Polinoamele simetrice $s_1, \dots, s_n$ din Propoziția precedentă se numesc polinoamele simetrice fundamentale din $A[X_1, \dots, X_n]$.

Exemplu. Fie $f = X_1^2 + \dots + X_n^2 \in A[X_1, \dots, X_n]$, care este polinom simetric. Atunci

$$f = (X_1 + \dots + X_n)^2 - 2(X_1 X_2 + \dots + X_1 X_n + \dots + X_{n-1} X_n)$$

$= s_1^2 - 2 s_2$, deci f se scrie ca un polinom de (unele dintre) $s_1, \dots, s_n$.

Vom arăta că acest fapt are loc pt. orice polinom simetric f, și de aceea $s_1, \dots, s_n$ sunt numite polinoame simetrice fundamentale.

Avem nevoie de câteva pregătiri.

În primul rând, pe mulțimea monoamelor de forma $X_1^{i_1} \dots X_n^{i_n}$ (adică monoame unitare), unde $i_1, \dots, i_n \in \mathbb{N}$, introducem o relație $<$ definită astfel:

dacă $M = X_1^{i_1} \dots X_n^{i_n}$ și $N = X_1^{j_1} \dots X_n^{j_n}$, atunci

$M < N$ dacă există $1 \leq p \leq n$ astfel încât

$i_r = j_r$ pt. orice $1 \leq r < p$, și $i_p < j_p$.

[așadar $M < N$ dacă:

sau $i_1 < j_1$,

sau $i_1 = j_1$ și $i_2 < j_2$,

sau $i_1 = j_1$, $i_2 = j_2$ și $i_3 < j_3$,

– – – – – – –

sau $i_1 = j_1, \dots, i_{n-1} = j_{n-1}$ și $i_n < j_n$].

Atunci relaţia $\leq$ definită prin:

$$M \leq N \iff M < N \text{ sau } M = N,$$

este o relaţie de ordine pe mulţimea monoamelor (de acest tip) (Exerciţiu: verificaţi). În plus, este clar că ea este o ordine totală, adică pt. orice monoame M şi N avem $M \leq N$ sau $N \leq M$. [într-adevăr, păstrând notaţiile precedente pt. M şi N, dacă $i_r = j_r$ pt. orice $1 \leq r \leq n$, atunci $M = N$. Altfel, fie p cel mai mic pt. care $i_p \neq j_p$; atunci dacă $i_p < j_p$ avem $M < N$, iar dacă $i_p > j_p$ avem $M > N$].

Relaţia $\leq$ se numeşte <u>ordinea lexicografică</u> pe mulţimea monoamelor unitare (numele este clar inspirat de ordinea în care sunt aranjate într-un dicţionar cuvintele atunci când ordinea literelor este stabilită; în cazul de faţă pe postul literelor stau nedeterminatele, iar ordinea lor este $X_1, \dots, X_n$).

<u>Exemple</u>. În $A[X_1, X_2, X_3]$ avem

$$X_1^2 X_2 X_3 > X_1 X_2^5 X_3^4 \; ; \quad X_1 X_3 > X_2^2 X_3^3 \; ; \quad X_1 X_2^2 > X_1 X_2 X_3^5 .$$

<u>Lemă</u>. Fie M_1, M_2, N, N_1, N_2 monoame unitare. Atunci:

(i) $M_1 > M_2 \implies M_1 N > M_2 N$.

(ii) $M_1 > N_1,\ M_2 > N_2 \implies M_1 M_2 > N_1 N_2$.

<u>Dem.</u> (i) Fie $M_1 = X_1^{i_1} \dots X_n^{i_n}$, $M_2 = X_1^{j_1} \dots X_n^{j_n}$.

Cum $M_1 > M_2$, există $1 \le p \le n$ cu $i_p > j_p$ și $i_r = j_r$ pt. orice $1 \le r < p$.

Fie acum $N = X_1^{h_1} \dots X_n^{h_n}$. Atunci $M_1 N = X_1^{i_1+h_1} \dots X_n^{i_n+h_n}$ și $M_2 N = X_1^{j_1+h_1} \dots X_n^{j_n+h_n}$ și evident $i_p + h_p > j_p + h_p$ și $i_r + h_r = j_r + h_r$ pt. $1 \le r < p$.

Rezultă că $M_1 N > M_2 N$.

(ii)
$$\left.\begin{array}{l} M_1 > N_1 \xrightarrow[\text{folosim (i)}]{\cdot M_2} M_1 M_2 > N_1 M_2 \\ M_2 > N_2 \xrightarrow[\text{folosim (i)}]{N_1 \cdot} N_1 M_2 > N_1 N_2 \end{array}\right\} \Rightarrow M_1 M_2 > N_1 N_2.$$

Fie $f \in A[X_1, \dots, X_n]$ un polinom nenul. Știm că f este sumă de monoame, cu anumiți coeficienți. Dintre toate monoamele (considerate ca monoame unitare) care apar cu coeficienți nenuli în reprezentarea lui f există unul care este cel mai mare în ordinea lexicografică (deoarece aceasta este o ordine totală). Termenul corespunzător a $X_1^{i_1} \dots X_n^{i_n}$ din reprezentarea lui f se numește termenul principal al lui f.

<u>Exemplu</u>. Fie $f = 2X_1X_3 + 4X_1^2X_2 - 5X_2^3X_3^3 + 7X_1X_2X_3 \in \mathbb{Z}[X_1, X_2, X_3]$. Atunci termenul principal al lui f este $4X_1^2X_2$.

Corolar. Fie $f, g \in A[X_1, \dots, X_n]$ polinoame nenule, având termeni principali $a X_1^{i_1} \dots X_n^{i_n}$ și $b X_1^{j_1} \dots X_n^{j_n}$.
Dacă $ab \neq 0$, atunci termenul principal al lui fg este $ab X_1^{i_1+j_1} \dots X_n^{i_n+j_n}$ (adică produsul termenilor principali ai lui f și g).

Dem. Notăm $M_1 = X_1^{i_1} \dots X_n^{i_n}$ și $M_2 = X_1^{j_1} \dots X_n^{j_n}$.
Atunci $M_1 M_2 = X_1^{i_1+j_1} \dots X_n^{i_n+j_n}$ și acest monom apare cu coeficientul $ab \neq 0$ în reprezentarea lui fg.
Orice alt monom din reprezentarea lui fg se obține prin înmulțirea unui monom cN_1 (din reprezentarea lui f) cu un monom dN_2 (din reprezentarea lui g).
Atunci $M_1 \geq N_1$ și $M_2 \geq N_2$ și nu ambele sunt egalități.
Din Lemă $\Rightarrow M_1 M_2 > N_1 N_2$. (dacă ambele inegalități sunt stricte, direct din Lemă (ii); dacă $M_1 = N_1$ și $M_2 > N_2$, din Lemă (i) înmulțind $M_2 > N_2$ cu M_1; la fel pt. $M_1 > N_1$, $M_2 = N_2$).

Corolar. Fie $a_1, \dots, a_n \in \mathbb{N}$. Atunci termenul principal al polinomului $s_1^{a_1} \dots s_n^{a_n}$ este $X_1^{a_1+a_2+\dots+a_n} X_2^{a_2+\dots+a_n} \dots X_n^{a_n}$.

Dem. Termenul principal al lui s_1 este X_1. Din Corolarul precedent $\Rightarrow$ termenul principal al lui $s_1^{a_1}$ este $X_1^{a_1}$.
Apoi termenul principal al lui s_2 este $X_1 X_2$, deci termenul principal al lui $s_2^{a_2}$ este $X_1^{a_2} X_2^{a_2}$.
În general, pt. $1 \leq i \leq n$, termenul principal al lui s_i este $X_1 \dots X_i$, deci al lui $s_i^{a_i}$ este $X_1^{a_i} \dots X_i^{a_i}$.

Aplicând din nou Corolarul precedent $\Rightarrow$ termenul principal al lui $s_1^{a_1} s_2^{a_2} \dots s_n^{a_n}$ este

$$X_1^{a_1} \cdot (X_1^{a_2} X_2^{a_2}) \cdot \ldots \cdot (X_1^{a_i} X_2^{a_i} \ldots X_i^{a_i}) \cdot \ldots \cdot (X_1^{a_n} X_2^{a_n} \ldots X_n^{a_n}) =$$

$$= X_1^{a_1+a_2+\ldots+a_n} X_2^{a_2+\ldots+a_n} \ldots X_n^{a_n}.$$

<u>Lemă</u> Fie $f \in A[X_1, \ldots, X_n]$ un polinom simetric nenul. Fie $a X_1^{h_1} \ldots X_n^{h_n}$ termenul principal al lui f. Atunci

$h_1 \geq h_2 \geq \ldots \geq h_n$.

<u>Dem.</u> Presupunem prin absurd că există $1 \leq i < n$ cu $h_i < h_{i+1}$. Atunci schimbând între ele nedeterminatele X_i și X_{i+1} în f (adică luând $\sigma^*(f)$ unde $\sigma = (i\ i+1)$) obținem tot f, deoarece acesta este simetric. Rezultă că f conține și termenul

$a X_1^{h_1} \ldots X_{i-1}^{h_{i-1}} X_i^{h_{i+1}} X_{i+1}^{h_i} X_{i+2}^{h_{i+2}} \ldots X_n^{h_n}$ și în plus

$X_1^{h_1} \ldots X_{i-1}^{h_{i-1}} X_i^{h_{i+1}} X_{i+1}^{h_i} X_{i+2}^{h_{i+2}} \ldots X_n^{h_n} > X_1^{h_1} \ldots X_{i-1}^{h_{i-1}} X_i^{h_i} X_{i+1}^{h_{i+1}} X_{i+2}^{h_{i+2}} \ldots X_n^{h_n}$,

contradicție.

<u>Observație cheie</u>. Fie $M = X_1^{h_1} \ldots X_n^{h_n}$ un monom cu $h_1 \geq \ldots \geq h_n$. Atunci există un număr finit de monoame de forma $X_1^{t_1} \ldots X_n^{t_n}$ cu $t_1 \geq \ldots \geq t_n$ mai mici ca M în ordinea lexicografică.

Într-adevăr $M > X_1^{t_1}\dots X_n^{t_n}$ implică $t_1 \le i_1$, deci t_1 poate lua doar un nr. finit de valori. Cum $t_2,\dots,t_n \le t_1$, și acestea pot lua doar un nr. finit de valori, deci există un număr finit de astfel de monoame $X_1^{t_1}\dots X_n^{t_n}$.

Putem demonstra acum rezultatul enunțat.

<u>Teorema fundamentală a polinoamelor simetrice</u>:

Fie A un inel comutativ, $n \in \mathbb{N}$, $n \ge 2$ și $f \in A[X_1,\dots,X_n]$ un polinom simetric. Atunci există un unic polinom $g \in A[X_1,\dots,X_n]$ astfel încât

$$f = g(s_1,\dots,s_n).$$

[Altfel spus: orice polinom simetric se scrie în mod unic ca un polinom de polinoame simetrice fundamentale]

<u>Demonstrație</u>.

<u>Existența</u>: Dacă $f=0$, este clar, luăm $g=0$.

Presupunem acum că $f \ne 0$ și fie $aX_1^{h_1}\dots X_n^{h_n}$ termenul principal al lui f. Am arătat că $h_1 \ge \dots \ge h_n$. Atunci polinomul $a s_1^{h_1-h_2} s_2^{h_2-h_3}\dots s_{n-1}^{h_{n-1}-h_n} s_n^{h_n}$ are termenul principal $a X_1^{h_1-h_2+h_2-h_3+\dots+h_{n-1}-h_n+h_n} X_2^{h_2-h_3+\dots+h_{n-1}-h_n+h_n}\dots X_{n-1}^{h_{n-1}-h_n+h_n} X_n^{h_n}$

$$= a X_1^{h_1} X_2^{h_2}\dots X_n^{h_n} \text{ (dintr-un Corolar precedent)},$$

adică același termen principal ca f. Rezultă că polinomul simetric $f - a s_1^{h_1-h_2} s_2^{h_2-h_3}\dots s_{n-1}^{h_{n-1}-h_n} s_n^{h_n}$ sau este 0, sau are termen principal de forma

$b X_1^{j_1}\dots X_n^{j_n}$, unde $j_1 \geq \dots \geq j_n$ și $X_1^{j_1}\dots X_n^{j_n} < X_1^{k_1}\dots X_n^{k_n}$.

În primul caz $f = a s_1^{k_1-k_2} s_2^{k_2-k_3}\dots s_n^{k_n}$, gata! În al doilea considerăm polinomul simetric $f - a s_1^{k_1-k_2}\dots s_n^{k_n} - b s_1^{j_1-j_2}\dots s_n^{j_n}$, care este sau 0, sau are termen principal de forma $c X_1^{i_1}\dots X_n^{i_n}$ cu $i_1 \geq \dots \geq i_n$ și $X_1^{i_1}\dots X_n^{i_n} < X_1^{j_1}\dots X_n^{j_n}$.

În primul caz obținem $f = a s_1^{k_1-k_2}\dots s_n^{k_n} + b s_1^{j_1-j_2}\dots s_n^{j_n}$, gata! În al doilea continuăm similar, scăzând din polinomul la care am ajuns un polinom de $s_1, \dots, s_n$ în așa fel încât să obținem sau 0, sau un polinom simetric de termen principal mai mic. După un număr finit de pași obținem cu siguranță 0, altfel am găsi un șir infinit $X_1^{k_1}\dots X_n^{k_n} > X_1^{j_1}\dots X_n^{j_n} > X_1^{i_1}\dots X_n^{i_n} > \dots$ (toate de forma $X_1^{t_1}\dots X_n^{t_n}$ cu $t_1 \geq \dots \geq t_n$, deoarece sunt monoame corespunzând termenilor principali din niște polinoame simetrice nenule) și ținând cont de observația cheie precedentă, obținem o contradicție. Așadar în acest proces recurent obținem la un moment dat 0, iar aceasta îl scrie pe f ca un polinom de $s_1, \dots, s_n$.

<u>Unicitatea</u>. Presupunem că $f = g(s_1, \dots, s_n) = h(s_1, \dots, s_n)$, unde $g, h \in A[X_1, \dots, X_n]$. Arătăm că $g = h$. Dacă nu ar fi așa, notăm $u = g - h \neq 0$. Avem $u(s_1, \dots, s_n) = 0$. Scriem $u = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} X_1^{i_1}\dots X_n^{i_n}$, deci avem $\sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} s_1^{i_1}\dots s_n^{i_n} = 0$. Să observăm că

termenii principali din $s_1^{i_1} \ldots s_n^{i_n}$ și $s_1^{j_1} \ldots s_n^{j_n}$ sunt egali dacă și numai dacă $i_1 = j_1, \ldots, i_n = j_n$; într-adevăr, aceștia sunt $X_1^{i_1+\ldots+i_n} X_2^{i_2+\ldots+i_n} \ldots X_n^{i_n}$, respectiv $X_1^{j_1+\ldots+j_n} X_2^{j_2+\ldots+j_n} \ldots X_n^{j_n}$, iar

$$\left.\begin{array}{c} i_1+\ldots+i_n = j_1+\ldots+j_n \\ i_2+\ldots+i_n = j_2+\ldots+j_n \\ \ldots\ldots\ldots \\ i_n = j_n \end{array}\right| \Rightarrow i_1 = j_1, i_2 = j_2, \ldots, i_n = j_n$$

Așadar polinoamele $s_1^{i_1} \ldots s_n^{i_n}$ (cele cu $a_{i_1 \ldots i_n} \neq 0$) au termeni principali distincți, și atunci cel mai mare dintre acești termeni principali nu se poate reduce cu niciun alt termen din suma $\sum_{i_1, \ldots, i_n} a_{i_1 \ldots i_n} s_1^{i_1} \ldots s_n^{i_n}$. Rezultă că această sumă e $\neq 0$, contradicție.

Rămâne că $g = h$, gata!

<u>Observație</u>. Fie $f \in A[X_1, \ldots, X_n]$ polinom simetric și $f = f_0 + \ldots + f_m$ reprezentarea lui ca sumă de polinoame omogene (f_d = componenta omogenă de grad d). Am văzut că $f_0, \ldots, f_m$ sunt toate polinoame simetrice. Metoda de reprezentare a lui f ca polinom de polinoame simetrice fundamentale, descrisă în demonstrația teoremei, partea de existență, se poate aplica direct pt. f, dar se poate aplica separat pt. $f_0, \ldots, f_m$, obținându-se prin sumare reprezentarea lui f.

1p 59

Avantajul lucrului cu polinoame simetrice omogene este că pe parcursul algoritmului lucrăm numai cu polinoame omogene de același grad cu cel inițial (Se vede de ce acesta este un avantaj în exemplul de mai jos).

Exemplu. Fie $f = X_1^3X_2 + X_1X_2^3 + X_1^3X_3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3 \in \mathbb{Z}[X_1, X_2, X_3]$.

Vrem să scriem f ca polinom de s_1, s_2, s_3.

Metoda 1. (urmând strict algoritmul din demonstrația teoremei). Termenul principal al lui f este $X_1^3X_2 = X_1^3X_2^1X_3^0$.

Știm că $s_1^{3-1}s_2^{1-0}s_3^0 = s_1^2s_2$ are același termen principal.

Calculăm $s_1^2s_2 = (X_1+X_2+X_3)^2(X_1X_2+X_1X_3+X_2X_3)$ $\underset{=}{\text{calcule}}$

$$= X_1^3X_2 + X_1X_2^3 + X_1^3X_3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3$$
$$+ 2X_1^2X_2^2 + 2X_1^2X_3^2 + 2X_2^2X_3^2 + 5X_1^2X_2X_3 + 5X_1X_2^2X_3 + 5X_1X_2X_3^2$$

Atunci $f - s_1^2s_2 = -2X_1^2X_2^2 - 2X_1^2X_3^2 - 2X_2^2X_3^2 - 5X_1^2X_2X_3 - 5X_1X_2^2X_3 - 5X_1X_2X_3^2$,

care are termenul principal $-2X_1^2X_2^2$.

Acum $-2s_1^{2-2}s_2^2 = -2s_2^2$ are același termen principal.

Cum $s_2^2 = (X_1X_2 + X_1X_3 + X_2X_3)^2$

$$= X_1^2X_2^2 + X_1^2X_3^2 + X_2^2X_3^2 + 2X_1^2X_2X_3 + 2X_1X_2^2X_3 + 2X_1X_2X_3^2,$$

obținem că $f - s_1^2s_2 + 2s_2^2 = -X_1^2X_2X_3 - X_1X_2^2X_3 - X_1X_2X_3^2$, care are termenul principal $-X_1^2X_2X_3$. Același termen principal îl are și $-s_1^{2-1}s_2^{1-1}s_3^1 = -s_1s_3$. Dar $s_1s_3 = (X_1+X_2+X_3)X_1X_2X_3 =$

$= X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2$ și atunci $f - s_1^2s_2 + 2s_2^2 + s_1s_3 = 0$.

Rezultă că $f = s_1^2s_2 - 2s_2^2 - s_1s_3$.

~~[illegible]~~ ip 60

<u>Metoda 2</u>. (a coeficienților nedeterminați). Aici folosim că f e omogen de grad 4. Știm (din dem. teoremei) că de-a lungul procedurii vor apărea doar polinoame simetrice omogene tot de grad 4. Cum termenul principal al lui f este $X_1^3 X_2$, ceilalți termeni principali mai mici decât acesta și având tot grad 4 sunt $X_1^2 X_2^2$ și $X_1^2 X_2 X_3$ cu anumiți coeficienți. ~~(ținem cont că~~ (ținem cont că dacă $X_1^{i_1} X_2^{i_2} X_3^{i_3}$ e termen principal într-un polinom simetric, atunci $i_1 \geq i_2 \geq i_3$). Dar termenul principal $X_1^3 X_2$ produce (în algoritmul din teoremă) $s_1^2 s_2$, termenul principal $X_1^2 X_2^2$ produce s_2^2, cu un coeficient a deocamdată necunoscut, iar $X_1^2 X_2 X_3$ produce $s_1 s_3$, cu un coeficient b. Așadar știm că

$$f = s_1^2 s_2 + a s_2^2 + b s_1 s_3$$ pt. niște $a, b \in \mathbb{Z}$ pe care trebuie să-i determinăm. O metodă simplă de a-i găsi pe a, b (coeficienții nedeterminați) este să dăm valori lui X_1, X_2, X_3 ($\Leftrightarrow$ să evaluăm funcțiile polinomiale în niște valori convenabile). Procedăm astfel

X_1	X_2	X_3	s_1	s_2	s_3	f
1	1	0	2	1	0	2
1	1	1	3	3	1	6

$\Rightarrow 2 = 4 + a \Rightarrow a = -2$

$\Rightarrow 6 = 27 + 9a + 3b \Rightarrow$

$\Rightarrow 3b = -21 + 18 \Rightarrow b = -1$

obținem $f = s_1^2 s_2 - 2 s_2^2 - s_1 s_3$.