Глава 3

Крайнопородени алгебри и модули над ньотеров пръстен

В настоящия въпрос са събрани някои предварителни сведения за доказателството на Теоремата на Хилберт за нулите. Междувременно, направената подготовка е използвана за доказване на Теоремата на Хилберт за базиса и Теоремата на Еми Ньотер за крайна породеност на алгебрата на инвариантните полиноми на крайна матрична група.

Определение 3.1. *Непразното множество M е модул над комутативния пръстен с единица R, ако в M са определени събиране*

$$M \times M \longrightarrow M,$$
$$(x, y) \mapsto x + y \quad за \quad x, y \in M$$

и умножение

$$R \times M \longrightarrow M,$$
$$(r, x) \mapsto rx \quad на\ x \in M\ с\ r \in R,$$

изпълняващи свойствата:
(i) асоциативност на събирането: $(x + y) + z = x + (y + z)$ *за* $\forall x, y, z \in M$;
(ii) комутативност на събирането : $x + y = y + x$ *за* $\forall x, y \in M$;
(iii) съществува нулев елемен 0_M, *така че* $x + 0_M = 0_M + x = x$ *за* $\forall x \in M$;
(iv) за $\forall x \in M$ *съществува противоположен елемент* $\exists(-x) \in M$, *така че* $x + (-x) = (-x) + x = 0_M$;
(v)дистрибутивен закон над скаларен множител: $(r + s)x = rx + sx$ *за* $\forall r, s \in R$, $\forall x \in M$;
(vi)дистрибутивен закон над векторен множител: $r(x+y) = rx+ry$ *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* $\forall x \in M$ *и* $1_R \in R$.

Всеки комутативен пръстен с единица R е модул над себе си.

Определение 3.2. *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 $r_1, \ldots, r_n \in R$ и $x_1, \ldots, x_n \in M$.

Определение 3.3. *Ако R и S са комутативни пръстени с единица и R е подпръстен на S, то казваме, че S е R-алгебра.*

Непосредствено се вижда, че ако пръстенът S е R-алгебра, то S е R-модул.

Определение 3.4. *Хомоморфизъм на R-алгебри S_1 и S_2 е хомоморфизъм на R-модули $\varphi : S_1 \to S_2$, който в същото време е и хомоморфизъм на пръстени.*

Пример 3.5. *Пръстенът $R[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от комутативен пръстен с единица R е R-алгебра.*

Определение 3.6. *Комутативният пръстен с единица S е крайнопородена алгебра над комутативния пръстен с единица R, ако съществуват елементи $a_1, \ldots, a_n \in S$, така че*

$$S = R[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in R[x_1, \ldots, x_n]\}$$

се състои от полиномите на $a_1, \ldots, a_n$ с коефициенти от R.

Ако $A = \{a_1, \ldots, a_n\}$ е множеството на пораждащите на R-алгебрата $S = R[a_1, \ldots, a_n]$, то естественото изображение

$$\pi_A : R[x_1, \ldots, x_n] \longrightarrow R[a_1, \ldots, a_n] = S,$$

$$\pi_A(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)$$

е хомоморфизъм на R-алгебри с образ $Im(\pi_A) = R[a_1, \ldots, a_n]$. Ядрото

$$I_A := Ker(\pi_A) = \{f \in R[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0\}$$

на този хомоморфизъм се нарича идеал на тъждествата на A. Съгласно теоремата за хомоморфизмите на пръстени, индуцираното изображение

$$\overline{\pi_A} : R[x_1, \ldots, x_n]/I_A \longrightarrow R[a_1, \ldots, a_n],$$

$$\overline{\pi_A}(f + I_A) = f(a_1, \ldots, a_n)$$

е изоморфизъм на пръстени. Още повече,

$$\overline{\pi_A}(r(f + I_A)) = \overline{\pi_A}(rf + I_A) = (rf)(a_1, \ldots, a_n) = rf(a_1, \ldots, a_n) = r\overline{\pi_A}(f + I_A)$$

за $\forall r \in R$ и $\forall f \in R[x_1, \ldots, x_n]$, така че $\overline{\pi_A}$ е изоморфизъм на R-алгебри.
По определение, всеки елемент на $S = R[a_1, \ldots, a_n]$ се представя във вида $a = f(a_1, \ldots, a_n)$ чрез някакъв полином $f \in R[x_1, \ldots, x_n]$. Ако $f(a_1, \ldots, a_n) = \widetilde{f}(a_1, \ldots, a_n)$ за $f, \widetilde{f} \in R[x_1, \ldots, x_n]$, то $\widetilde{f} - f = h \in I_A$. По този начин, всички представяния на $a = f(a_1, \ldots, a_n)$ чрез полиноми на $a_1, \ldots, a_n$ с коефициенти от R са от вида $a = (f + h)(a_1, \ldots, a_n)$ за произволни $h \in I_A$.

Определение 3.7. *Идеалът $\mathfrak{p}$ в комутативния пръстен с единица R се нарича прост, ако от $ab \in \mathfrak{p}$ за $a, b \in R$ следва, че $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$.*

Да напомним, че комутативният пръстен с единица S се нарича област или област на цялост, ако от $s_1 s_2 = 0_S$ за $s_1, s_2 \in S$ следва $s_1 = 0_S$ или $s_2 = 0_S$. С други думи, R е област точно когато нулевият идеал $\{0_R\} \lhd R$ е прост.

Лема 3.8. *Идеалът $\mathfrak{p}$ в комутативния пръстен с единица R е прост тогава и само тогава, когато фактор-пръстенът $R/\mathfrak{p}$ е област на цялост.*

Доказателство: Ако идеалът $\mathfrak{p} \lhd R$ е прост и $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = \mathfrak{p}$ за някакви $a, b \in R$, то $ab \in \mathfrak{p}$ води до $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Следователно $a + \mathfrak{p} = \mathfrak{p}$ или $b + \mathfrak{p} = \mathfrak{p}$ и $R/\mathfrak{p}$ няма ненулеви делители на нулата.
Обратно, ако $R/\mathfrak{p}$ е област на цялост и $ab \in \mathfrak{p}$ за някакви $a, b \in R$, то анулирането на произведението $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = \mathfrak{p}$ изисква $a + \mathfrak{p} = \mathfrak{p}$ или $b + \mathfrak{p} = \mathfrak{p}$. Следователно $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$ и идеалът $\mathfrak{p} \lhd R$ е прост, Q.E.D.
В частност, крайнопородената R-алгебра $R[a_1, \ldots, a_n] \simeq R[x_1, \ldots, x_n]/I_A$ е област на цялост точно когато идеалът $I_A \lhd k[x_1, \ldots, x_n]$ на тъждествата на A е прост.

Определение 3.9. *Комутативният пръстен с единица R се нарича ньотеров, ако всеки идеал $I \lhd R$ е крайнопороден, т.е. съществуват $r_1, \ldots, r_n \in I$, така че*

$$I = \langle r_1, \ldots, r_n \rangle = \left\{ \sum_{i=1}^{n} r_i s_i \,\middle|\, \forall s_i \in R, \right\}.$$

ТВЪРДЕНИЕ 3.10. *Ако R е ньотеров комутативен пръстен с единица, то пръстенът на полиномите $R[x]$ на x с коефициенти от R е също ньотеров.*

Доказателство: Нулевият идеал $\{0_R\} = \langle 0_R \rangle \triangleleft R[x]$ е крайнопороден, така че остава да установим крайната породеност на произволен ненулев идеал $\{0_R\} \neq I \triangleleft R[x]$. За целта избираме редица от ненулеви полиноми $f_1, \ldots, f_i \ldots \in I$, така че
(i) $0_R \neq f_1 \in I$ е от минимална степен;
(ii) ако $\langle f_1, \ldots, f_i \rangle \subsetneqq I$, то избираме $f_{i+1} \in I \setminus \langle f_1, \ldots, f_i \rangle$ от минимална степен;
(iii) ако $\langle f_1, \ldots, f_i \rangle = I$, то спираме избирането на полиноми от тази редица.
Идеалите $J_i = \langle LC(f_1), \ldots, LC(f_i) \rangle$ в R, породени от старшите коефициенти на $f_1, \ldots, f_i$ образуват ненамаляваща редица

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq J_{i-1} \subseteq J_i \subseteq J_{i+1} \subseteq \ldots .$$

Тяхното обединение $J = \cup_{i=1}^{\infty} J_i$ е идеал в R. Твърдим, че $J = J_m = J_{m+1} = \ldots$ за някое естествено m. За целта използваме, че пръстенът R е ньотеров, така че идеалът $J = \langle r_1, \ldots, r_s \rangle$ е крайнопороден. Ако пораждащите $r_j \in J_{i(j)}$ за всички $1 \leq j \leq s$ и $m = \max(i(1), \ldots, i(s))$, то $r_1, \ldots, r_s \in J_m$, откъдето $J = \langle r_1, \ldots, r_s \rangle \subseteq J_m \subseteq J$. Следователно $J = J_m = J_{m+1} = \ldots$ съгласно $J_k \subseteq J = J_m \subseteq J_k$ за $\forall k > m$. Твърдим, че $\langle f_1, \ldots, f_m \rangle = I$. В противен случай, избираме $f_{m+1} \in I \setminus \langle f_1, \ldots, f_m \rangle$ от минимална степен. Старшият коефициент $LC(f_{m+1}) \in J_{m+1} = J = \langle LC(f_1), \ldots, LC(f_m) \rangle$ се представя във вида $LC(f_{m+1}) = \sum\limits_{i=1}^{m} LC(f_i) r_i$ чрез подходящи $r_i \in R$. Ако $\deg(f_s) = d_s$, то по построение $d_{m+1} \geq d_i$ за $\forall 1 \leq i \leq m$. Полиномът

$$g(x) = f_{m+1}(x) - \sum_{i=1}^{m} r_i x^{d_{m+1} - d_i} f_i(x)$$

е от степен $\deg(g) < d_{m+1}$. По построение, от тук следва, че $g \in \langle f_1, \ldots, f_m \rangle$. Следователно $f_{m+1} = g + \sum\limits_{i=1}^{m} r_i x^{d_{m+1} - d_i} f_i(x) \in \langle f_1, \ldots, f_m \rangle$, което противоречи на избора на $f_{m+1} \in I \setminus \langle f_1, \ldots, f_m \rangle$. Това доказва, че $I = \langle f_1, \ldots, f_m \rangle = I$, Q.E.D.

СЛЕДСТВИЕ 3.11. *Ако $\varphi : R \to S$ е хомоморфизъм на комутативни пръстени с единица и R е ньотеров пръстен, то образът $Im(\varphi) := \{\varphi(r) \,|\, r \in R\}$ на φ е ньотеров пръстен.*

Доказателство: Трябва да докажем, че произволен идеал $I \triangleleft Im(\varphi)$ е крайнопороден. За целта използваме, че пълният праобраз

$$\varphi^{-1}(I) := \{r \in R \,|\, \varphi(r) \in I\}$$

е идеал в R. Наистина, за произволни $a, b \in \varphi^{-1}(I)$ и $r \in R$ е в сила $a - b, ar \in \varphi^{-1}(I)$ съгласно $\varphi(a-b) = \varphi(a) - \varphi(b) \in I$ и $\varphi(ar) = \varphi(a)\varphi(r) \in I$ за $\varphi(a), \varphi(b) \in I$. Доколкото пръстенът R е ньотеров, идеалът $\varphi^{-1}(I) \triangleleft R$ е крайнопороден, т.е. съществуват $r_1, \ldots, r_n \in \varphi^{-1}(I)$, така че

$$\varphi^{-1}(I) = \langle r_1, \ldots, r_n \rangle = \left\{ \sum_{i=1}^{n} r_i s_i \,\middle|\, s_i \in R,\, 1 \leq i \leq n \right\}.$$

Твърдим, че

$$I = \langle \varphi(r_1), \ldots, \varphi(r_n) \rangle = \left\{ \sum_{i=1}^{n} \varphi(r_i)\varphi(s_i) \,\middle|\, s_i \in R,\, 1 \leq i \leq n \right\}$$

се поражда от $\varphi(r_1), \ldots, \varphi(r_n)$ като идеал в пръстена $Im(\varphi) = \{\varphi(s) \,|\, s \in R\}$. Наистина, всеки елемент на $I \lhd Im(\varphi)$ е от вида $\varphi(r)$ за някое $r \in R$. По определението на $\varphi^{-1}(I)$ имаме $r \in \varphi^{-1}(I)$, така че $r = \sum_{i=1}^{n} r_i s_i$ за подходящи $s_1, \ldots, s_n \in R$. Следователно $\varphi(r) = \sum_{i=1}^{n} \varphi(r_i)\varphi(s_i) \in \langle \varphi(r_i), \ldots, \varphi(r_n) \rangle$, така че идеалът $I = \langle \varphi(r_1), \ldots, \varphi(r_n) \rangle$ е крайнопороден и пръстенът $Im(\varphi)$ е ньотеров, Q.E.D.

Следствие 3.12. *Ако R е ньотеров пръстен, то всяка крайнопородена R-алгебра $S = R[a_1, \ldots, a_n]$ е също ньотеров пръстен.*

Доказателство: С индукция по броя на променливите n, първо ще установим, че пръстенът на полиномите $R[x_1, \ldots, x_n]$ на $x_1, \ldots, x_n$ с коефициенти от R е ньотеров. Случаят $n = 1$ е доказан от Твърдение 3.10. Ако допуснем, че пръстенът $R[x_1, \ldots, x_{i-1}]$ е ньотеров, то отново по Твърдение 3.10 получаваме, че и пръстенът $R[x_1, \ldots, x_{i-1}][x_i] = R[x_1, \ldots, x_i]$ е ньотеров.
Ако $\pi_A : R[x_1, \ldots, x_n] \to S = R[a_1, \ldots, a_n]$ е естественият епиморфизъм, чието ядро $Ker(\pi_A) = I_A$ е идеалът на тъждествата на $A = \{a_1, \ldots, a_n\}$, то Следствие 3.11 гарантира, че $Im(\pi_A) = R[a_1, \ldots, a_n] = S$ ньотеров пръстен, щом пръстенът на полиномите $R[x_1, \ldots, x_n]$ е ньотеров, Q.E.D.
В частност, ньотеровостта на пръстена $F[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле F е известна като Теорема на Хилберт за базиса.

Определение 3.13. *Нека R е комутативен пръстен с единица, M е R-модул, а N е непразно подмножество на M. Ако за произволни $x, y \in N$ и $r \in R$ е в сила $x - y, rx \in N$, то казваме, че N е R-подмодул на M.*

Ако N е R-подмодул на R-модула M, то $(N, +)$ е нормална подгрупа на $(M, +)$ и можем да образуваме фактор-групата $(M/N, +)$. За произволни $m + N \in M/N$ и $r \in R$ полагаме

$$r(m + N) := rm + N.$$

Така зададената операция е коректно определена, защото ако $m + N = m' + N$, то $rm + N = rm' + N$ съгласно $rm' - rm = r(m' - m) \in N$ за $m' - m \in N$. Непосредствено се проверява, че аксиомите за R-модул са изпълнени за така определените събиране и умножение с $r \in R$ в M/N. Казваме, че M/N е фактор-модулът на M по N.
Естественият хомоморфизъм

$$\pi_N : M \longrightarrow M/N$$

на адитивната група $(M, +)$ върху адитивната фактор-група $(M/N, +)$ с ядро $Ker(\pi_N) = N$ е R-модулен хомоморфизъм съгласно

$$\pi_N(rx) = rx + N = r(x + N) = r\pi_N(x)$$

за $\forall r \in R$, $\forall x \in M$. По този начин, всеки R-подмодул N на R-модул M се реализира като ядро на R-модулен хомоморфизъм на M върху фактор-модула M/N на M по N.
В частност, всеки комутативен пръстен с единица R е R-модул. При това, R-подмодулите на R са точно идеалите $I \lhd R$ и всички те се реализират като ядра на естествени R-модулни хомоморфизми $\pi_I : R \to R/I$. Да отбележим, че π_I е и хомоморфизъм на пръстени, съгласно $\pi_I(rs) = rs + I = (r + I)(s + I) = \pi_I(r) + \pi_I(s)$ за $\forall r, s \in R$.
Като непосредствено обобщение на теоремата на хомоморфизмите на пръстени получаваме следната теорема за хомоморфизмите на R-модули:
Ако $\varphi : M \to N$ е хомоморфизъм на R-модули, то ядрото $Ker(\varphi) := \{x \in M \,|\, \varphi(x) = 0_N\}$ е R-подмодул на M, образът $Im(\varphi) := \{\varphi(x) \,|\, x \in M\}$ е R-подмодул на N и

$$\overline{\varphi} : M/Ker(\varphi) \longrightarrow Im(\varphi),$$

$$\overline{\varphi}(x + Ker(\varphi)) = \varphi(x) \quad \text{за } \forall x \in M$$

е изоморфизъм на R-модули.
По-точно, φ е хомоморфизъм на $(M,+)$ в $(N,+)$, така че по теоремата за хомоморфизмите на групи получаваме, че $\overline{\varphi}$ е изоморфизъм на $(M/Ker(\varphi),+)$ с $(Im(\varphi),+)$ Още повече,

$$\overline{\varphi}(r(x + Ker(\varphi))) = \overline{\varphi}(rx + Ker(\varphi)) = \varphi(rx) = r\varphi(x) = r\overline{\varphi}(x + Ker(\varphi))$$

за $\forall r \in R$ и $\forall x + Ker(\varphi) \in M/Ker(\varphi)$, така че $\overline{\varphi}$ е изоморфизъм на R-модули.

Определение 3.14. *Казваме, че M е крайнопороден R-модул, ако съществуват краен брой елементи $\mu_1, \ldots, \mu_n \in M$, така че*

$$M = R\mu_1 + \ldots + R\mu_n = \left\{ \sum_{i=1}^{n} r_i\mu_i \,\middle|\, r_i \in R, \forall 1 \leq i \leq n \right\}.$$

Можем да кажем, че комутативният пръстен с единица R е ньотеров точно тогава, когато всеки негов R-подмодул е крайнопороден R-модул. В частност, Следствие 3.11 установява, че ако R е ньотеров пръстен, а $\varphi : R \to S$ е хомоморфизъм на пръстени, то всеки $Im(\varphi)$-подмодул на $Im(\varphi)$ е крайнопороден $Im(\varphi)$-модул. Това твърдение може да се модифицира по следния начин:

Лема 3.15. *(i) Ако R е ньотеров пръстен, а $\psi : R \to M$ е хомоморфизъм на R-модули, то всеки R-подмодул на $Im(\psi)$ е крайнопороден R-модул.*
(ii) Ако R е ньотеров пръстен и R-модулът $M_o = R\mu$ се поражда от единствен свой елемент μ, то всеки R-подмодул на M_o е крайнопороден.

Доказателство: (i) Ако $\mu := \psi(1_R) \in M$, то за $\forall r \in R$ е в сила

$$\psi(r) = \psi(r.1_R) = r\psi(1_R) = r\mu,$$

така че $Im(\psi) = R\mu$ се поражда от μ като R-модул. За произволен R-подмодул N на $Im(\psi) = R\mu$ твърдим, че пълният праобраз

$$\psi^{-1}(N) := \{r \in R \,|\, \psi(r) = r\mu \in N\}$$

е идеал в R. Наистина, ако $r_1, r_2 \in \psi^{-1}(N)$, то $\psi(r_j) = r_j\mu \in N$ за $j = 1, 2$ и $\psi(r_1 - r_2) = \psi(r_1) - \psi(r_2) = r_1\mu - r_2\mu \in N$, така че $r_1 - r_2 \in \pi^{-1}(N)$. За $\forall r \in \psi^{-1}(N)$ и $\forall s \in R$ е в сила $\psi(rs) = s\psi(r) = s(r\mu) \in N$ съгласно $r\mu \in N$. Това доказва, че $\psi^{-1}(N) \triangleleft R$. Доколкото пръстенът R е ньотеров, съществуват краен брой пораждащи $r_1, \ldots, r_n \in \psi^{-1}(N)$ на идеала

$$\psi^{-1}(N) = \langle r_1, \ldots, r_n \rangle = \left\{ \sum_{i=1}^{n} r_i s_i \,\middle|\, s_i \in R, \forall 1 \leq i \leq n \right\}.$$

Твърдим, че

$$N = Rr_1\mu + \ldots + Rr_n\mu$$

се поражда от образите им $\psi(r_i) = r_i\mu$ като R-модул. От една страна, $r_i\mu \in N$ води до $Rr_1\mu + \ldots + Rr_n\mu \subseteq N$. От друга страна, ако $r\mu \in N$, то $r \in \psi^{-1}(N)$, така че $r = \sum_{i=1}^{n} r_i s_i$ за подходящи $s_i \in R$. В резултат,

$$r\mu = \psi(r) = \psi\left(\sum_{i=1}^{n} r_i s_i\right) = \sum_{i=1}^{n} s_i\psi(r_i) = \sum_{i=1}^{n} s_i(r_i\mu) \in Rr_1\mu + \ldots + Rr_n\mu.$$

Това установява включването $N \subseteq Rr_1\mu + \ldots + Rr_n\mu$, а оттам и съвпадението $N = Rr_1\mu + \ldots + Rr_n\mu$.
(ii) Естествената проекция

$$\pi : R \longrightarrow R\mu = M_o,$$
$$\pi(r) = r\mu \quad \text{за} \quad \forall r \in R$$

е хомоморфизъм на R-модули, доколкото $\pi(r+s) = (r+s)\mu = r\mu + s\mu = \pi(r) + \pi(s)$ и $\pi(rs) = (rs)\mu = r(s\mu) = r\pi(s)$ за $\forall r, s \in R$. Образът $Im(\pi) = R\mu = M_o$, защото $\forall r\mu = \pi(r)$. Съгласно (i), всеки подмодул на $M_o = Im(\pi)$ е крайнопороден R-модул, Q.E.D.
Сега ще обобщим Лема 3.15 (ii) чрез следното

Твърдение 3.16. *Ако R е ньотеров комутативен пръстен с единица, а M е крайнопороден модул над R, то всеки подмодул N на M е крайнопороден.*

Доказателство: Ще работим с индукция по броя n на пораждащите $\mu_1, \ldots, \mu_n$ на $M = R\mu_1 + \ldots + R\mu_n$ като R-модул. Лема 3.15 (ii) установява верността на твърдението за $n = 1$. За произволно естествено n да разгледаме естествения хомоморфизъм на R-модули

$$\pi_n : M = R\mu_1 + \ldots + R\mu_n \longrightarrow M/R\mu_n,$$

$$\pi_n\left(\sum_{i=1}^{n} r_i\mu_i\right) = \sum_{i=1}^{n} r_i\mu_i + R\mu_n = \sum_{i=1}^{n-1} r_i\mu_i + R\mu_n$$

с ядро $Ker(\pi_n) = R\mu_n$ и образ $Im(\pi_n) = M/R\mu_n$. Твърдим, че

$$M/R\mu_n = R(\mu_1 + R\mu_n) + \ldots + R(\mu_{n-1} + R\mu_n)$$

се поражда от $\mu_i + R\mu_n$ с $1 \leq i \leq n-1$ като R-модул. От една страна, всички елементи $\mu_i + R\mu_n \in M/R\mu_n$, така че $\sum_{i=1}^{n-1} R(\mu_i + R\mu_n)$ е R-подмодул на фактор-модула $M/R\mu_n$. Обратно, всеки елемент на $M/R\mu_n$ е от вида $\sum_{i=1}^{n} r_i\mu_i + R\mu_n = \sum_{i=1}^{n-1} r_i\mu_i + R\mu_n = \sum_{i=1}^{n-1} r_i(\mu_i + R\mu_n) \in R(\mu_1 + R\mu_n) + \ldots + R(\mu_{n-1} + R\mu_n)$, така че $M/R\mu_n = R(\mu_1 + R\mu_n) + \ldots + R(\mu_{n-1} + R\mu_n)$. Ако N е R-подмодул на M, то π_n се ограничава до хомоморфизъм на R-модули

$$\pi_n : N \longrightarrow (N + R\mu_n)/R\mu_n.$$

По индукционно предположение, подмодулът $(N+R\mu_n)/R\mu_n$ на фактор-модула $M/R\mu_n = R(\mu_1 + R\mu_n) + \ldots + R(\mu_{n-1} + R\mu_n)$ е крайнопороден. Нека

$$(N + R\mu_n)/R\mu_n = R(\nu_1 + R\mu_n) + \ldots + R(\nu_m + R\mu_n)$$

за някакви $\nu_1, \ldots, \nu_m \in N$. От друга страна, $N \cap R\mu_n$ е R-подмодул на $R\mu_n$, така че се поражда от краен брой елементи $\lambda_1, \ldots, \lambda_l \in N \cap R\mu_n$ съгласно Лема 3.15 (ii),

$$N \cap R\mu_n = R\lambda_1 + \ldots + R\lambda_l.$$

Твърдим, че

$$N = R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m.$$

От една страна, $\lambda_1, \ldots, \lambda_l, \nu_1, \ldots, \nu_m \in N$ пораждат R-подмодула $R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m$ на N. От друга страна, произволен елемент $x \in N$ се изобразява в $\pi_n(x) = \sum_{i=1}^{m} r_i(\nu_i + R\mu_n)$ под действие на естествения хомоморфизъм π_n с ядро $R\mu_n$. По този начин, $x_o := x - \sum_{i=1}^{m} r_i\nu_i \in N$ има образ

$$\pi_n(x_o) = \pi_n(x) - \sum_{i=1}^{m} r_i(\nu_i + R\mu_n) = R\mu_n$$

и $x_o \in N \cap R\mu_n$. В резултат, $x_o = \sum_{j=1}^{l} s_j\lambda_j$ за подходящи $s_j \in R$ и $x = \sum_{j=1}^{l} s_j\lambda_j + \sum_{i=1}^{m} r_i\nu_i \in R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m$. Това установява, че

$$N = R\lambda_1 + \ldots + R\lambda_l + R\nu_1 + \ldots + R\nu_m$$

е крайнопороден R-модул, Q.E.D.
Основният резултат на настоящия въпрос е следното

ТВЪРДЕНИЕ 3.17. *Нека R е ньотеров пръстен, $R[a_1, \ldots, a_n]$ е крайнопородена R-алгебра, а S е такъв подпръстен на $R[a_1, \ldots, a_n]$, съдържащ R, че $R[a_1, \ldots, a_n]$ е крайнопороден S-модул. Тогава S е крайнопородена R-алгебра.*

Доказателство: Нека

$$R[a_1, \ldots, a_n] = Sb_1 + \ldots + Sb_m.$$

Без ограничение на общността можем да считаме, че $b_m = 1_R$. (Ако $b_i \neq 1_R$ за всички $1 \leq i \leq m$, то полагаме $b_{m+1} := 1_R$ и увеличаваме броя на пораждащите на $R[a_1, \ldots, a_n]$ като S-модул.) От $a_p \in R[a_1, \ldots, a_n]$ за $\forall 1 \leq p \leq n$ следва съществуването на $\alpha_{p1}, \ldots, \alpha_{pm} \in S$, така че

$$a_p = \sum_{q=1}^{m} \alpha_{pq} b_q.$$

От друга страна, за произволни $1 \leq i < j \leq m$ елементите $b_i, b_j \in R[a_1, \ldots, a_n]$ имат произведение $b_i b_j \in R[a_1, \ldots, a_n]$, така че

$$b_i b_j = \sum_{q=1}^{m} \alpha_{ijq} b_q$$

за подходящи $\alpha_{ijq} \in S$. Да разгледаме крайнопородената R-алгебра

$$S_o := R[\alpha_{pq}, \alpha_{ijq} \,|\, 1 \leq p \leq n,\, 1 \leq i, j, q \leq m].$$

Пръстенът R е ньотеров, така че и пръстенът S_o е ньотеров съгласно Следствие 3.12. Твърдим, че

$$R[a_1, \ldots, a_n] = S_o b_1 + \ldots + S_o b_m$$

се поражда като S_o-модул от фиксираните си пораждащи като S-модул. От една страна,

$$S_o b_1 + \ldots + S_o b_m \subseteq Sb_1 + \ldots + Sb_m = R[a_1, \ldots, a_n],$$

доколкото S_o е подпръстен на S. За обратното включване трябва да покажем, че всеки полином $f = \sum_{\beta \in B} r_\beta a^\beta$ на $a_1, \ldots, a_n$ с коефициенти $r_\beta \in R$ принадлежи на S_o-модула $M_o = S_o b_1 + \ldots + S_o b_m$. Вземайки предвид, че M_o е подгрупа на адитивната група $(R[a_1, \ldots, a_n], +)$, достатъчно е да проверим, че всеки моном $r_\beta a^\beta$ принадлежи на M_o. С индукция по общата степен $|\beta| = \sum_{i=1}^{n} \beta_i$ ще докажем, че $a^\beta \in M_o$. Доколкото M_o е S_o-модул, а R е подпръстен на S_o, оттук следва $r_\beta a^\beta \in M_o$ за произволно $r_\beta \in R$. Ако $|\beta| = \sum_{i=1}^{n} \beta_i = 0$, то $\beta_1 = \ldots = \beta_n = 0$ и $a^\beta = 1_R = b_m \in M_o$. Да допуснем, че $a^\gamma \in M_o$ за всички $\gamma = (\gamma_1, \ldots, \gamma_n)$ с $|\gamma| = \sum_{i=1}^{n} \gamma_i < \sum_{i=1}^{n} \beta_i = |\beta|$ и да изберем $1 \leq i \leq n$ с $\beta_i \geq 1$. Тогава за $\beta' = (\beta_1, \ldots, \beta_{i-1}, \beta_i - 1, \beta_{i+1}, \ldots, \beta_n)$ е в сила индукционното предположение $a^{\beta'} = \sum_{j=1}^{m} s_j b_j \in M_o$, така че

$$a^\beta = a^{\beta'} a_i = \left(\sum_{j=1}^{m} s_j b_j \right) \left(\sum_{q=1}^{m} \alpha_{iq} b_q \right) = \sum_{j=1}^{m} \sum_{q=1}^{m} s_j \alpha_{iq} \left(\sum_{p=1}^{m} \alpha_{jqp} b_p \right) =$$

$$\sum_{j=1}^{m} \sum_{q=1}^{m} \sum_{p=1}^{m} s_j \alpha_{iq} \alpha_{jqp} b_p \in S_o b_1 + \ldots + S_o b_m = M_o.$$

Това установява, че

$$R[a_1, \ldots, a_n] = S_o b_1 + \ldots + S_o b_m.$$

По построение, S_o е подпръстен на S, така че S е S_o-модул. Още повече, S_o е ньотеров пръстен, а S е S_o-подмодул на крайнопородения S_o-модул $R[a_1, \ldots, a_n]$, така че

$$S = S_o \sigma_1 + \ldots + S_o \sigma_l$$

е крайнопороден S_o-модул по Твърдение 3.16. От една страна,

$$S = S_o\sigma_1 + \ldots + S_o\sigma_l \subseteq S_o[\sigma_1, \ldots, \sigma_l],$$

доколкото всички полиноми на $\sigma_1, \ldots, \sigma_l$ с коефициенти от S_o съдържат хомогенните линейни полиноми. От друга страна,

$$S_o[\sigma_1, \ldots, \sigma_l] \subseteq S,$$

защото S_o е подпръстен на S и $\sigma_1, \ldots, \sigma_l \in S$, така че $S_o[\sigma_1, \ldots, \sigma_l]$ е подпръстен на S. Следователно

$$S = S_o[\sigma_1, \ldots, \sigma_l] = R[\alpha_{pq}, \alpha_{ijq} \,|\, 1 \leq p \leq n,\ 1 \leq i, j, q \leq m][\sigma_r \,|\, 1 \leq r \leq l] =$$
$$R[\alpha_{pq}, \alpha_{ijq}, \sigma_r \,|\, 1 \leq p \leq n,\ 1 \leq i, j, q \leq m,\ 1 \leq r \leq l]$$

е крайнопородена R-алгебра, Q.E.D.

Определение 3.18. *Елементът a на R-алгебрата S се нарича цял над R, ако съществуват $r_1, \ldots, r_n \in R$, така че*

$$a^n + r_1a^{n-1} + \ldots + r_{n-1}a + r_n = 0.$$

Ясно е, че всеки елемент $r \in R$ е цял над R, в качеството си на корен на полинома $x - r = 0$.
Ако E е подполе на поле F, то казваме, че $a \in F$ е алгебричен над E, ако съществуват $e_0, e_1, \ldots, e_n \in E$, $e_0 \neq 0_E$, така че

$$e_0a^n + e_1a^{n-1} + \ldots + e_{n-1}a + e_n = 0_E.$$

Доколкото всички ненулеви елементи на полето E са обратими, $a \in F$ е алгебричен над E тогава и само тогава, когато a е цял над E.
Нека полето F е разширение на полето E. Елементите $a_1, \ldots, a_k \in F$ са алгебрични над E, ако съществува нетъждествено нулев полином $0 \not\equiv f(x_1, \ldots, x_k) \in E[x_1, \ldots, x_k]$, така че $f(a_1, \ldots, a_k) = 0$. Ако $a_1, \ldots, a_k \in F$ не са алгебрични над E, то казваме, че $a_1, \ldots, a_k$ са трансцендентни над E.

Лема 3.19. *Ако елементът a на R-алгебрата S е цял над R, то пръстенът $R[a]$ е крайнопороден R-модул.*
В частност, ако полето F е разширение на полето E и елементът $a \in F$ е алгебричен над E, то пръстенът $E[a]$ е поле и крайномерно линейно пространство над E.

Доказателство: Ако $a^n + r_1a^{n-1} + \ldots + r_n = 0$ за някакви $r_1, \ldots, r_n \in R$, то

$$a^n = -r_1a^{n-1} - \ldots - r_{n-1}a - r_n \in R.1_R + Ra + \ldots + Ra^{n-1} =: M_o.$$

С индукция по $k \geq n$ ще установим, че мономът a^k принадлежи на крайнопородения R-модул M_o. По този начин, $R[a] \subseteq M_o$, а оттам и $R[a] = M_o$. Базата на индукцията $k = n$ е вече установена. Ако допуснем, че $a^{k-1} = \sum_{i=1}^{n} t_ia^{n-i}$ за някакви $t_i \in R$, то

$$a^k = (t_1a^{n-1} + t_2a^{n-2} + \ldots + t_n)a =$$
$$t_1(-r_1a^{n-1} - \ldots - r_{n-1}a - r_n) + t_2a^{n-1} + \ldots + t_na =$$
$$(t_2 - t_1r_1)a^{n-1} + \ldots + (t_n - t_1r_{n-1})a - t_1r_n \in M_o.$$

Нека $f(x) \in E[x]$ е полином от минимална степен с корен a. Без ограничение на общността можем да считаме, че старшият коефициент на $f(x)$ е $1 = 1_E$. Горните разглеждания доказват, че ако $\deg(f) = n$, то $E[a] = E + Ea + \ldots + Ea^{n-1}$. Остава да докажем, че $E[a]$ е подполе на F. Преди всичко да споменем, че полиномът $f(x) \in E[x]$ е неразложим над полето E поради минималността на степента му $\deg(f)$. Произволен ненулев елемент $0_E \neq g(a) \in E[a]$ е представен с полином $g(x) \in E[x]$, който е взаимно прост с $f(x)$. Следователно

съществуват полиноми $u(x), v(x) \in E[x]$, реализиращи тъждеството на Безу $f(x)u(x) + g(x)v(x) = 1$. Замествайки $x = a$ получаваме че $g(a)v(a) = 1$, откъдето $g(a)^{-1} = v(a) \in E[a]$. Това доказва, че $E[a]$ е подполе на F, Q.E.D.
За по-нататъшното изучаване на свойствата на цялата зависимост е необходима следната

Лема 3.20. *Ако R-алгебрата S е крайнопородена като R-модул и M е крайнопороден S-модул, то M е крайнопороден R-модул.*

Доказателство: Нека $S = Rs_1 + \ldots + Rs_m$ за подходящи $s_1, \ldots s_m \in S$ и $M = S\mu_1 + \ldots + S\mu_n$ за подходящи $\mu_1, \ldots, \mu_n \in M$. Тогава твърдим, че

$$M = \sum_{j=1}^{m} \sum_{i=1}^{n} Rs_j\mu_i$$

се поражда като R-модул от своите елементи $s_j\mu_i \in M$. Наистина, включването $\sum_{j=1}^{m} \sum_{i=1}^{n} Rs_j\mu_i \subseteq M$ е ясно от това, че R е подпръстен на S, $s_i \in S$ и $\mu_i \in M$. Обратно, всеки елемент $\mu \in M$ се представя във вида $\mu = \sum_{i=1}^{n} \sigma_i\mu_i$ чрез някакви $\sigma_i \in S$. От своя страна, $\sigma_i = \sum_{j=1}^{m} r_{ij}s_j$ за подходящи $r_{ij} \in R$, така че

$$\mu = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} r_{ij}s_j \right) \mu_i = \sum_{j=1}^{m} \sum_{i=1}^{n} r_{ij}(s_j\mu_i).$$

Това установява, че $M \subseteq \sum_{j=1}^{m} \sum_{i=1}^{n} Rs_j\mu_i$, а оттам и $M = \sum_{j=1}^{m} \sum_{i=1}^{n} Rs_j\mu_i$, Q.E.D.

Твърдение 3.21. *Ако $S = R[a_1, \ldots, a_n]$ е крайнопородена R-алгебра и $a_1, \ldots, a_n \in S$ са цели над R, то S е крайнопороден R-модул.*

Доказателство: Ще разсъждаваме с индукция по броя на пораждащите n на S като R-алгебра. От Лема 3.19 знаем, че R-алгебрата $R[a_1]$ е крайнопороден R-модул, ако a_1 е цял над R. За произволно естествено $n > 1$, R-алгебрата $R[a_1, \ldots, a_{n-1}]$ е крайнопороден R-модул по индукционно предположение. Цялата зависимост

$$a_n^m + r_1 a_n^{m-1} + \ldots + r_{m-1}a_n + r_m = 0_R$$

на a_n над $R \ni r_1, \ldots, r_m$ представлява и цяла зависимост на a_n над R-алгебрата $R[a_1, \ldots, a_{n-1}] \ni r_1, \ldots, r_m$, така че $R[a_1, \ldots, a_{n-1}, a_n] = R[a_1, \ldots, a_{n-1}][a_n]$ е крайнопороден $R[a_1, \ldots, a_{n-1}]$-модул съгласно Лема 3.19. Прилагайки Лема 3.20 получаваме, че $R[a_1, \ldots, a_n]$ е крайнопороден R-модул, Q.E.D.
Като приложение на Твърдение 3.17 и Твърдение 3.21, ще докажем Теоремата на Еми Ньотер за крайна породеност на k-алгебрата $k[x_1, \ldots, x_n]^G$ на инвариантните полиноми на крайна матрична група G. Да напомним, че общата линейна група над поле k се състои от неособените квадратни матрици

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

с обичайната операция умножение на матрици. Ако $x = \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix}$ е стълб от променливи, то съответствието $x \mapsto Ax$ се продължава до действие $f(x) \mapsto f(Ax)$ на $GL_n(k)$ върху пръстена $k[x] = k[x_1, \ldots, x_n]$ на полиномите на тези променливи. Крайните подгрупи G на $GL_n(k)$ ще наричаме накратко крайни матрични групи. Полиномът $f(x)$ е G-инвариантен, ако $f(Ax) = f(x)$ за $\forall A \in G$. Множеството $k[x_1, \ldots, x_n]^G$ на G-инвариантните полиноми $f(x)$ на $x =$

$\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$ с коефициенти от k е подпръстен на всичките полиноми $k[x_1, \dots, x_n]$. Полето k е подпръстен на $k[x_1, \dots, x_n]^G$, така че $k[x_1, \dots, x_n]^G$ е k-алгебра.

Лема 3.22. *Ако $G \subset GL_n(k)$ е крайна матрична група, а $f(x) \in k[x_1, \dots, x_n]$ е полином на n променливи, то $f(x)$ е цял над пръстена $k[x_1, \dots, x_n]^G$ на G-инвариантните полиноми на $x_1, \dots, x_n$.*

Доказателство: Да разгледаме произведението

$$F_{f(x)}(y) := \prod_{A \in G} [y - f(Ax)].$$

Понеже $f(Ax) \in k[x_1, \dots, x_n]$ за $\forall A \in G$, изразът $F_{f(x)}(y)$ е полином на y с коефициенти от $k[x_1, \dots, x_n]$. Продължаваме действието на G върху $k[x_1, \dots, x_n]$ до действие на G върху $k[x_1, \dots, x_n][y]$, което оставя на място y. Тогава образът на $F_{f(x)}(y)$ под действие на произволно $B \in G$ е

$$F_{f(x)}(y) = \prod_{A \in G} [y - f(ABx)] = \prod_{C \in G} [y - f(Cx)] = F_{f(x)}(y),$$

защото A пробягва групата G точно когато $C = AB$ пробягва G. Следователно полиномът $F_{f(x)}(y)$ е G-инвариантен и $F_{f(x)}(y) \in k[x_1, \dots, x_n]^G[y]$. Степента на $F_{f(x)}(y)$ относно y съвпада с реда $\mathrm{card}(G)$ на G. Старшият коефициент на $F_{f(x)}(y)$ е 1. Освен това, $y = f(x)$ е корен на $F_{f(x)}(y)$, защото $F_{f(x)}(y)$ има множител $y - f(E_n x) = y - f(x)$, където $E_n \in G$ единичната матрица. По определение, гореспоменатите свойства означават, че $f(x)$ е цял над $k[x_1, \dots, x_n]^G$, Q.E.D.

Твърдение 3.23. *Ако G е крайна матрична група над поле k, то пръстенът*

$$k[x_1, \dots, x_n]^G = k[f_1(x), \dots, f_m(x)]$$

на G-инвариантните полиноми се поражда като k-алгебра от краен брой хомогенни G-инвариантни полиноми $f_1(x), \dots, f_m(x)$.

Докаазтелство: Полето k е ньотеров пръстен. Полиномиалният пръстен $k[x_1, \dots, x_n]$ е крайнопородена k-алгебра, а множеството $k[x_1, \dots, x_n]^G$ на G-инвариантните полиноми е подпръстен на $k[x_1, \dots, x_n]$, съдържащ k. Твърдим, че

$$k[x_1, \dots, x_n] = k[x_1, \dots, x_n]^G[x_1, \dots, x_n].$$

Включването $k[x_1, \dots, x_n] \subseteq k[x_1, \dots, x_n]^G[x_1, \dots, x_n]$ следва от това, че константите от k са G-инвариантни полиноми, $k \subseteq k[x_1, \dots, x_n]^G$. Обратно, G-инвариантните полиноми $k[x_1, \dots, x_n]^G$ се съдържат в пръстена $k[x_1, \dots, x_n]$ на всички полиноми и $x_1, \dots, x_n \in k[x_1, \dots, x_n]$, така че $k[x_1, \dots, x_n]^G[x_1, \dots, x_n]$ се съдържа в пръстена $k[x_1, \dots, x_n]$. По този начин,

$$k[x_1, \dots, x_n] = k[x_1, \dots, x_n]^G[x_1, \dots, x_n]$$

се оказва крайнопородена $k[x_1, \dots x_n]^G$-алгебра. От Лема 3.22 следва, че $x_1, \dots, x_n$ са алгебрични над $k[x_1, \dots, x_n]^G$, така че $k[x_1, \dots, x_n] = k[x_1, \dots, x_n]^G[x_1, \dots, x_n]$ е крайнопороден $k[x_1, \dots, x_n]^G$-модул, съгласно Твърдение 3.21. Това дава възможност да приложим Твърдение 3.17 и да получим съществуването на полиноми $g_1(x), \dots, g_k(x) \in k[x_1, \dots, x_n]^G$, пораждащи

$$k[x_1, \dots, x_n]^G = k[g_1(x), \dots, g_k(x)]$$

като k-алгебра. Полином $h(x) = \sum_{i=0}^{d} h^{(i)}(x) \in k[x_1, \dots, x_n]$ с хомогенни компоненти $h^{(i)}(x) \in k[x_1, \dots, x_n]^{(i)}$ е G-инвариантен тогава и само тогава, когато

всяка от хомогенните му компоненти е G-инвариантна. По-точно, за $\forall A \in G$ образът $h^{(i)}(Ax) \in k[x_1, \ldots, x_n]$ на $h^{(i)}(x)$ е хомогенен полином на $x_1, \ldots, x_n$ от степен i. Затова равенството

$$\sum_{i=0}^{d} h^{(i)}(Ax) = h(Ax) = h(x) = \sum_{i=0}^{d} h^{(i)}(x)$$

се свежда до равенствата $h^{(i)}(Ax) = h^{(i)}(x)$ за $\forall 0 \leq i \leq d$ и доказва G-инвариант -ността на всички хомогенни компоненти $h^{(i)}(x)$ на G-инвариантен полином $h(x)$. Нека $f_1(x), \ldots, f_m(x)$ са G-инвариантните хомогенни компоненти на пораждащите $g_1(x), \ldots, g_k(x)$ на $k[x_1, \ldots, x_n]^G$ като k-алгебра. Представяйки всеки от полиномите $g_j(x)$ като сума на своите хомогенни компоненти получаваме включването $k[x_1, \ldots, x_n]^G = k[g_1(x), \ldots, g_k(x)] \subseteq k[f_1(x), \ldots, f_m(x)]$. Обратно, $k[f_1(x), \ldots, f_m(x)] \subseteq k[x_1, \ldots, x_n]^G$ следва от $f_1(x), \ldots, f_m(x) \in k[x_1, \ldots, x_n]^G$ и от факта, че $k[x_1, \ldots, x_n]^G$ е пръстен. Следователно, пръстенът на G-инвариантните полиноми $k[x_1, \ldots, x_n]^G = k[f_1(x), \ldots, f_m(x)]$ се опражда като k-алгебра от краен брой хомогенни G-инвариантни полиноми $f_1(x), \ldots, f_m(x) \in k[x_1, \ldots, x_n]^G$, Q.E.D.
За да изложим по-конкретна формулировка на Теоремата на Еми Ньотер, трябва да въведем така наречения оператор на Рейонлдс.

Лема-Определение 4. *Ако $G \subset GL_n(k)$ е крайна матрична група над поле k с характериситка* $\mathrm{char}(k) = 0$*, то изображението*

$$R_G : k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n],$$
$$R_G(f)(x) = \frac{1}{\mathrm{card}(G)} \sum_{A \in G} f(Ax)$$

е хомоморфизъм на $k[x_1, \ldots, x_n]^G$-модули

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

който трансформира хомогенните полиноми $h(x)$ от степен d в хомогенни полиноми $R_G(h)(x)$ от степен d и оставя на място $R_G(g)(x) = g(x)$ всеки G-инвариантен полином $g(x) \in k[x_1, \ldots, x_n]^G$.
Изображението R_G се нарича оператор на Рейнолдс на G.

Доказателство: Да отбележим, че изискването $\mathrm{char}(k) = 0$ е нужно, за да можем да делим на броя на елементите $\mathrm{card}(G)$ на крайната матрична група G, в определението на R_G. Образът $R_g(f)(x)$ на произволен полином $f(x) \in k[x_1, \ldots, x_n]$ е G-инвариантен, защото

$$R_G(f)(Bx) = \frac{1}{\mathrm{card}(G)} \sum_{A \in G} f(ABx) = \frac{1}{\mathrm{card}(G)} \sum_{C \in G} f(Cx) = f(x)$$

за всяко фиксирано $B \in G$. Ако $g(x) \in k[x_1, \ldots, x_n]^G$ е G-инвариантен полином, то $g(Ax) = g(x)$ за $\forall A \in G$, откъдето $R_G(g)(x) = \frac{1}{\mathrm{card}(G)} \mathrm{card}(G) g(x) = g(x)$. Ако $h(x) \in k[x_1, \ldots, x_n]^{(d)}$ е хомогенен полином от степен d, то за всички $A \in G$ полиномите $h(Ax) \in k[x_1, \ldots, x_n]^{(d)}$ са хомогенни и от същата степен d, така че $R_G(h)(x) \in k[x_1, \ldots, x_n]^{(d)}$ е хомогенен полином от степен d. За произволни $g_1(x), \ldots, g_m(x) \in k[x_1, \ldots, x_n]^G$ и $f_1(x), \ldots, f_m(x) \in k[x_1, \ldots, x_n]$ пресмятаме, че

$$R_G\left(\sum_{i=1}^{m} g_i f_i\right)(x) = \frac{1}{\mathrm{card}(G)} \sum_{A \in G} \left(\sum_{i=1}^{m} g_i f_i\right)(Ax) =$$
$$\frac{1}{\mathrm{card}(G)} \sum_{A \in G} \left(\sum_{i=1}^{m} g_i(Ax) f_i(Ax)\right) = \frac{1}{\mathrm{card}(G)} \sum_{A \in G} \left(\sum_{i=1}^{m} g_i(x) f_i(Ax)\right).$$

Разменяйки реда на сумиране получаваме

$$R_G\left(\sum_{i=1}^{m} g_i f_i\right)(x) = \sum_{i=1}^{m} g_i(x)\left[\frac{1}{\mathrm{card}(G)}\sum_{A\in G} f_i(Ax)\right] = \sum_{i=1}^{m} g_i(x) R_G(f_i)(x).$$

Следователно изображението $R_G : k[x_1,\ldots,x_n] \to k[x_1,\ldots,x_n]^G$ е хомоморфизъм на $k[x_1,\ldots,x_n]^G$-модули, Q.E.D.

Теорема 5. *Нека $G \subset GL_n(k)$ е крайна матрична група над поле k с характеристика* $\mathrm{char}(k) = 0$. *Тогава пръстенът на G-инвариантните полиноми*

$$k[x_1,\ldots,x_n]^G = k\left[R_G(x^\alpha)\,\middle|\, 1 \le |\alpha| = \sum_{i=1}^{m}\alpha_i \le \mathrm{card}(G)\right]$$

се поражда като k-алгебра от образите $R_G(x^\alpha)$ на мономите $x^\alpha = x_1^{\alpha_1}\ldots x_n^{\alpha_n}$ от степен $|\alpha| \le \mathrm{card}(G)$ под действие на оператора на Рейнолдс R_G на G.

Доказателство: Пръстенът $k[x_1,\ldots,x_n]^G$ на G-инвариантните полиноми се поражда като k-алгебра от всички мономи x^β, $\beta \in (\mathbb{Z}^{\ge 0})^n$. Наистина, ако $f(x) = \sum\limits_{\beta\in B} c_\beta x^\beta \in k[x_1,\ldots,x_n]^G$ е G-инвариантен полином, то

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

съгласно G-инвариантността на $c_\beta \in k$.
Твърдим, че за произволни променливи $z_1,\ldots,z_n$ и произволно естествено d е изпълнено

$$(z_1+\ldots+z_n)^d = \sum_{|\beta|=d}\frac{d!}{\beta_1!\ldots\beta_n!}z^\beta.$$

По-точно, $z_1^{\beta_1}$ се избира по

$$\left(\begin{array}{c} d \\ \beta_1 \end{array}\right) = \frac{d!}{\beta_1!(d-\beta_1)!}$$

начина от $(z_1+\ldots+z_n)^d$. При фиксирано $z_1^{\beta_1}$ избираме $z_2^{\beta_2}$ по

$$\left(\begin{array}{c} d-\beta_1 \\ \beta_2 \end{array}\right) = \frac{(d-\beta_1)!}{\beta_2!(d-\beta_1-\beta_2)!}$$

начина. Продължаваме по същия начин, като избираме $z_{n-1}^{\beta_{n-1}}$ по

$$\left(\begin{array}{c} d-\beta_1-\ldots-\beta_{n-2} \\ \beta_{n-1} \end{array}\right) = \frac{(d-\beta_1-\ldots-\beta_{n-2})!}{\beta_{n-1}!(d-\beta_1-\ldots-\beta_{n-1})!}$$

начина и накрая $z_n^{\beta_n}$ по

$$\left(\begin{array}{c} d-\beta_1-\ldots-\beta_{n-1} \\ \beta_n \end{array}\right) = \frac{(d-\beta_1-\ldots-\beta_{n-1})!}{\beta_n!(d-\beta_1-\ldots-\beta_n)!}$$

начина. Окончателно, броят на мономите $z^\beta = z_1^{\beta_1}\ldots z_n^{\beta_n}$ в $(z_1+\ldots+z_n)^d$ е

$$\left(\begin{array}{c} d \\ \beta_1 \end{array}\right)\left(\begin{array}{c} d-\beta_1 \\ \beta_2 \end{array}\right)\ldots\left(\begin{array}{c} d-\beta_1-\ldots-\beta_{n-1} \\ \beta_n \end{array}\right) = \frac{d!}{\beta_1!\ldots\beta_n!}.$$

Въвеждаме променливи $u = (u_1,\ldots,u_n)$. Представяме произволна матрица $A \in G \subset GL_n(k)$ като съвкупност от вектор-редове $A = \left(\begin{array}{c} a_1 \\ \ldots \\ a_n \end{array}\right)$, така че

$uAx = u_1a_1x + \ldots + u_na_nx$ за $x = \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix}$. Тогава

$$(uAx)^d \sum_{|\beta|=d} \frac{d!}{\beta_1! \ldots \beta_n!}(u_1a_1x)^{\beta_1} \ldots (u_na_nx)^{\beta_n} = \sum_{|\beta|=d} \frac{d!}{\beta_1! \ldots \beta_n!}u^\beta (Ax)^\beta.$$

Нека $\mathrm{card}(G) = m$ и $G = \{E_n = A_1, \ldots, A_m\}$. Разглеждаме множеството $M = \{uA_ix \,|\, 1 \leq i \leq m\}$. Действието $x \mapsto A_jx$ чрез $\forall A_j \in G$ индуцира действие $uA_ix \mapsto uA_iA_jx$ върху M чрез пермутации. Съответният хомоморфизъм на G в групата на взаимно-еднозначните изображения на M, може да се разглежда като реализация на G като подгрупа на симетричната група $\mathcal{G}_m$, съгласно Теоремата на Кейли. Нека $S_d := \sum\limits_{A\in G}(uAx)^d$ е d-тият степенен сбор на елементите на M. Тогава

$$S_d = \sum_{|\beta|=d} \frac{d!}{\beta_1! \ldots \beta_n!}u^\beta \left[\sum_{A\in G}(Ax)^\beta\right] = \sum_{|\beta|=d} \frac{d!}{\beta_1! \ldots \beta_n!}\mathrm{card}(G)u^\beta R_G(x^\beta).$$

Понеже S_d е симетрична функция на uA_ix за $1 \leq i \leq m$, съществува полином $F'(y_1, \ldots, y_m) \in k[y_1, \ldots, y_m]$, така че

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

където

$$\begin{aligned}
\sigma_1 &= \sum_{i=1}^{m} uA_ix, \\
\sigma_2 &= \sum_{1\leq i_1<i_2\leq m} (uA_{i_1}x)(uA_{i_2}x), \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\sigma_k &= \sum_{1\leq i_1<\ldots<i_k\leq m} (uA_{i_1}x)\ldots(uA_{i_k}x), \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\sigma_m &= (uA_1x)\ldots(uA_mx)
\end{aligned}$$

са елементарните симетрични полиноми на $uA_1x, \ldots, uA_mx$. Твърдим, че за всяко $1 \leq i \leq m$ съществува полином $H_i(y_1, \ldots, y_m) \in k[y_1, \ldots, y_m]$, така че i-тият елементарен симетричен полином

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

се представя като полином H_i на първите i степенни сборове $S_1, \ldots, S_i$ на $uA_1x, \ldots, uA_mx$. Тогава

$$S_d = F'(H_1(S_1), \ldots, H_m(S_1, \ldots, S_m)) = F(S_1, \ldots, S_m)$$

се оказва полином $F(y_1, \ldots, y_m) \in k[y_1, \ldots, y_m]$ на първите m степенни сборове $S_1, \ldots, S_m$ на $uA_1x, \ldots, uA_mx$. По-точно,

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

за $\forall d \in \mathbb{N}$, така че $R_G(x^\beta)$ с $|\beta| = d$ е полином на $R_G(x^\gamma)$, $1 \leq |\gamma| \leq m$, с коефициенти от k.

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

$$S_i - \sigma_1S_{i-1} + \ldots + (-1)^j\sigma_jS_{i-j} + \ldots + (-1)^{i-1}\sigma_{i-1}S_1 + (-1)^i\sigma_ii = 0$$

за $\forall 1 \leq i \leq m$. Над полето k с $\mathrm{char}(k) = 0$, можем да изразим

$$\sigma_i = \frac{(-1)^{i+1}}{i} \left[S_i - \sigma_1 S_{i-1} + \ldots + (-1)^j \sigma_j S_{i-j} + \ldots + (-1)^{i-1} \sigma_{i-1} S_1 \right]. \quad (3.1)$$

С индукция по $1 \leq i \leq m$, от (3.1) получаваме съществуването на $H_i(y_1, \ldots, y_i) \in k[y_1, \ldots, y_i]$ с $H_i(S_1, \ldots, S_i) = \sigma_i$, Q.E.D.