Глава 14

Въпрос 14: Крайни матрични групи и пръстени на техните инвариантни полиноми

За прозиволно поле k и произволно естествено число n, общата линейна група

$$GL(n,k) := \{A \in k_{n\times n} \mid \det(A) \neq 0\}$$

се състои от обратимите $n \times n$-матрици A с елементи от k. Можем да интерпретираме $A \in GL(n,k)$ като обратими k-линейни оператори $A : k_{n\times 1} \to k_{n\times}$, $x \mapsto A^{-1}x$ в пространството $k_{n\times 1}$ на наредените n-торки $x = (x_1, \ldots, x_n)^t$ с елементи $x_i \in k$.

Определение 14.1. *Под крайна матрична група G ще разбираме крайна подгрупа $G \subset GL(n,k)$.*

Примери 14.2. (Примери за крайни матрични групи) *(i) Нека $A \in GL(n,k)$ е неособена матрица с някаква естествена степен $A^M = E_n$, равна на единичната матрица E_n. Ако m е минималното естествено число със свойството $A^m = E_n$, равна на единичната матрица E_n. Ако m е минималното естествено число със свойството $A^m = E_n$, то цикличната група*

$$\langle A \rangle = \{A^i \mid 0 \leq i \leq m-1\} \subset GL(n,k)$$

е крайна матрична група от ред m.
(ii) На всяка пермутация $\sigma \in S_n$ да съпоставим матрицата $M_\sigma \in k_{n\times n}$ с елементи

$$(M_\sigma)_{ij} = \begin{cases} 1 & \text{за} \quad i = \sigma(j), \\ 0 & \text{за} \quad i \neq \sigma(j). \end{cases}$$

Тогава $M_\sigma \in GL(n,k)$, доколкото

$$\det(M_\sigma) = (-1)^{[\sigma(1),\ldots,\sigma(n)]}(M_\sigma)_{\sigma(1),1}(M_\sigma)_{\sigma(2),2}\ldots(M_\sigma)_{\sigma(n),n} = (-1)^{[\sigma(1),\ldots,\sigma(n)]} = \pm 1 \neq 0,$$

където $[\sigma(1),\ldots,\sigma(n)]$ е броят на инверсиите в пермутацията $\sigma(1),\ldots,\sigma(n)$. (Казваме, че числата $\sigma(i)$ и $\sigma(j)$ образуват инверсия, ако $i < j$ и $\sigma(i) > \sigma(j)$.) Непосредствено се пресмята, че

$$(M_\tau M_\sigma)_{ij} = \begin{cases} 1 & \text{за} \quad i = \tau\sigma(j), \\ 0 & \text{за} \quad i \neq \tau\sigma(j), \end{cases}$$

така че $M_\tau M_\sigma = M_{\tau\sigma}$ и разглежданото изображение е хомоморфизъм на групи. По този начин, взаимно-еднозначното съответствие

$$S_n \longrightarrow \mathbb{S}_n = \{M_\sigma \mid \sigma \in S_n\}$$

се оказва изоморфизъм на групи и $\mathbb{S}_n \subset GL(n,k)$ е крайна матрична група. Да отбележим, че

$$M_{\sigma^{-1}}x = M_{\sigma^{-1}} \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma(1)} \\ \ldots \\ x_{\sigma(n)} \end{pmatrix} \qquad \text{за } \forall \sigma \in S_n.$$

Да напомним, че действие на група G върху множество M е изображение

$$G \times M \longrightarrow M,$$
$$(g, m) \mapsto g^{-1}m \quad \text{за } g \in G, \quad m \in M$$

със свойствата
(i) $(gh)^{-1}m = h^{-1}(g^{-1}m)$ за $\forall g, h \in G$, $\forall m \in M$ и
(ii) $e^{-1}m = m$ за $\forall m \in M$ и неутралния елемент $e \in G$.
Да напомним, че записваме неизвестните в стълб $x = (x_1 \dots, x_n)^t$ и да означим с $\alpha_1, \dots, \alpha_n$ вектор-редовете на матрицата $A^{-1} \in GL(n, k)$. Съответствието

$$GL(n, k) \times k[x_1, \dots, x_n] \longrightarrow k[x_1, \dots, x_n],$$
$$(A, f(x)) \mapsto f(A^{-1}x) = f(\alpha_1 x, \dots, \alpha_n x).$$

изпълнява условията

$$f((AB)^{-1}x) = f(B^{-1}(A^{-1}x)) \quad \text{и}$$
$$f(E_n^{-1}x) = f(x)$$

за единечната матрица $E_n \in GL(n, k)$ и задава действие на абщата линейна група $GL(n, k)$ върху пръстена на полиномите $k[x_1, \dots, x_n]$. То се ограничава до действие на произволна крайна матрична група $G \subset GL(n, k)$ върху $k[x_1, \dots, x_n]$.

Определение 14.3. *Нека $G \subset GL(n, k)$ е крайна матрична група. Полиномът $f(x) \in k[x_1, \dots, x_n]$ се нарича G-инвариантен, ако*

$$f(x) = f(A^{-1}x) \quad \text{за} \quad \forall A \in G.$$

Множеството на G-инвариантните полиноми от $k[x_1, \dots, x_n]$ се бележи с $k[x_1, \dots, x_n]^G$.

Пример 14.4. *Да напомним, че полиномът $f \in k[x_1, \dots, x_n]$ е симетричен ако*

$$f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \quad \text{за} \quad \forall \sigma \in S_n.$$

Следователно полиномът $f(x) \in k[x_1, \dots, x_n]$ е инвариантен относно крайната матрична група $\mathbb{S}_n \subset GL(n, k)$, въведена в Пример 14.4 (ii), тогава и само тогава, когато $f(x)$ е симетричен.

Твърдение 14.5. *Нека $G \subset GL(n, k)$ е крайна матрична група. Тогава множеството $k[x_1, \dots, x_n]^G$ на G-инвариантните полиноми от $k[x_1, \dots, x_n]$ образува подпръстен на $k[x_1, \dots, x_n]$, съдържащ полето k.*

Доказателство: Достатъчно е да проверим, че за произволни $f, g \in k[x_1, \dots, x_n]^G$ е в сила $f - g, fg \in k[x_1, \dots, x_n]^G$. Наистина, за $\forall A \in G$ имаме

$$(f - g)(A^{-1}x) = f(A^{-1}x) - g(A^{-1}x) = f(x) - g(x) = (f - g)(x),$$
$$(fg)(A^{-1}x) = f(A^{-1}x)g(A^{-1}x) = f(x)g(x) = (fg)(x).$$

Следователно $k[x_1, \dots, x_n]^G$ е подпръстен на $k[x_1, \dots, x_n]$. Включването $k \subset k[x_1, \dots, x_n]^G$ следва непосредствено от

$$c(A^{-1}x) = c = c(x)$$

за произволен константен полином $c \in k$ и $A \in G \subset GL(n, k)$, Q.E.D.

Определение 14.6. *Казваме, че $f = \sum_{\mu \in M} c_\mu x^\mu \in k[x_1, \dots, x_n]$ е хомогенен полином от степен d, ако $|\mu| = \sum_{i=1}^n \mu_i = d$ за $\forall \mu \in M$ с $c_\mu \neq 0$.*

Произволен полином $f \in k[x_1, \dots, x_n]$ се представя еднозначно като сума $f = \sum_{i=1}^m f^{(d_i)}$ на хомогенни полиноми $f^{(d_i)} \in k[x_1, \dots, x_n]$ от степен d_i. Полиномите $f^{(d_i)}$ се наричат хомогенни компоненти на полинома f.

Твърдение 14.7. *Нека $G \subset GL(n,k)$ е крайна матрична група, а $f = \sum_{i=1}^{m} f^{(d_i)} \in k[x_1,\dots,x_n]$ е полином с хомогенни компоненти $f^{(d_i)} \in k[x_1,\dots,x_n]$ от степен d_i. В такъв случай, f е G-инвариантен полином тогава и само тогава, когато всички негови хомогенни компоненти $f^{(d_i)}$ са G-инвариантни.*

Доказателство: Ако всички $f^{(d_i)} \in k[x_1,\dots,x_n]^G$ са G-инвариантни, то ясно е, че тяхната сума $f = \sum_{i=1}^{m} f^{(d_i)} \in k[x_1,\dots,x_n]^G$ е G-инвариантна.
Обратно, нека $f = \sum_{\mu\in M} c_\mu x^\mu \in k[x_1,\dots,x_n]^G$ е G-инвариантен полином. Тогава за всеко $A \in G \subset GL(n,k)$ е изпълнено

$$\sum_{\mu\in M} c_\mu x^\mu = \sum_{\mu\in M} c_\mu (A^{-1}x)^\mu. \tag{14.1}$$

Ако $A^{-1} = (\alpha_{i,j})_{i,j=1}^n$, то

$$(A^{-1}x)^\mu = \left(\sum_{s=1}^{n} \alpha_{1s}x_s\right)^{\mu_1} \dots \left(\sum_{s=1}^{n} \alpha_{ns}x_s\right)^{\mu_n}$$

е хомогенен полином от степен $|\mu| = \mu_1 + \ldots + \mu_n$. Тогава хомогенните компоненти от степен d на двете страни на (14.1) са

$$f^{(d)}(x) = \sum_{|\mu|=d} c_\mu x^\mu = \sum_{|\mu|=d} c_\mu (A^{-1}x)^\mu = f^{(d)}(A^{-1}x),$$

Q.E.D.

Определение 14.8. *Елементите $A_1,\dots,A_m \in G$ пораждат крайната матрична група G, ако за всеки елемент $A \in G$ съществуват $i_1,\dots,i_l \in \{1,\dots,m\}$, така че*

$$A = A_{i_l} \dots A_{i_1}.$$

Твърдение 14.9. *Ако $A_1,\dots,A_m \in G$ пораждат крайната матрична група $G \subset GL(n,k)$, то полиномът $f \in k[x_1,\dots,x_n]$ е G-инваиантен тогава и само тогава, когато*

$$f(x) = f(A_1^{-1}x) = \ldots = f(A_m^{-1}x).$$

Доказателство: Ако $f \in k[x_1,\dots,x_n]^G$, то ясно е, че $f(x) = f(A_i^{-1}x)$ за всеки пораждащ A_i на G. С индукция по l ще докажем, че ако $f(x) = f(A_j^{-1}x)$ за $\forall 1 \le j \le m$, то $f(x) = f((A_{i_l}\dots A_{i_1})^{-1}x) = f(A_{i_1}^{-1}\dots A_{i_{l-1}}^{-1}A_{i_l}^{-1}x)$. За $l=1$ няма какво да проверяваме. Да допуснем, че $f(x) = f(A_{i_1}^{-1}\dots A_{i_{l-1}}^{-1}x)$. Тогава

$$f(A_{i_1}^{-1}\dots A_{i_{l-1}}^{-1}A_{i_l}^{-1}x) = f(A_{i_l}^{-1}x) = f(x),$$

Q.E.D.

Пример 14.10. *Множеството*

$$G_4 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \,\middle|\, a,b \in \{\pm 1\} \right\} \subset GL(2,k)$$

е крайна матрична група от ред 4, породена от елементите си

$$A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{и} \quad A_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ако полето k е с характеристика $char(k) = 0$, то пръстенът на G_4-инвариантните полиноми

$$k[x,y]^{G_4} = k[x^2,y^2]$$

съвпада с полиномите на x^2 и y^2.

Непосредствено се проверява, че множеството G_4 е затворено относно умножението и обръщането на матрици, така че G_4 е крайна матрична група. При това,

$$G_4 = \{A_1,\ A_2\, A_1 A_2,\ E_2 = A_1^2 = A_2^2\}$$

се поражда от A_1 и A_2. Съгласно Твърдение 14.9,

$$k[x,y]^{G_4} = \left\{ f \in k[x,y] \,|\, f(x,y) = f\left(A_1^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \right) = f\left(A_2^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \right) \right\}.$$

По-точно,

$$k[x,y]^{G_4} = \{f \in k[x,y] \,|\, f(x,y) = f(-x,y) = f(x,-y)\}.$$

Равенството на полиноми

$$f(-x,y) = \sum_{i,j} (-1)^i c_{i,j} x^i y^j = \sum_{i,j} c_{i,j} x^i y^j = f(x,y)$$

с коефициенти $c_{i,j}$ от поле k с $char(k) = 0$ е в сила точно когато $c_{2i+1,j} = 0$ за $\forall i \in \mathbb{Z}$, $i \geq 0$. Аналогично,

$$f(x,-y) = \sum_{i,j} (-1)^j c_{2i,j} x^{2i} y^j = \sum_{i,j} c_{2i,j} x^{2i} y^j = f(x,y)$$

тогава и само тогава, когато $c_{2i,2j+1} = 0$ за $\forall j \in \mathbb{Z}$, $j \geq 0$. Следователно G_4-инвариантните полиноми имат вида

$$f(x,y) = \sum_{i,j} c_{2i,2j} x^{2i} y^{2j} \in k[x^2,y^2],$$

така че $k[x,y]^{G_4}$ е подпръстен на $k[x^2,y^2]$. Обратно, $x^2, y^2 \in k[x,y]^{G_4}$ води до $k[x^2,y^2] \subseteq k[x,y]^{G_4}$, откъдето $k[x,y]^{G_4} = k[x^2,y^2]$.

Пример 14.11. *Над поле k с характеристика $char(k) = 0$ матричната група*

$$G_2 = \{\pm E_2\} \subset GL(2,k)$$

от ред 2 има пръстен на инвариантните полиноми

$$k[x,y]^{G_2} = k[x^2,y^2,xy].$$

Непосредствено пресмятаме, че

$$f\left((-E_2)^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \right) = f(-x,-y) = f(x,y)$$

тогава и само тогава, когато

$$\sum_{i,j} (-1)^{i+j} c_{i,j} x^i y^j = \sum_{i,j} c_{i,j} x^i y^j.$$

Последното равенство на полиноми с коефициенти от поле k с $char(k) = 0$ е изпълнено точно, когато $c_{i,j} = 0$ за $i + j = 2m + 1$. С други думи,

$$f = \sum_{i,m} c_{i,2m-i} x^i y^{2m-i} =$$

$$\sum_{i,m} c_{2i,2m-2i} x^{2i} y^{2(m-i)} + \sum_{i,m} c_{2i-1,2m-2i+1} x^{2(i-1)} y^{2(m-i)} (xy).$$

Следователно $k[x,y]^{G_2} \subseteq k[x^2,y^2,xy]$. Обратно, x^2, y^2, xy не се променят под действие на нетривиалния елемент $(x,y) \mapsto (-x,-y)$ на G_2, така че $k[x^2,y^2,xy] \subseteq k[x,y]^{G_2}$. С това установихме, че

$$k[x,y]^{G_2} = k[x^2,y^2,xy].$$