Глава 15

Въпрос 15: Оператор на Рейнолдс. Крайна породеност на пръстена от инвариантни полиноми на крайна матрична група.

Навсякъде в настоящия въпрос полето k е с характеристика $char(k) = 0$.
За произволни полиноми $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ множеството

$$k[f_1, \ldots, f_m] = \{H(f_1, \ldots, f_m) \mid H \in k[y_1, \ldots, y_m]\}$$

е затворено относно изваждане и умножение, така че представлява подпръстен на $k[x_1, \ldots, x_n]$. Казваме, че $k[f_1, \ldots, f_m]$ е подпръстенът на $k[x_1, \ldots, x_n]$, породен от $f_1, \ldots, f_m$ над k.

Определение 15.1. *За произволна крайна матрична група $G \subset GL(n, k)$, операторът на Рейнолдс*

$$R_G : k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n]$$

съпоставя на полином $f \in k[x_1, \ldots, x_n]$ полинома

$$R_G(f)(x) = \frac{1}{|G|} \sum_{A \in G} f(A^{-1}x),$$

където $|G|$ е редът на групата G, т.е. броят на елементите в G.

Изискването $char(k) = 0$ е необходимо за обратимостта на произволно естествено число $|G| \in \mathbb{N}$ в k.
За да докажем някои свойства на оператора на Рейнолдс са необходими още няколко определения.

Определение 15.2. *Непразното множество M е модул над комутативния пръстен с единица R, ако в M са определени събиране*

$$M \times M \longrightarrow M,$$

$$(x, y) \mapsto x + y \quad \text{за} \quad x, y \in M$$

и умножение

$$R \times M \longrightarrow M,$$

$$(r, x) \mapsto rx \quad \text{на } x \in M \text{ с } r \in R,$$

изпълняващи свойствата:
(i) $(x + y) + z = x + (y + z)$ *за* $\forall x, y, z \in M$;
(ii) $x + y = y + x$ *за* $\forall x, y \in M$;
(iii) $\exists 0_M$, *така че* $x + 0_M = 0_M + x = x$ *за* $\forall x \in M$;
(iv) за $\forall x \in M$ $\exists(-x) \in M$, *така че* $x + (-x) = (-x) + x = 0_M$;
(v) $(r + s)x = rx + sx$ *за* $\forall r, s \in R$, $\forall x \in M$;
(vi) $r(x + y) = rx + ry$ *за* $\forall r \in R$, $\forall x, y \in M$;
(vii) $(rs)x = r(sx) = s(rx)$ *за* $\forall r, s \in R$, $\forall x \in M$;
(viii) $1_R x = x$ *за* $\forall x \in M$.

Примери 15.3. *(i) Всеки комутативен пръстен с единица R е модул над себе си.*
(ii) Ако $G \subset GL(n,k)$ е крайна матрична група, то пръстенът $k[x_1,\dots,x_n]$ на полиномите на $x_1,\dots,x_n$ е модул над подпръстена $k[x_1,\dots,x_n]^G$ на G-инвариантните полиноми.

Определение 15.4. *Изображението $\varphi : M \to N$ е хомоморфизъм на R-модула M в R-модула N, ако*

$$\varphi\left(\sum_{i=1}^{n} r_i x_i\right) = \sum_{i=1}^{n} r_i \varphi(x_i)$$

за произволни $r_1,\dots,r_n \in R$ и $x_1,\dots,x_n \in M$.

Твърдение 15.5. *Нека $G \subset GL(n,k)$ е крайна матрична група над поле k с $char(k) = 0$, а $k[x_1,\dots,x_n]^G$ е пръстенът на G-инвариантните полиноми. Тогава операторът на Рейнолдс*

$$R_G : k[x_1,\dots,x_n] \longrightarrow k[x_1,\dots,x_n]^G$$

е хомоморфизъм на $k[x_1,\dots,x_n]^G$-модули, трансформиращ произволен хомогенен полином от степен d в хомогенен полином от степен d и оставящ на място G-инвариантните полиноми.

Доказателство: Първо ще проверим, че произволен полином $f \in k[x_1,\dots,x_n]$ се изобразява в G-инвариантен полином $R_G(f)$. За целта е достатъчно да отбележим, че за всеки елемент $B \in G$ е в сила

$$R_G(f)(B^{-1}x) = \frac{1}{|G|}\sum_{A\in G} f(A^{-1}B^{-1}x) = \frac{1}{|G|}\sum_{BA\in G} f((BA)^{-1}x) = R_G(f)(x),$$

доколкото множеството $\{BA \,|\, A \in G\}$ се състои от $|G|$ различни елемента на G и съвпада с G.
За произволни $f_1,\dots,f_m \in k[x_1,\dots,x_n]^G$ и $h_1,\dots,h_m \in k[x_1,\dots,x_n]$ пресмятаме непосредствено, че

$$R_G\left(\sum_{i=1}^{m} f_i h_i\right) = \frac{1}{|G|}\sum_{A\in G}\left(\sum_{i=1}^{m} f_i h_i\right)(A^{-1}x) =$$

$$\frac{1}{|G|}\sum_{A\in G}\sum_{i=1}^{m} f_i(A^{-1}x)h_i(A^{-1}x) = \frac{1}{|G|}\sum_{A\in G}\sum_{i=1}^{m} f_i(x)h_i(A^{-1}x).$$

Разменяйки реда на сумиране получаваме

$$R_G\left(\sum_{i=1}^{m} f_i h_i\right) = \sum_{i=1}^{m} f_i(x)\left[\frac{1}{|G|}\sum_{A\in G} h_i(A^{-1}x)\right] = \sum_{i=1}^{m} f_i(x)R_G(h_i)(x) = \sum_{i=1}^{m} f_i R_G(h_i).$$

Това доказва, че операторът на Рейнолдс $R_G : k[x_1,\dots,x_n] \to k[x_1,\dots,x_n]^G$ е хомоморфизъм на $k[x_1,\dots,x_n]^G$-модули.
Нека $f = \sum_{|\mu|=d} c_\mu x^\mu \in k[x_1,\dots,x_n]$ е хомогенен полином от степен d. Пръстенът $k[x_1,\dots,x_n]^G$ съдържа полето k, така че операторът на Рейнолдс R_G е в частност, k-линейно изображение. По този начин,

$$R_G(f) = \sum_{|\mu|=d} c_\mu R_G\left(x^\mu\right).$$

От своя страна, произволен моном x^μ от степен $|\mu| = d$ се изобразява в хомогенен полином

$$R_G(x^\mu) = \frac{1}{|G|}\sum_{A\in G}(A^{-1}x)^\mu$$

от степен d, така че $R_G(f)$ е хомогенен G-инвариантен полином от степен d. Накрая, ако $f \in k[x_1, \ldots, x_n]^G$ е G-инвариантен полином, то

$$R_G(f) = \frac{1}{|G|} \sum_{A \in G} f(A^{-1}x) = \frac{1}{|G|} \sum_{A \in G} f(x) = f(x)$$

остава на място под действие на оператора на Рейнолдс, Q.E.D.

Пример 15.6. *Нека $C_4 \subset GL(2,k)$ е цикличната матрична група от ред 4, породена от*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Тогава

$$R_{C_4}(x) = R_{C_4}(y) = 0,$$

$$R_{C_4}(x^2) = R_{C_4}(y^2) = \frac{1}{2}(x^2 + y^2),$$

$$R_{C_4}(xy) = 0,$$

$$R_{C_4}(x^3) = R_{C_4}(x^2y) = R_{C_4}(xy^2) = R_{C_4}(y^3) = 0,$$

$$R_{C_4}(x^4) = R_{C_4}(y^4) = \frac{1}{2}(x^4 + y^4),$$

$$R_{C_4}(x^3y) = -R_{C_4}(xy^3) = \frac{1}{2}(x^3y - xy^3),$$

$$R_{C_4}(x^2y^2) = x^2y^2.$$

В частност,

$$k[x^2 + y^2, x^4 + y^4, x^3y - xy^3] \subseteq k[x,y]^{C_4}.$$

За пресмятане на оператора на Рейнолдс R_{C_4} да отбележим, че $A^2 = -E_2$, $A^3 = -A$ и $A^4 = E_2 = A^0$. Следователно

$$R_{C_4}(f)(x,y) = \frac{1}{4}(f(x,y) + f(y,-x) + f(-x,-y) + f(-y,x).$$

Чрез непосредствено заместване получаваме образите на изброените мономи под действие на оператора на Рейнолдс R_{C_4}. Вземайки предвид, че $R_{C_4}(x^a y^b) \in k[x,y]^{C_4}$, получаваме, че

$$S := k[x^2 + y^2, x^4 + y^4, x^3y - xy^3, x^2y^2]$$

е подпръстен на $k[x,y]^{C_4}$. Доколкото

$$x^2y^2 = \frac{1}{2}(x^2 + y^2)^2 - \frac{1}{2}(x^4 + y^4) \in k[x^2 + y^2, x^4 + y^4],$$

имаме $S = k[x^2+y^2, x^4+y^4, x^3y-xy^3]$. От следващата Теорема 1 на Еми Ньотер следва, че $S = k[x,y]^{C_4}$.

Теорема 11. (Еми Ньотер) *Нека $G \subset GL(n,k)$ е крайна матрична група над поле k с характеристика $char(k) = 0$. Тогава пръстенът на G-инвариантните полиноми*

$$k[x_1, \ldots, x_n]^G = k[R_G(x^\beta) \mid 1 \leq |\beta| \leq |G|]$$

се поражда над k от образите $R_G(x^\beta)$ на мономите x^β от степен $1 \leq |\beta| \leq |G|$ под действие на оператора на Рейнолдс R_G.
В частност, $k[x_1, \ldots, x_n]^G$ се поражда от краен брой хомогенни G-инвариантни полиноми над k.

Доказателство: Ако $f = \sum_{\gamma \in C} c_\gamma x^\gamma \in k[x_1, \ldots, x_n]^G$, то

$$f = R_G(f) = R_G\left(\sum_{\gamma \in C} c_\gamma x^\gamma\right) = \sum_{\gamma \in C} c_\gamma R_G(x^\gamma),$$

доколкото R_G стабилизира G-инвариантните полиноми и е k-линейно изображение. Остава да докажем, че $R_G(x^\gamma) \in k[R_G(x^\alpha) \,|\, 1 \leq |\alpha| \leq |G|]$ за произволни мономи x^γ на $x_1, \ldots, x_n$.
С тази цел да отбележим, че за произволно естествено число d и променливи $z_1, \ldots, z_n$ е в сила

$$(z_1 + \ldots + z_n)^d = \sum_{|\gamma|=d} \frac{d!}{\gamma_1! \ldots \gamma_n!} z^\gamma. \tag{15.1}$$

Наистина, коефициентът $\frac{d!}{\gamma_1! \ldots \gamma_n!}$ на $z^\gamma = z_1^{\gamma_1} \ldots z_n^{\gamma_n}$ е равен на броя на начините, по които се получава z^γ от $(z_1 + \ldots + z_n)^d$. Множителят $z_1^{\gamma_1}$ се избира по $\left(\begin{array}{c} d \\ \gamma_1 \end{array} \right) = \frac{d!}{\gamma_1!(d-\gamma_1)!}$ начина. След избиране на $z_1^{\gamma_1}$ изборът на $z_2^{\gamma_2}$ се осъществява по $\left(\begin{array}{c} d-\gamma_1 \\ \gamma_2 \end{array} \right) = \frac{(d-\gamma_1)!}{\gamma_2!(d-\gamma_1-\gamma_2)!}$ начина. Продължаваме аналогично по-нататък, като избираме $z_{n-1}^{\gamma_{n-1}}$ по $\left(\begin{array}{c} d-\gamma_1-\ldots-\gamma_{n-2} \\ \gamma_{n-1} \end{array} \right) = \frac{(d-\gamma_1-\ldots-\gamma_{n-2})!}{\gamma_{n-1}!(d-\gamma_1-\ldots-\gamma_{n-1})!}$ начина и накрая $z_n^{\gamma_n}$ по $\left(\begin{array}{c} d-\gamma_1-\ldots-\gamma_{n-1} \\ \gamma_n \end{array} \right) = \frac{(d-\gamma_1-\ldots-\gamma_{n-1})!}{\gamma_n!(d-\gamma_1-\ldots-\gamma_n)!} = 1$ начин. Доколкото изборът на $z_i^{\gamma_i}$ е независим за всяко $1 \leq i \leq n$, мономът z^γ се избира по

$$\left(\begin{array}{c} d \\ \gamma_1 \end{array} \right) \left(\begin{array}{c} d-\gamma_1 \\ \gamma_2 \end{array} \right) \ldots \left(\begin{array}{c} d-\gamma_1-\ldots-\gamma_{n-2} \\ \gamma_{n-1} \end{array} \right) \left(\begin{array}{c} d-\gamma_1-\ldots-\gamma_{n-1} \\ \gamma_n \end{array} \right) = \frac{d!}{\gamma_1! \ldots \gamma_n!}$$

начина, което доказва (1.1. В частност, $\frac{d!}{\gamma_1! \ldots \gamma_n!} \in \mathbb{N}$ за всички $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^{\geq 0}$ с $|\gamma| = d$.
Сега да въведем нови променливи $u = (u_1, \ldots, u_n)$ и да разгледаме матрица $A \in G \subset GL(n, k)$ с вектор-редове $\alpha_1, \ldots, \alpha_n \in k_{1 \times n}$ на нейната обратна $A^{-1} \in G$. За $x = (x_1, \ldots, x_n)^t$ и произволно естествено $d \in \mathbb{N}$ прилагаме към

$$(uA^{-1}x)^d = (u_1\alpha_1 x + \ldots + u_n\alpha_n x)^d$$

равенството (1.1) и получаваме

$$(uA^{-1}x)^d = \sum_{|\gamma|=d} \frac{d!}{\gamma_1! \ldots \gamma_n!} (u_1\alpha_1 x)^{\gamma_1} \ldots (u_n\alpha_n x)^{\gamma_n} = \sum_{|\gamma|=d} \frac{d!}{\gamma_1! \ldots \gamma_n!} u^\gamma (A^{-1}x)^\gamma. \tag{15.2}$$

Всеки елемент B на G действа върху стълба от променливи x по правилото $x \mapsto B^{-1}x$. При това действие дясната страна на (1.2) се трансформира в $\sum_{|\gamma|=d} \frac{d!}{\gamma_1! \ldots \gamma_n!} u^\gamma [(BA)^{-1}x]^\gamma$ и индуцира съответствие $(uA^{-1}x)^d \mapsto [u(BA)^{-1}x]^d$ на лявата страна. За $G = \{A_1, \ldots, A_{|G|}\}$ разглеждаме $uA_i^{-1}x$ с $1 \leq i \leq |G|$ като $|G|$ променливи и забелязваме, че G действа върху $\{uA_i^{-1}x \,|\, 1 \leq i \leq |G|\}$ чрез пермутации. Този факт може да се разглежда като конкретна реализация на Теоремата на Кейли, която установява, че всяка крайна група G е изоморфна на подгрупа на симетричната група $S_{|G|}$. Сумата на равенствата (1.2) за всички $A \in G$ дава

$$S_d := \sum_{A \in G} (uA^{-1}x)^d = \sum_{|\gamma|=d} \frac{d!}{\gamma_1! \ldots \gamma_n!} u^\gamma \left[\sum_{A \in G} (A^{-1}x)^\gamma \right] =$$

$$\sum_{|\gamma|=d} \frac{d!}{\gamma_1! \dots \gamma_n!} |G| u^\gamma R_G(x^\gamma).$$

Ако групата G се състои от елементите $A_1 = E_n, A_2, \dots, A_m$, то степенният сбор $S_d = \sum_{i=1}^m (uA_i^{-1}x)^d$ е симетрична функция на променливите $uA_i^{-1}x$ за $1 \leq i \leq m$. Съгласно Основната Теорема за симетричните полиноми, съществува полином $F' \in k[y_1, \dots, y_m]$, така че

$$S_d = F'(\sigma_1, \dots, \sigma_m)$$

за елементарните симетрични полиноми

$$\sigma_1 = \sum_{i=1}^m uA_i^{-1}x,$$

$$\sigma_2 = \sum_{1 \leq i_1 < i_2 \leq m} (uA_{i_1}^{-1}x)(uA_{i_2}^{-1}x),$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq m} (uA_{i_1}^{-1}x) \dots (uA_{i_k}^{-1}x)$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$\sigma_m = (uA_1^{-1}x) \dots (uA_m^{-1}x)$$

на $uA_i^{-1}x$. Ще докажем, че за всяко $1 \leq i \leq m$ съществува полином $H_i \in k[y_1, \dots, y_i]$, представящ елементарната симетрична функция

$$\sigma_i = H_i(S_1, \dots, S_i)$$

чрез степенните сборове $S_j = \sum_{i=1}^m (uA_i^{-1}x)^j$ за $1 \leq j \leq i$. В резултат ще получим съществуването на полином $F \in k[y_1, \dots, y_m]$, така че

$$S_d = F(S_1, \dots, S_m).$$

По-подробно,

$$\sum_{|\gamma|=d} \frac{d!}{\gamma_1! \dots \gamma_n!} |G| u^\gamma R_G(x^\gamma) = F\left(\sum \frac{|\beta|!}{\beta_1! \dots \beta_n!} |G| u^\beta R_G(x^\beta) \,|\, 1 \leq |\beta| \leq m \right) =$$

$$\widetilde{F}(u^\beta R_G(x^\beta) \,|\, 1 \leq |\beta| \leq m),$$

вземайки предвид, че коефициентите $\frac{i!}{\beta_1! \dots \beta_n!}$ се влагат в простото подполе $k_o \simeq \mathbb{Q}$ на полето k с характеристика $char(k) = 0$. Сега сравнявайки коефициентите на u^γ от двете страни получаваме, че

$$\frac{d!}{\gamma_1! \dots \gamma_n!} |G| R_G(x^\gamma) = \widetilde{F}(R_G(x^\beta) \,|\, 1 \leq |\beta| \leq m) \in k[R_G(x^\beta) \,|\, 1 \leq |\beta| \leq m],$$

откъдето $R_G(x^\gamma) \in k[R_G(x^\beta \,|\, 1 \leq |\beta| \leq |G|]$. С други думи, въвеждането на нови променливи $u_1, \dots, u_n$ дава възможност за извеждане на алгебричната зависимост на $R_G(x^\gamma)$ с $|\gamma| = d$ от $R_G(x^\beta)$, $1 \leq |\beta| \leq |G|$, използвайки алгебричната зависимост на степенните сборове S_d от $S_1, \dots, S_{|G|}$.

За изразяването на σ_i чрез полиноми на $S_1, \dots, S_i$ да напомним формулите на Нютон

$$S_i - \sigma_1 S_{i-1} + \dots + (-1)^j \sigma_j S_{i-j} + \dots + (-1)^{i-1} \sigma_{i-1} S_1 + (-1)^i \sigma_i i = 0$$

за $\forall 1 \leq i \leq m$. Над поле k с характеристика $char(k) = 0$, оттук изразяваме

$$\sigma_i = \frac{(-1)^{i+1}}{i} \left[S_i - \sigma_1 S_{i-1} + \dots + (-1)^j \sigma_j S_{i-j} + \dots + (-1)^{i-1} \sigma_{i-1} S_1 \right]. \quad (15.3)$$

С индукция по $1 \leq i \leq m$ от (1.3) получаваме, че $\sigma_i = H_i(S_1, \dots, S_i)$ за подходящи полиноми $H_i \in k[y_1, \dots, y_i]$. Наистина, $\sigma_1 = S_1$. Ако допуснем, че $\sigma_j = H_j(S_1, \dots, S_j)$ за всички $1 \leq j \leq i-1$, то от (1.3) следва, че $\sigma_i = H_i(S_1, \dots, S_i)$

за $H_i \in k[y_1, \ldots, y_i]$. Това завършва доказателството на Теоремата на Ньотер за крайната породеност на $k[x_1, \ldots, x_n]^G$ като пръстен над k, Q.E.D.
Използвайки Теоремата на Хилберт за базиса ще докажем по втори начин следната

Теорема 12. *Пръстенът $k[x_1, \ldots, x_n]^G$ на полиномиалните инварианти на крайна матрична група $G \subset GL(n, k)$ се поражда от краен брой хомогенни G-инвариантни полиноми над полето k.*

Доказателство: Нека $I \lhd k[x_1, \ldots, x_n]$ е идеалът, породен от хомогенните G-инвариантни полиноми $f \in k[x_1, \ldots, x_n]$ от обща степен $\deg(f) > 0$. Твърдим, че I се поражда от краен брой хомогенни G-инвариантни $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]^G$ от обща степен $\deg(f_i) > 0$. Наистина, при допускане на противното, за $\forall i \in \mathbb{N}$ и произволни хомогенни G-инвариантни $f_1, \ldots, f_i \in k[x_1, \ldots, x_n]^G$ от обща степен $\deg(f_j) > 0$ за $\forall 1 \leq j \leq i$, идеалът $\langle f_1, \ldots, f_i \rangle \lhd k[x_1, \ldots, x_n]$, породен от $f_1, \ldots, f_i$ се съдържа строго в I. Следователно съществува хомогенен G-инвариантен полином $f_{i+1} \in I \setminus \langle f_1, \ldots, f_i \rangle$ от обща степен $\deg(f_{i+1}) > 0$, така че идеалът $\langle f_1, \ldots, f_i, f_{i+1} \rangle \lhd k[x_1, \ldots, x_n]$ съдържа строго $\langle f_1, \ldots, f_i \rangle$. По този начин получаваме безкрайна строго растяща редица

$$\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \ldots \subsetneq \langle f_1, \ldots, f_i \rangle \subsetneq \langle f_1, \ldots, f_i, f_{i+1} \rangle \subsetneq \ldots$$

от идеали в $k[x_1, \ldots, x_n]$. Това противоречи на ньотеровостта на $k[x_1, \ldots, x_n]$ и доказва, че

$$I = \langle f_1, \ldots, f_m \rangle$$

за подходящи хомогенни G-инвариантни полиноми f_i с обща степен $\deg(f_i) > 0$. Ще докажем, че

$$k[x_1, \ldots, x_n]^G = k[f_1, \ldots, f_m].$$

Включването $k[f_1, \ldots, f_m] \subseteq k[x_1, \ldots, x_n]^G$ е ясно. За $k[x_1, \ldots, x_n]^G \subseteq k[f_1, \ldots, f_m]$ трябва да установим, че всеки G-инвариантен полином $F \in k[x_1, \ldots, x_n]^G$ е полином на $f_1, \ldots, f_m$ с коефициенти от k. Доколкото$F = \sum_{i=1}^{s} F^{(d_i)}$ е сума на своите хомогенни компоненти $F^{(d_i)}$ от степен $\deg(F^{(d_i)}) = d_i$, достатъчно е да докажем, че всеки хомогенен G-инвариантен полином $f \in k[x_1, \ldots, x_n]^G$ принадлежи на пръстена $k[f_1, \ldots, f_m]$. Ако $\deg(f) = 0$, то $f \in k \subset k[f_1, \ldots, f_m]$. Остава да проверим, че всеки хомогенен G-инвариантен полином $f \in k[x_1, \ldots, x_n]^G$ с обща степен $\deg(f) > 0$ попада в $k[f_1, \ldots, f_m]$. Да допуснем противното и да изберем хомогенен G-инвариантен полином $f \notin k[f_1, \ldots, f_m]$ от минимална обща степен $\deg(f) > 0$. Съгласно $f \in I$ съществуват $h_i \in k[x_1, \ldots, x_n]$, изразяващи f във вида

$$f = \sum_{i=1}^{m} f_i h_i. \tag{15.4}$$

Хомогенността на f и f_i гарантира хомогенността на h_i. Още повече, общата степен $\deg(h_i) = \deg(f) - \deg(f_i) < \deg(f)$ за $\forall 1 \leq i \leq m$. Прилагайки оператора на Рейнолдс към (1.4) получаваме, че

$$f = R_G(f) = R_G\left(\sum_{i=1}^{m} f_i h_i\right) = \sum_{i=1}^{m} f_i R_G(h_i).$$

Хомогенните полиноми $R_G(h_i)$ с обща степен $\deg(R_G(h_i)) = \deg(h_i) < \deg(f)$ принадлежат на $R[f_1, \ldots, f_m]$ съгласно избора на $f \notin k[f_1, \ldots, f_m]$ от минимална степен $\deg(f)$. Оттук следва, че и $f \in k[f_1, \ldots, f_m]$. Противоречието гарантира, че $k[x_1, \ldots, x_n]^G \subseteq k[f_1, \ldots, f_m]$, а оттам и $k[x_1, \ldots, x_n]^G = k[f_1, \ldots, f_m]$, Q.E.D.

ТВЪРДЕНИЕ 15.7. *Нека $>$ е мономна наредба в $k[x_1,\dots,x_n,y_1,\dots,y_m]$, спрямо която всеки моном $x^\alpha y^\beta$ с $|\alpha|=\sum_{i=1}^n \alpha_i > 0$ е по-голям от всеки моном y^γ. За произволни полиноми $f_1,\dots,f_m \in k[x_1,\dots,x_n]$ нека G е базис на Грьобнер на идеала*

$$J := \langle f_1 - y_1, \dots, f_m - y_m\rangle \lhd k[x_1,\dots,x_n,y_1,\dots,y_m],$$

а $g = \overline{f}^G$ е остатъкът на $f \in k[x_1,\dots,x_n]$ при деление с G в $k[x_1,\dots,x_n,y_1,\dots,y_m]$. В такъв случай:
(i) $f \in k[f_1,\dots,f_m]$ тогава и само тогава, когато $g \in k[y_1,\dots,y_m]$;
(ii) ако $f \in k[f_1,\dots,f_m]$, то $f = g(f_1,\dots,f_m)$ е представяне на f като полином на $f_1,\dots,f_m$.

Доказателство: Нека $G = \{g_1,\dots,g_t\}$ и $A_1,\dots,A_t \in k[x_1,\dots,x_n,y_1,\dots,y_m]$ са частните при деление на f с G, така че

$$f = \sum_{i=1}^t g_i A_i + g.$$

Ако $g \in k[y_1,\dots,y_m]$, то замествайки y_j с f_j получаваме $g_i(x_1,\dots,x_n,f_1,\dots,f_m) = 0 \in k[x_1,\dots,x_n]$ за всички $1 \le i \le t$, доколкото

$$g_i = \sum_{s=1}^m (f_s - y_s)h_s \in J = \langle f_1 - y_1,\dots,f_m - y_m\rangle.$$

В резултат, $f(x_1,\dots,x_n) = g(f_1,\dots,f_m) \in k[f_1,\dots,f_m]$ и $g(f_1,\dots,f_m)$ е представяне на f като полином на $f_1,\dots,f_m$.
Обратно, нека $f = H(f_1,\dots,f_m) \in k[f_1,\dots,f_m]$ за някакъв полином $H \in k[y_1,\dots,y_m]$. Да отбележим, че всеки моном $f_1^{\alpha_1}\dots f_m^{\alpha_m}$ се различава от $y_1^{\alpha_1}\dots y_m^{\alpha_m}$ с елемент на идеала $J \lhd k[x_1,\dots,x_n,y_1,\dots,y_m]$. По-точно,

$$f_1^{\alpha_1}\dots f_m^{\alpha_m} = [y_1 - (y_1 - f_1)]^{\alpha_1}\dots[y_m - (y_m - f_m)]^{\alpha_m} =$$

$$y_1^{\alpha_1}\dots y_m^{\alpha_m} + B_1(y_1 - f_1) + \dots + B_m(y_m - f_m)$$

за подходящи $B_1,\dots,B_m \in k[x_1,\dots,x_n,y_1,\dots,y_m]$. Следователно стойността на полинома $H(y_1,\dots,y_m) = \sum_{\alpha\in A} c_\alpha y_1^{\alpha_1}\dots y_m^{\alpha_m}$ за $y_j = f_j$ се представя във вида

$$H(f_1,\dots,f_m) = H(y_1,\dots,y_m) + C_1(y_1 - f_1) + \dots + C_m(y_m - f_m) \qquad (15.5)$$

чрез някакви полиноми $C_1,\dots,C_m \in k[x_1,\dots,x_n,y_1,\dots,y_m]$. Нека $G' := G \cap k[y_1,\dots,y_m]$ и $G' = \{g_1,\dots,g_s\}$ след евентуална пермутация на полиномите $g_1,\dots,g_t$ от базиса на Грьобнер G на J. Ако $H_1,\dots,H_s \in k[y_1,\dots,y_m]$ са частни, а $r' \in k[y_1,\dots,y_m]$ е остатък при деление на $H \in k[y_1,\dots,y_m]$ с G' в $k[y_1,\dots,y_m]$, то замествайки

$$H(y_1,\dots,y_m) = \sum_{i=1}^s g_i(y_1,\dots,y_m)H_i(y_1,\dots,y_m) + r'(y_1,\dots,y_m)$$

в (1.5) получаваме, че

$$f = H(f_1,\dots,f_m) =$$

$$\sum_{j=1}^m C_j(x_1,\dots,x_n,y_1,\dots,y_m)(y_j - f_j) + \sum_{i=1}^s g_i(y_1,\dots,y_m)H_i(y_1,\dots,y_m) + r'(y_1,\dots,y_m).$$

Достатъчно е да докажем, че r' е остатъкът при делението на $f \in k[x_1,\dots,x_n]$ с G в $k[x_1,\dots,x_n,y_1,\dots,y_m]$, доколкото $r' \in k[y_1,\dots,y_m]$. Еквивалентно, твърдим, че нито един моном на r' не се дели на $LT(g_j)$ за $1 \le j \le t$. Ако допуснем, че някакъв старши член $LT(g_i)$ дели моном $b_\mu y^\mu$ на $r'(y_1,\dots,y_m)$, то

$LT(g_i)$ не зависи от $x_1, \ldots, x_n$. Следователно $g_i \in k[y_1, \ldots, y_m]$, защото в противен случай g_i има моном $x^\alpha y^\beta$ с $|\alpha| > 0$, който трябва да е по-голям от $LT(g_i) \in k[y_1, \ldots, y_m]$ съгласно предположението за $>$. Но $LT(g_1), \ldots, LT(g_s)$ не делят мономите на r', защото r' е остатъкът при делението на $H(y_1, \ldots, y_m)$ с $G' = \{g_1, \ldots, g_s\}$. Следователно $\overline{f}^G = r' \in k[y_1, \ldots, y_m]$, Q.E.D.

Пример 15.8. *Цикличната група $C_3 \subset GL(2,k)$, породена от матрицата*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

е от ред 3 и пръстенът на C_3-инвариантните полиноми на x, y е

$$k[x,y]^{C_3} = k[x^2 - xy + y^2, x^2y - xy^2, x^3 - 3x^2y + y^3].$$

Непосредствено се проверява, че $A^2 \neq E_2$, $A^3 = E_2$, така че $C_3 = \langle A \rangle$ е от ред 3. По Теоремата на Ньотер 1, пръстенът $k[x,y]^{C_3}$ на C_3-инвариантните полиноми на x и y се поражда от хомогенните полиноми

$$R_{C_3}(x), R_{C_3}(y), R_{C_3}(x^2), R_{C_3}(xy), R_{C_3}(y^2),$$
$$R_{C_3}(x^3), R_{C_3}(x^2y), R_{C_3}(xy^2), R_{C_3}(y^3),$$

където операторът на Рейнолдс

$$R_{C_3}(f) = \frac{1}{3}[f(x,y) + f(-y, x-y) + f(-x+y, -x)]$$

за всеки полином $f \in k[x,y]$. Вземайки предвид, че

$$x^3 + y^3 - 3xy^2 = (x^3 + y^3 - 3x^2y) + 3(x^2y - 3xy^2),$$

стигаме до извода, че

$$k[x,y]^{C_3} = k[x^2 - xy + y^2, x^2y - xy^2, x^3 - 3x^2y + y^3].$$