правая лежит в $A^G I = I$, поэтому $a \in I$ и $AI \cap A^G = I$. □

Замечание 1.5. В доказательстве леммы фактически использовались не конечность группы G, а свойство полной приводимости ее представлений над полем k (оператор симметризации — это G-эквивариантный функториальный проектор на подпространство инвариантов). Группа, любое представление которой над полем k вполне приводимо, называется редуктивной (над полем k). Таким образом, предположение о взаимной простоте характеристики поля и порядка группы можно заменить на предположение о редуктивности группы G.

Следствие 1.6. *Если алгебра A нетерова, а группа G редуктивна, то алгебра инвариантов A^G нетерова.*

Доказательство: пусть $I_1 \subset I_2 \subset \cdots \subset A^G$ — возрастающая цепочка идеалов в A^G. Тогда $AI_1 \subset AI_2 \subset \cdots \subset A$ — возрастающая цепочка идеалов в A. Из нетеровости A следует, что $AI_{k+1} = AI_k$ при $k \gg 0$. Но тогда $I_{k+1} = AI_{k+1} \cap A^G = AI_k \cap A^G = I_k$, значит A^G нетерово. $\square$

Изучим теперь геометрический смысл кольца инвариантов. Пусть $A = A_X$ — координатная алгебра многооюразия $X \subset \mathbb{A}^m$. Напомним, что функтор перехода от многообразия к его координатной алгебре вполне строгий (т.е. индуцирует биекцию на множестве морфизмов), поэтому действие группы G на A задает действие группы G на X. Далее, поскольку алгебра инвариантов A^G коммутативна и конечно порождена, то она является координатной алгеброй многообразия $Y \subset \mathbb{A}^n$, а вложение алгебр $A^G \to A$ индуцирует отображение многообразий $X \to Y$. Ясно, что при этом отображении точка, соответствующая максимальному идеалу $\mathfrak{m} \subset A$ переходит в точку, соответствующую максимальному идеалу $\mathfrak{m} \cap A^G \subset A^G$.

Лемма 1.7. *Пусть $\mathfrak{m}_0 \subset A^G$ — максимальный идеал. Всякий простой идеал $\mathfrak{p} \subset A$, такой что $\mathfrak{p} \cap A^G = \mathfrak{m}_0$ максимален, а группа G действует на множестве таких идеалов транзитивно.*

Доказательство: пусть $\mathfrak{m}, \mathfrak{p} \subset A$ — максимальный и простой идеалы, такие что $\mathfrak{m} \cap A^G = \mathfrak{p} \cap A^G = \mathfrak{m}_0$ и предположим, что $\forall g \in G$ имеем $\mathfrak{m} \not\subset g\mathfrak{p}$ (в противном случае $\mathfrak{m} \subset g\mathfrak{p}$ влечет $\mathfrak{m} = g\mathfrak{p}$ так как $\mathfrak{m}$ максимален, откуда следует как максимальность идеала $\mathfrak{p}$, так и транзитивность действия группы G). Тогда, согласно приведенной ниже лемме имеем $\mathfrak{m} \not\subset \bigcup_{g\in G} g\mathfrak{p}$. Выберем $a \in \mathfrak{m}$, так что $a \notin g\mathfrak{p}$ при всех $g \in G$ и рассмотрим $b = \prod_{g\in G} ga$. Ясно, что $b \in A^G$. Кроме того, $a \in \mathfrak{m}$, значит $b \in \mathfrak{m}$, значит $b \in \mathfrak{m} \cap A^G = \mathfrak{m}_0$. С другой стороны, при всех $g \in G$ имеем $ga \notin \mathfrak{p}$ (иначе $a \in g^{-1}\mathfrak{p}$), следовательно $b \notin \mathfrak{p}$ в силу простоты $\mathfrak{p}$, что противоречит тому, что $b \in \mathfrak{m}_0 = \mathfrak{p} \cap A^G$. $\square$

Лемма 1.8. *Если $\mathfrak{a}$ — идеал, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ — простые идеалы и $\mathfrak{a} \not\subset \mathfrak{p}_i$ для всех i, то $\mathfrak{a} \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$.*

Доказательство: воспользуемся индукцией по n. Случай $n = 1$ очевиден. Предположим, что утверждение доказано для $n-1$. Тогда для всех j имеем $\mathfrak{a} \not\subset \bigcup_{i\neq j} \mathfrak{p}_i$. Выберем элементы $x_j \in \mathfrak{a}$, $x_j \notin \bigcup_{i\neq j} \mathfrak{p}_i$, то есть $x_j \notin \mathfrak{p}_i$ при $i \neq j$. Если при каком-то j имеем $x_j \notin \mathfrak{p}_j$, то $x_j \in \mathfrak{a}$ и $x_j \notin \bigcup_{i=1}^n \mathfrak{p}_i$, и утверждение доказано. Иначе имеем $x_j \in \mathfrak{p}_j$ при всех j. Положим $x = \sum_{j=1}^n \prod_{i\neq j} x_i$. Тогда $x \in \mathfrak{a}$, но каждое из слагаемых $\prod_{i\neq j} x_i$ лежит в каждом из $\mathfrak{p}_i$ при $i \neq j$ и не лежит в $\mathfrak{p}_j$ (так как $\mathfrak{p}_j$ — простой). Следовательно $x \notin \bigcup_{j=1}^n \mathfrak{p}_j$ и утверждение доказано. $\square$

Следствие 1.9. *Если $A = A_X$, где X — аффинное алгебраическое многообразие, то $A^G = A_Y$, где Y — аффинное алгебраическое многообразие, вложение $A^G \to A$ индуцирует отображение $X \to Y$, которое задает биекцию между множеством орбит действия G на X и множеством точек Y.*

Иначе говоря, многообразие Y является фактором многообразия X по действию конечной группы G и обозначается $X/\!/G$.

Часть 2. Симметрические многочлены

Рассмотрим действие группы $\mathfrak{S}_n$ на аффинном пространстве $\mathbb{A}^n$ перестановками координат. Координатной алгеброй аффинного пространства является алгебра многочленов $\mathsf{k}[x_1, \dots, x_n]$, поэтому координатной алгеброй фактора $\mathbb{A}^n /\!/ \mathfrak{S}_n$ является алгебра симметрических многочленов

$$\mathsf{k}[x_1, \dots, x_n]^{\mathfrak{S}_n} := \{\, f(x_1, \dots, x_n) \mid f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})\ \forall \sigma \in \mathfrak{S}_n \,\}.$$

Элементарными симметрическими многочленами называются многчлены

$$s_1 = x_1 + \cdots + x_n, \qquad \dots \qquad s_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \cdot \cdots \cdot x_{i_k}, \qquad \dots \qquad s_n = x_1 \cdot \cdots \cdot x_n.$$

Лемма 2.1. *Элементарные симметрические многочлены порождают алгебру $\mathsf{k}[x_1, \dots, x_n]^{\mathfrak{S}_n}$.*

Доказательство: поскольку элементарные симметрические многочлены однородны, то достаточно проверить, что всякий однородный симметрический многочлен степени d представляет как многочлен от симметрических. Воспользуемся одновременной индукцией по n и d. Основание индукции ($d = 1$) очевидно — всякий однородный симметрический многочлен степени 1 равен λs_1, $\lambda \in \mathsf{k}$. Пусть теперь $f(x_1, \dots, x_n)$ — однородный симметрический многочлен степени d. Подставляя $x_n = 0$ получаем однородный симметрический многочлен степени d от переменных $x_1, \ldots, x_{n-1}$, поэтому, по предположению индукции найдется многочлен $g(y_1, \ldots, y_{n-1})$, такой что $f(x_1, \ldots, x_{n-1}, 0) = g(s_1(x_1, \ldots, x_{n-1}, 0), \ldots, s_{n-1}(x_1, \ldots, x_{n-1}, 0))$. Рассмотрим разность $f'(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - g(s_1(x_1, \ldots, x_n), \ldots, s_{n-1}(x_1, \ldots, x_n))$. Ясно, что $f'(x_1, \ldots, x_{n-1}, 0) = 0$, поэтому f' делится на x_n. Кроме того, f' симметрический многочлен, поэтому f' также делится и на каждое из x_i, $1 \leqslant i \leqslant n$. Но все x_i попарно взаимно просты, поэтому f' делится на $s_n = x_1 \cdot \cdots \cdot x_n$, следовательно $f = g(s_1, \ldots, s_{n-1}) + s_n f''$, причем f'' — однородный симметрический многочлен меньшей степени. Остается еще раз воспользоваться предположением индукции. $\square$

Лемма 2.2. *Элементарные симметрические многочлены алгебраически независимы над* k.

Доказательство: определим $\deg' y_1^{k_1} \cdot \ldots \cdot y_n^{k_n} = \sum i k_i$. Тогда $\deg f(s_1, \ldots, s_n) = \deg' f(y_1, \ldots, y_n)$, поэтому достаточно проверить, что не существует однородного (относительно $\deg'$) многочлена $f(y_1, \ldots, y_n) \neq 0$, такого что $f(s_1, \ldots, s_n) = 0$. Воспользуемся одновременной индукцией по n и $d = \deg' f$. Основание индукции ($d = 1$) очевидно — если $\deg' f(y_1, \ldots, y_n) = 1$, то $f(y_1, \ldots, y_n) = \lambda y_1$ и $f(s_1, \ldots, s_n) = \lambda s_1$. Пусть теперь $\deg' f(y_1, \ldots, y_n) = d$, и $f(s_1, \ldots, s_n) = 0$. Положим $g(y_1, \ldots, y_{n-1}) = f(y_1, \ldots, y_{n-1}, 0)$. Тогда $g(s_1(x_1, \ldots, x_{n-1}), \ldots, s_{n-1}(x_1, \ldots, x_{n-1})) = f((x_1, \ldots, x_{n-1}, 0), \ldots, s_n(x_1, \ldots, x_{n-1}, 0)) = 0$, поэтому по предположению индукции $g = 0$. Значит, f делится на y_n, то есть $f = y_n f'$. Следовательно, $s_n f'(s_1, \ldots, s_n) = 0$ и в силу целосности кольца многочленов $f'(s_1, \ldots, s_n) = 0$. Но степень многочлена f' меньше d, значит по предположению индукции $f' = 0$, то есть $f = 0$. $\square$

Из доказанных утверждений немедленно вытекает теорема.

Теорема 2.3. *Алгебра симметрических многочленов изоморфна алгебре многочленов от n переменных.*

Доказательство: гомоморфизм алгебр $\mathsf{k}[y_1, \ldots, y_n] \to \mathsf{k}[x_1, \ldots, x_n]^{\mathfrak{S}_n}$, $y_i \mapsto s_i(x_1, \ldots, x_n)$ сюръективен по первой лемме и инъективен по второй. $\square$

Следствие 2.4. *Имеем* $\mathbb{A}^n /\!/ \mathfrak{S}_n \cong \mathbb{A}^n$.

Часть 3. Дискриминант и результант

Пусть $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_m$, $g(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$ — многочлены с коэффициентами в поле k. Рассмотрим матрицу $\mathfrak{R}$ размера $(m+n) \times (m+n)$ и ее определитель $R(f,g) = \det \mathfrak{R}$. Ясно, что $R(f,g)$ является многочленом от a_i, b_j с коэффициентами в $\mathbb{Z}$. Он называется **результантом** многчленов $f(x)$ и $g(x)$.

$$\mathfrak{R} = \begin{pmatrix} a_0 & a_1 & \ldots & a_m & & & & \\ & a_0 & a_1 & \ldots & a_m & & & \\ & & \ddots & \ddots & & \ddots & & \\ & & & a_0 & a_1 & \ldots & a_m & \\ b_0 & b_1 & \ldots & \ldots & b_n & & & \\ & b_0 & b_1 & \ldots & \ldots & b_n & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \ldots & \ldots & b_m \end{pmatrix}$$

Лемма 3.1. *Найдутся многочлены $\phi, \psi \in \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n, x]$, такие что $\phi \cdot f + \psi \cdot g = R(f,g)$.*

Доказательство: рассмотрим матрицу $\mathfrak{R}$ как матрицу с коэффициентами в кольце $\mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n, x]$, прибавим к последнему столбцу первый, умноженный на x^{m+n-1}, второй, умноженный на x^{m+n-2}, …, предпоследний, умноженный на x, и разложим определитель по последнему столбцу. $\square$

Следствие 3.2. *Если f и g имеют общий корень в* $\overline{\mathsf{k}}$, *то* $R(f,g) = 0$.

Доказательство: подставим общий корень f и g вместо x в равенство $\phi \cdot f + \psi \cdot g = R(f,g)$. $\square$

Лемма 3.3. *Если $f(x) = a_0(x - \alpha_1) \cdot \cdots \cdot (x - \alpha_m)$, $g(x) = b_0(x - \beta_1) \cdot \cdots \cdot (x - \beta_n)$, то $R(f,g) = a_0^n b_0^m \prod_{i,j=1}^n (\alpha_i - \beta_j)$.*

Доказательство: разделив первые n строк матрицы $\mathfrak{R}$ на a_0, а последние m строк — на b_0 мы своди утверждение к случаю $a_0 = b_0 = 1$. В этом случае, как левая, так и правая части являются многочленами от α_i, β_j с коэффициентами в $\mathbb{Q}$, причем левая часть делится на правую, так как при $\alpha_i = \beta_j$ имеем $R(f,g) = 0$. Кроме того, обе части однородны степени mn, поэтому частное является константой. Наконец, константа равна 1, так как член $b_n^m = ((-1)^m \prod_i \beta_i)^n$ входит в обе части с коэффициентом 1. $\square$

Теорема 3.4. *Результант обращается в ноль $\iff$ многочлены имеют общий корень.*

Дискриминантом многчлена $f(x) = a_0(x - \alpha_1) \ldots (x - \alpha_m)$ назывется $D(f) = a_0^{2n-2} \prod_{i \neq j} (\alpha_i - \alpha_j)$. Ясно, что правая часть является симметрическим многочленом от $\alpha_1, \ldots, \alpha_n$, поэтому дискриминант $D(f)$ является многочленом от коэффициентов многочлена f с целыми коэффициентами. Дискриминант обращается в ноль $\iff$ многочлен имеет кратный корень.