Глава 3

Въпрос 16: Крайно породени алгебри и модули над ньотеров пръстен

В настоящия въпорс са събрани някои предварителни сведения за доказателството на Теоремата на Хилберт за нулите. Междувременно, направената подготовка е използвана за предоставяне на още едно доказателство на Теоремата на Еми Ньотер за крайна породеност на пръстена $k[x_1, \ldots, x_n]^G$ от инвариантни полиноми на крайна матрична група $G \subset GL(n, k)$.

Определение 3.1. *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.

Примери 3.2. *(i) 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.*
(ii) Ако $G \subset GL(n, k)$ е крайна матрична група над поле k, а $k[x_1, \ldots, x_n]^G$ е пръстенът на G-инвариантните полиноми на $x_1, \ldots, x_n$ с коефициенти от k, то пръстенът $k[x_1, \ldots, x_n]$ на всички полиноми на $x_1, \ldots, x_n$ с коефициенти от k е $k[x_1, \ldots, x_n]^G$-алгебра.

Определение 3.3. *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.*

Определение 3.4. *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 3.5. *Идеалът I в комутативния пръстен с единица R се нарича прост, ако от $ab \in I$ за $a, b \in R$ следва, че $a \in I$ или $b \in I$.*

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, област на цялост е пръстен без делители на нулата. Непосредствено се вижда, че крайнопородената R-алгебра $S = R[a_1, \ldots, a_n]$ е област тогава и само тогава, когато идеалът I_A на тъждествата на A е прост. Поточно, ако $S = R[a_1, \ldots, a_n]$ е област и $fg \in I_A$ за $f, g \in R[x_1, \ldots, x_n]$, то $f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0_S$, откъдето $f(a_1, \ldots, a_n) = 0_S$ или $g(a_1, \ldots, a_n) = 0_S$. По този начин, $f \in I_A$ или $g \in I_A$ и идеалът $I_A \lhd R[x_1, \ldots, x_n]$ е прост. Обратно, ако $I_A \lhd R[x_1, \ldots, x_n]$ е прост идеал и $f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0_S$, то $fg \in I_A$ води до $f \in I_A$ или $g \in I_A$. В резултат, $f(a_1, \ldots, a_n) = 0_S$ или $g(a_1, \ldots, a_n) = 0_S$ и $S = R[a_1, \ldots, a_n]$ е област на цялост.
Преди да формулираме и докажем обобщен вариант на теоремата на Хилберт за базиса, да напомним, че 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 3.6. *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 $\{0_R\} = \langle 0_R \rangle \lhd R[x]$ е крайнопороден, така че остава да установим крайната породеност на произволен ненулев идеал $\{0_R\} \neq I \lhd R[x]$. За целта избираме редица от ненулеви полиноми $f_1, \ldots, f_i \in I$, 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.
Разглеждаме редицата $LC(f_1), \ldots, LC(f_i) \in R$ от старшите коефициенти на избраните полиноми и образуваме идеала $J \lhd R$, породен от тези $LC(f_j)$. Доколкото R е ньотеров пръстен, идеалът J е крайнопороден. С други думи, съществува естествено число $m \in \mathbb{N}$, така че

$$J = \langle LC(f_1), \ldots, LC(f_m) \rangle.$$

Твърдим, че първоначалният идеал I се поражда от полиномите $f_1, \ldots, f_m$, т.е.

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

Ако допуснем противното, то избраната редица от ненулеви полиноми съдържа $f_{m+1} \in I \setminus \langle f_1, \ldots, f_m \rangle$. По построение, $\deg(f_{m+1}) \geq \deg(f_i)$ за $\forall 1 \leq i \leq m$. От друга страна, старшият коефициент $LC(f_{m+1}) \in J$ се представя във вида

$$LC(f_{m+1}) = \sum_{i=1}^{m} LC(f_i) b_i$$

чрез подходящи $b_1, \ldots, b_m \in R$. В резултат,

$$g := \sum_{i=1}^{m} b_i x^{\deg(f_{m+1}) - \deg(f_i)} f_i$$

е полином на x със старши член

$$LT(g) = \left[\sum_{i=1}^{m} b_i LC(f_i)\right] x^{\deg(f_{m+1})} = LT(f_m).$$

Следователно разликата $f_{m+1} - g \in I$ е от степен $\deg(f_{m+1} - g) < \deg(f_{m+1})$ и съгласно избора на $f_{m+1} \in I \setminus \langle f_1, \ldots, f_m\rangle$ от минимална степен, имаме $f_{m+1} - g \in \langle f_1, \ldots, f_m\rangle$. Прибавяйки $g \in \langle f_1, \ldots, f_m\rangle$ получаваме $f_{m+1} \in \langle f_1, \ldots, f_m\rangle$. Противоречието установява, че $I = \langle f_1, \ldots, f_m\rangle$ е крайнопороден идеал, Q.E.D.

Следствие 3.7. *Ако $\varphi : R \to S$ е хомоморфизъм на комутативни пръстени с единица и R е нътеров пръстен, то образът $Im(\varphi) := \{\varphi(r) \,|\, r \in R\}$ на φ е нътеров пръстен.*

Доказателство: Трябва да докажем, че произволен идеал $I \lhd Im(\varphi)$ 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 нътеров, идеалът $\varphi^{-1}(I) \lhd R$ е крайнопороден, т.е. съществуват $r_1, \ldots, r_n \in \varphi^{-1}(I)$, така че

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

Твърдим, че

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

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 нътеров, Q.E.D.

Следствие 3.8. *Ако R е нътеров пръстен, то всяка крайнопородена R-алгебра $S = R[a_1, \ldots, a_n]$ е също нътеров 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 нътеров. Случаят $n = 1$ е доказан от Твърдение 3.6. Ако допуснем, че пръстенът $R[x_1, \ldots, x_{i-1}]$ е нътеров, то отново по Твърдение 3.6 получаваме, че и пръстенът $R[x_1, \ldots, x_{i-1}][x_i] = R[x_1, \ldots, x_i]$ е нътеров.
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 3.7 гарантира, че $Im(\pi_A) = R[a_1, \ldots, a_n] = S$ нътеров пръстен, щом пръстенът на полиномите $R[x_1, \ldots, x_n]$ е нътеров, Q.E.D.

Определение 3.9. *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 $r \in R$ и $m + N \in M/N$ 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 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 $I\triangleleft R$ 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 3.10. *Казваме, че M е крайнопороден R-модул, ако съществуват краен брой елементи $\mu_1,\ldots,\mu_n\in M$, така че*

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

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 3.7 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 3.11. *(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 3.11 (ii) чрез следното

Твърдение 3.12. *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 3.11 (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 $\mu_i + R\mu_n \in M/R\mu_n$, така че $\sum_{i=1}^{n-1} R(\mu_i + R\mu_n)$ е R-подмодул на фактормодула $M/R\mu_n$. 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

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

По индукционно предположение, подмодулът $(N + R\mu_n)/R\mu_n$ на $M/R\mu_n = R(\mu_1 + R\mu_n) + \ldots + R(\mu_{n-1} + R\mu_n)$ 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 3.11 (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 3.13. *Нека R е ньотеров комутативен пръстен с единица, $R[a_1, \ldots, a_n]$ 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 $b_ib_j \in R[a_1, \ldots, a_n]$, така че

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

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 3.8. Твърдим, че

$$R[a_1, \ldots, a_n] = S_ob_1 + \ldots + S_ob_m$$

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

$$S_ob_1 + \ldots + S_ob_m \subseteq Sb_1 + \ldots + Sb_m = R[a_1, \ldots, a_n],$$

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 3.12. 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 3.14. *Елементът a на R-алгебрата S се нарича цял над R, ако съществуват $r_1, \ldots, r_n \in R$, така че*

$$a^n + r_1 a^{n-1} + \ldots + r_{n-1} a + r_n = 0.$$

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

$$e_0 a^n + e_1 a^{n-1} + \ldots + e_{n-1} a + e_n = 0_E.$$

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.

Лема 3.15. *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 $a^n + r_1 a^{n-1} + \ldots + r_n = 0$ за някакви $r_1, \ldots, r_n \in R$, то

$$a^n = -r_1 a^{n-1} - \ldots - r_{n-1} a - r_n \in R.1_R + Ra + \ldots + Ra^{n-1} =: M_o.$$

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 $a^{k-1} = \sum_{i=1}^{n} s_i a^{n-i}$ за някакви $s_i \in R$, то

$$a^k = (s_1 a^{n-1} + s_2 a^{n-2} + \ldots + s_n)a =$$

$$s_1(-r_1 a^{n-1} - \ldots - r_{n-1} a - r_n) + s_2 a^{n-1} + \ldots + s_n a =$$

$$(s_2 - s_1 r_1)a^{n-1} + \ldots + (s_n - s_1 r_{n-1})a - s_1 r_n \in M_o.$$

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 3.16. *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 $s_1, \ldots_m \in S$ 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 $s_j \mu_i \in M$. 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 3.17. *Ако $S = R[a_1, \ldots, a_n]$ е крайнопородена R-алгебра и елементите $a_1, \ldots, a_n$ на 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 3.15 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 пръстена $R[a_1, \ldots, a_{n-1}] \ni r_1, \ldots, r_m$, 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 3.15. Прилагайки Лема 3.16 получаваме, че $R[a_1, \ldots, a_n]$ е крайнопороден R-модул, Q.E.D.

Определение 3.18. *Казваме, че R-алгебрата S е цяла над R, ако всеки елемент на S е цял над R.*

Лема 3.19. *За произволна крайна матрична група $G \subset GL(n, k)$, пръстенът $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле k е цяла алгебра относно подпръстена $k[x_1, \ldots, x_n]^G$ на G-инвариантните полиноми.*

Доказателство: За произволен полином $f \in k[x_1, \ldots, x_n]$ на $x_1, \ldots, x_n$ с коефициенти от k разглеждаме полинома

$$F(x, y) := \prod_{A \in G} [y - f(A^{-1}x)]$$

на y от степен $|G|$ със старши коефициент 1. За $A = E_n \in G$ множителят $y - f(E_n^{-1}x) = y - f(x)$ на $F(x, y)$ се анулира при полагане на $y = f$, така че $F(x, f) = 0 \in k[x_1, \ldots, x_n]$. Твърдим, че коефициентите на F като полином на y са G-инвариантни полиноми на $x_1, \ldots, x_n$. За целта да напомним, че $A^{-1}x$ е n-торка хомогенни линейни полиноми на $x_1, \ldots, x_n$ с коефициенти от k, така че $f(A^{-1}x) \in k[x_1, \ldots, x_n]$ за $\forall A \in G$. Следователно $F(x, y) \in k[x_1, \ldots, x_n][y]$. Действието на G върху $k[x_1, \ldots, x_n]$ се продължава до действие

$$G \times k[x_1, \ldots, x_n][y] \longrightarrow k[x_1, \ldots, x_n][y],$$
$$(A, H(x, y)) \mapsto H(A^{-1}x, y),$$

което изпълнява тъждеството

$$(H_1 H_2)(A^{-1}x, y) = H_1(A^{-1}x, y) H_2(A^{-1}x, y)$$

за произволни $H_1(x, y), H_2(x, y) \in k[x_1, \ldots, x_n][y]$. При това, един полином $H(x, y) = \sum_{i=0}^{n} H_i y^i$ е G-инвариантен елемент на $k[x_1, \ldots, x_n][y]$ тогава и само тогава, когато

$$\sum_{i=0}^{n} H_i(x) y^i = H(x) = H(A^{-1}x) = \sum_{i=0}^{n} H_i(A^{-1}x) y^i.$$

за всички $A \in G$. Последното равенство на полиноми от $k[x_1, \ldots, x_n][y]$ е равносилно на $H_i(x) = H_i(A^{-1}x)$ за всички $0 \leq i \leq n$. С други думи, G-инвариантните полиноми от $k[x_1, \ldots, x_n][y]$ образуват подпръстена $k[x_1, \ldots, x_n]^G[y]$ на $k[x_1, \ldots, x_n][y]$. Но за фиксирания полином $F(x, y) = \prod_{A \in G}(y - f(A^{-1}x)) \in k[x_1, \ldots, x_n][y]$ и за всяко $B \in G$ е в сила

$$F(B^{-1}x, y) = \prod_{A \in G} (y - f(A^{-1}B^{-1}x)) = \prod_{BA \in G} (y - f((BA)^{-1}x)) = F(x, y),$$

така че $F(x, y)$ е G-инвариантен и $F(x, y) \in k[x_1, \ldots, x_n]^G[y]$. По определение, това означава, че всяко $f \in k[x_1, \ldots, x_n]$ е цяло над $k[x_1, \ldots, x_n]^G$, Q.E.D.

Следствие 3.20. *Пръстенът $k[x_1, \ldots, x_n]^G$ на инвариантните полиноми на крайна матрична група $G \subset GL(n, k)$ над поле k е крайнопородена k-алгебра.*

Доказателство: Полето k е ньотеров пръстен. Пръстенът $k[x_1,\dots,x_n]$ на полиномите на $x_1,\dots,x_n$ с коефициенти от k е крайнопородена k-алгебра, а пръстенът $k[x_1,\dots,x_n]^G$ на G-инвариантните полиноми е подпръстен на $k[x_1,\dots,x_n]$, съдържащ k. Твърдим, че

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

се поражда от $x_1,\dots,x_n$ като $k[x_1,\dots,x_n]^G$-алгебра. Наистина, k е подпръстен на $k[x_1,\dots,x_n]^G$, така че

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

От своя страна, $k[x_1,\dots,x_n]^G$-алгебрата $k[x_1,\dots,x_n]^G[x_1,\dots,x_n]$ се състои от полиноми на $x_1,\dots,x_n$ с коефициенти от k, така че $k[x_1,\dots,x_n]^G[x_1,\dots,x_n] \subseteq k[x_1,\dots,x_n]$. Това дава съвпадението $k[x_1,\dots,x_n] = k[x_1,\dots,x_n]^G[x_1,\dots,x_n]$. Като частен случай от Лема 3.19 получаваме, че $x_1,\dots,x_n$ са цели над пръстена $k[x_1,\dots,x_n]^G$. По този начин, $k[x_1,\dots,x_n]$ се оказва крайнопороден $k[x_1,\dots,x_n]^G$-модул, съгласно Твърдение 3.17. Накрая, прилагаме Твърдение 3.13 и получаваме, че $k[x_1,\dots,x_n]^G = k[f_1,\dots,f_m]$ за подходящи $f_1,\dots,f_m \in k[x_1,\dots,x_n]^G$ е крайнопородена k-алгебра, Q.E.D.

Да напомним, че алгоритъмът на Бухбергер предоставя начин за намиране на базис на Грьобнер на полиномиален идеал $I \lhd k[x_1,\dots,x_n]$ по зададена система пораждащи за I. В редица случаи, в които не разполагаме с пораждащи на I, можем да разширим този идеал в полиномиален пръстен с повече променливи, така че полученият идеал J има явно зададени пораждащи и I е негов елиминационен идеал. Подходящо обобщение на Теоремата за елиминация гарантира, че сечението на базис на Грьобнер на J с първоначалния полиномиален пръстен е базис на Грьобнер на I.

В настоящия въпрос ще илюстрираме тази идеология с идеала $I_F \lhd k[y_1,\dots,y_m]$ на тъждествата на крайнопородена k-подалгебра $k[f_1,\dots,f_m]$, $F = \{f_1,\dots,f_m\}$ на $k[x_1,\dots,x_n]$.

Гореспоменатото обобщение на Теоремата за елиминация представлява съдържанието на следващата

Лема 3.21. *Нека $>$ е такава мономна наредба в $k[x_1,\dots,x_n,y_1,\dots,y_m]$, спрямо която $x^\alpha y^\beta > y^\gamma$ за всички $|\alpha| = \sum_{i=1}^n \alpha_i > 0$, а G е базис на Грьобнер на идеал $J \lhd k[x_1,\dots,x_n,y_1,\dots,y_m]$ относно $>$. Тогава*

$$G' := G \cap k[y_1,\dots,y_m]$$

е базис на Грьобнер на идеала

$$I := J \cap k[y_1,\dots,y_m] \lhd k[y_1,\dots,y_m]$$

относно ограничението на $>$ върху $k[y_1,\dots,y_m]$.

Доказателство: Преди всичко да отбележим, че всяка линейна наредба $>$ в множество M се ограничава до линейна наредба $>$ в произволно подмножество $N \subseteq M$. При това, ако $>$ е артинова наредба в M, то $>$ е артинова наредба в N. Накрая, ако $>$ е артинова линейна наредба на мономи от $k[x_1,\dots,x_n,y_1,\dots,y_m]$, в която е съгласувана с произведението, то ограничението на $>$ до мономите от $k[y_1,\dots,y_m]$ е също артинова линейна анредба, съгласувана с произведението. С други думи, всяка мономна наредба $>$ в $k[x_1,\dots,x_n,y_1,\dots,y_m]$ се ограничава до мономна наредба $>$ в $k[y_1,\dots,y_m]$. След евентуална преномерация на елементите на $G = \{g_1,\dots,g_t\}$ можем да считаме, че $G' = \{g_1,\dots,g_s\}$ за някакво естествено $1 \leq s \leq t$.

Първо ще установим, че $G' \subset I$ поражда идеала $I \lhd k[y_1,\dots,y_m]$. За целта използваме, че произволен полином $f \in I \subset J$ се дели без остатък на базиса на Грьобнер G на $J \lhd k[x_1,\dots,x_n,y_1,\dots,y_m]$. Нека $f = \sum_{i=1}^t g_i h_i$ с

$h_i \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ е резултатът от това деление. Твърдим, че ако текущото делимо $f'(y_1, \ldots, y_m)$ е полином на $y_1, \ldots, y_m$, то при осъществяване на същинско деление на f' с G, текущите частни $h_{s+1}, \ldots, h_t$ не получават ненулеви мономи, а някое от текущите частни $h_1, \ldots, h_s$ получава моном на $y_1, \ldots, y_m$. По този начин, ако разглежданото същинско деление в $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ е деление с $g_i \in k[y_1, \ldots, y_m]$ за някое $1 \leq i \leq s$, то и следващото текущо делимо $f'' := f' - \frac{LT(f')}{LT(g_i)} g_i$ е полином на $y_1, \ldots, y_m$. Наистина, същинско деление на f' с g_i се осъществява точно когато старшият член $LT(g_i)$ на g_i дели старшия член $LT(f')$ на f'. Доколкото $LT(f') \in k[y_1, \ldots, y_m]$, мономът $LT(g_i)$ не зависи от никое x_j и принадлежи на $k[y_1, \ldots, y_m]$. Това изисква $g_i \in k[y_1, \ldots, y_m]$, доколкото в противен случай g_i има моном, зависещ от x_j за някое $1 \leq j \leq n$ и този моном е по-голям от $LT(g_i) \in k[y_1, \ldots, y_m]$ съгласно предположението относно мономната наредба $>$. Следователно същинско деление на f' с g_i се осъществява само за $1 \leq i \leq s$ и към текущото частно h_i се прибавя монома $\frac{LT(f')}{LT(g_i)} \in k[y_1, \ldots, y_m]$. Прилагайки горното разсъждение върху всички стъпки на същинско деление получаваме, че делението на f с G в $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ дава $f = \sum_{i=1}^{s} g_i h_i$ с $h_i \in k[y_1, \ldots, y_m]$ и съвпада с делението на f с G' в $k[y_1, \ldots, y_m]$. В частност, $f \in \langle G' \rangle$ и $I = \langle G' \rangle$.

За да твърдим, че G' е базис на Грьобнер на $I = \langle G' \rangle \lhd k[y_1, \ldots, y_m]$, достатъчно е да проверим, че за произволни $1 \leq l \neq m \leq s$ остатъкът $\overline{S(g_l, g_m)}^{G'}$ на S-полинома $S(g_l, g_m)$ при деление с G' в $k[y_1, \ldots, y_m]$ е нулев. Наистина, $S(g_l, g_m) \in J \cap k[y_1, \ldots, y_m] = I$, така че делението на $S(g_l, g_m)$ с G в $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ съвпада с делението на $S(g_l, g_m)$ с G' в $k[y_1, \ldots, y_m]$ и има вида

$$S(g_l, g_m) = \sum_{i=1}^{s} g_i h_i^{(l,m)}$$

за подходящи полиноми $h_i^{(l,m)} \in k[y_1, \ldots, y_m]$. По този начин, $\overline{S(g_l, g_m)}^{G'} = 0 \in k[y_1, \ldots, y_m]$ се анулира и G' се оказва базис на Грьобнер на $I \lhd k[y_1, \ldots, y_m]$, Q.E.D.

Твърдение 3.22. *Нека k е поле, а $k[f_1, \ldots, f_m]$ е крайнопородена k-подалгебра на $k[x_1, \ldots, x_n]$. Да означим с $F = \{f_1, \ldots, f_m\}$ множеството на пораждащите на $k[f_1, \ldots, f_m]$ и да разгледаме идеала*

$$J_F = \langle f_1 - y_1, \ldots, f_m - y_m \rangle \lhd k[x_1, \ldots, x_n, y_1, \ldots, y_m].$$

Тогава идеалът на тъждествата

$$I_F = J_F \cap k[y_1, \ldots, y_m].$$

В частност, ако G е базис на Грьобнер на J_F относно мономна наредба $>$ в $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ с $x^\alpha y^\beta > y^\gamma$ за всички неотрицателни цели $\alpha_i, \beta_j, \gamma_j$ с $|\alpha| = \sum_{i=1}^{n} \alpha_i > 0$, то $G' := G \cap k[y_1, \ldots, y_m]$ е базис на Грьобнер на I_F относно индуцираната от $>$ мономна наредба в $k[y_1, \ldots, y_m]$.

Доказателство: Твърдим, че полином $p \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ принадлежи на J_F тогава и само тогава, когато $p(x_1, \ldots, x_n, f_1, \ldots, f_m) = 0 \in k[x_1, \ldots, x_n]$ е нулевият полином на $x_1, \ldots, x_n$. Наистина, ако $p \in J_F = \langle f_1 - y_1, \ldots, f_m - y_m \rangle$, то заместването на y_i с f_i за всички $1 \leq i \leq m$ анулира произволен пораждащ на J_F, а оттам и всички елементи на J_F. Обратно, нека $p(x_1, \ldots, x_n, f_1, \ldots, f_m) = 0 \in k[x_1, \ldots, x_n]$ за $p \in k[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Всеки моном y^β се представя във вида

$$y^\beta = y_1^{\beta_1} \ldots y_m^{\beta_m} = [f_1 - (f_1 - y_1)]^{\beta_1} \ldots [f_m - (f_m - y_m)]^{\beta_m} =$$

$$f_1^{\beta_1} \dots f_m^{\beta_m} + A_1(f_1 - y_1) + \dots + A_m(f_m - y_m)$$

с подходящи полиноми $A_1, \dots, A_m \in k[x_1, \dots, x_n, y_1, \dots, y_m]$. Следователно всеки моном на p има вида

$$a_{\alpha,\beta} x^\alpha y^\beta = a_{\alpha,\beta} x^\alpha f_1^{\beta_1} \dots f_m^{\beta_m} + A_1' x^\alpha (f_1 - y_1) + \dots + A_m' x^\alpha (f_m - y_m)$$

и сумата им

$$p(x_1, \dots, x_n, y_1, \dots, y_m) = p(x_1, \dots, x_n, f_1, \dots, f_m) + B_1(f_1 - y_1) + \dots + B_m(f_m - y_m)$$

за подходящи полиноми $B_1, \dots, B_m \in k[x_1, \dots, x_n, y_1, \dots, y_m]$. В частност, ако $p(x_1, \dots, x_n, f_1, \dots, f_m) = 0$, то

$$p(x_1, \dots, x_n, y_1, \dots, y_m) = B_1(f_1 - y_1) + \dots + B_m(f_m - y_m) \in J_F$$

Сега пресичайки с $k[y_1, \dots, y_m]$ получаваме, че полиномът $p \in k[y_1, \dots, y_m]$ принадлежи на $J_F \cap k[y_1, \dots, y_m]$ тогава и само тогава, когато $p(f_1, \dots, f_m) = 0 \in k[x_1, \dots, x_n]$. Последното условие е в сила точно когато $p \in I_F$ е от идеала на тъждествата на F, Q.E.D.