CURSUL 6: INELE DE POLINOAME DE MAI MULTE VARIABILE. POLINOAME SIMETRICE

G. MINCU

1. INELE DE POLINOAME DE MAI MULTE VARIABILE

Definiţia 1. Fie R un inel comutativ şi unitar. Inelul de polinoame de mai multe variabile cu coeficienţi în R se defineşte inductiv astfel: $R[X_1, X_2, \dots, X_{n+1}] = R[X_1, X_2, \dots, X_n][X_{n+1}]$.

Observaţia 2. Elementele lui $R[X_1, X_2, \dots, X_{n+1}]$ se scriu în mod unic sub forma

$$\sum_{i=0}^{r} P_i X_{n+1}^i$$

cu $r \in \mathbb{N}$ şi $P_i \in R[X_1, X_2, \dots, X_n]$.

Observaţia 3. Elementele lui $R[X_1, X_2, \dots, X_n]$ se scriu în mod unic sub forma

$$\sum_{i_1, i_2, \dots, i_n = 0}^{r_1, r_2, \dots, r_n} a_{i_1, i_2, \dots, i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n},$$

cu $r_1, r_2, \dots r_n \in \mathbb{N}$ şi $a_{i_1, i_2, \dots, i_n} \in R$.

Notaţie: Vom nota polinoamele din $R[X_1, X_2, \dots, X_n]$ fie prescurtat (de exemplu, f), fie punând în evidenţă variabilele (de exemplu, $f(X_1, X_2, \dots, X_n)$), în funcţie de necesităţile de moment.

Definiţia 4. Un polinom de forma $aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n} \in R[X_1, X_2, \dots, X_n]$ se numeşte **monom**.

Definiţia 5. Prin **gradul** monomului

$$aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n} \in R[X_1, X_2, \dots, X_n] \setminus \{0\}$$

înţelegem numărul natural $i_1 + i_2 + \dots + i_n$.

Definiţia 6. Prin **gradul** polinomului $f \in R[X_1, X_2, \dots, X_n] \setminus \{0\}$ înţelegem cel mai mare dintre gradele termenilor lui f. Considerăm că gradul polinomului nul este $-\infty$.

Vom nota gradul polinomului $f \in R[X_1, X_2, \ldots, X_n]$ cu grad f.

Observăm în acest punct că maniera în care am definit gradul pentru polinoamele din $R[X_1, X_2, \ldots, X_n]$ prezintă o ambiguitate: grad f în noua accepţie diferă de gradul lui $f \in R[X_1, X_2, \ldots, X_{n-1}][X_n]$ aşa cum a fost el definit la prezentarea polinoamelor de o variabilă. Pentru a înlătura această ambiguitate, constatăm următoarele: Mulţumită proprietăţii de universalitate a inelului de polinoame în mai multe variabile (pe care o prezentăm mai jos), pentru orice partiţie $\{i_1, i_2, \ldots, i_r\} \cup \{j_1, j_2, \ldots, j_s\}$ a mulţimii $\{1, 2, \ldots, n\}$ există un izomorfism canonic

$$R[X_1, X_2, \ldots, X_n] \xrightarrow{\sim} R[X_{i_1}, X_{i_2}, \ldots, X_{i_r}][X_{j_1}, X_{j_2}, \ldots, X_{j_s}].$$

Definiţia pe care am dat-o pentru grad face însă ca acest izomorfism **să nu păstreze gradele!** De aceea, vom nota gradul polinomului f privit ca element din $R[X_{i_1}, X_{i_2}, \ldots, X_{i_r}][X_{j_1}, X_{j_2}, \ldots, X_{j_s}]$ cu $\mathrm{grad}_{X_{j_1}, X_{j_2}, \ldots, X_{j_s}} f$, pentru a-l deosebi de gradul lui f privit ca element din $R[X_1, X_2, \ldots, X_n]$ (pe care l-am notat deja cu grad f). În această lumină, dacă $n \geq 2$, gradul polinomului $f \in R[X_1, X_2, \ldots, X_{n-1}][X_n]$ va fi notat $\mathrm{grad}_{X_n} f$.

Definiţia 7. Cu notaţiile de mai sus, $\mathrm{grad}_{X_{j_1}, X_{j_2}, \ldots, X_{j_s}} f$ se numeşte **gradul polinomului** $f \in R[X_1, X_2, \ldots, X_n]$ **în raport cu variabilele** $X_{j_1}, X_{j_2}, \ldots, X_{j_s}$.

Propoziţia 8. Dacă $f, g \in R[X_1, X_2, \ldots, X_n]$, atunci
a) $\mathrm{grad}(f + g) \leq \max\{\mathrm{grad}\ f, \mathrm{grad}\ g\}$
b) $\mathrm{grad}(fg) \leq \mathrm{grad}\ f + \mathrm{grad}\ g$.
Dacă, în plus, R este domeniu de integritate, atunci
b') $\mathrm{grad}(fg) = \mathrm{grad}\ f + \mathrm{grad}\ g$.

Definiţia 9. Polinomul $f \in R[X_1, X_2, \ldots, X_n]$ se numeşte **omogen** dacă toţi termenii săi au acelaşi grad.

Definiţia 10. Dat fiind polinomul

$$f = \sum_{i_1, i_2, \ldots, i_n = 0}^{r_1, r_2, \ldots, r_n} a_{i_1, i_2, \ldots, i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n} \in R[X_1, X_2, \ldots, X_n],$$

polinomul

$$f_d = \sum_{i_1 + i_2 + \cdots + i_n = d} a_{i_1, i_2, \ldots, i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$$

se numeşte **componenta omogenă de grad** d a lui f.

Observaţia 11. Orice polinom $f \in R[X_1, X_2, \ldots, X_n]$ se scrie în mod unic ca sumă de componente omogene.

Propoziţia 12. Fie R un inel comutativ şi unitar şi $f \in R[X_1, X_2, \dots, X_n]$. Atunci:
i) f este nilpotent dacă şi numai dacă toţi coeficienţii săi sunt nilpotenţi.
ii) f este inversabil dacă şi numai dacă termenul său liber este inversabil, iar toţi ceilalţi coeficienţi ai săi sunt nilpotenţi.
iii) f este idempotent dacă şi numai dacă este element idempotent al lui R.
iv) f este divizor al lui zero dacă şi numai dacă există $a \in R \setminus \{0\}$ astfel încât $af = 0$.

Observaţia 13. Fie R un inel şi $n \in \mathbb{N}^*$. Funcţia $j : R \to R[X_1, X_2, \dots, X_n]$, $j(a) = a$ este un morfism injectiv de inele. El se numeşte **injecţia** (sau **incluziunea**) **canonică** a lui R în $R[X_1, X_2, \dots, X_n]$.

Proprietatea de universalitate a inelului de polinoame în mai multe nedeterminate. Fie R un inel comutativ şi unitar, $n \in \mathbb{N}^*$ şi j injecţia canonică a lui R în $R[X_1, X_2, \dots, X_n]$. Atunci, pentru orice morfism de inele comutative $f : R \to S$ şi orice $s_1, s_2, \dots, s_n \in S$ există un unic morfism de inele $u : R[X_1, X_2, \dots, X_n] \to S$ astfel încât $f = u \circ j$ şi $u(X_i) = s_i$ pentru orice $i \in \{1, 2, \dots, n\}$.

Definiţia 14. Prin **valoarea polinomului**

$$f = \sum_{i_1, i_2, \dots, i_n = 0}^{r_1, r_2, \dots, r_n} a_{i_1, i_2, \dots, i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$$

în $(t_1, t_2, \dots, t_n) \in R^n$ înţelegem elementul (notat $f(t_1, t_2, \dots, t_n)$)

$$\sum_{i_1, i_2, \dots, i_n = 0}^{r_1, r_2, \dots, r_n} a_{i_1, i_2, \dots, i_n} t_1^{i_1} t_2^{i_2} \dots t_n^{i_n} \in R.$$

Definiţia 15. Prin **funcţia polinomială asociată lui** $f \in R[X_1, X_2, \dots, X_n]$ înţelegem funcţia $\widetilde{f} : R^n \to R$, $\widetilde{f}(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n)$.

2. POLINOAME SIMETRICE

Fie $f \in R[X_1, X_2, \dots, X_n]$ şi $\sigma \in S_n$. **Vom nota** cu $\overline{\sigma} f$ polinomul $f(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)}) \in R[X_1, X_2, \dots, X_n]$.

Observaţia 16. Pentru orice $\sigma, \tau \in S_n$ şi orice $f, g \in R[X_1, X_2, \dots, X_n]$ au loc relaţiile:
(i) $(\overline{\sigma} \cdot \overline{\tau}) f = \overline{\sigma}(\overline{\tau} f)$.
(ii) $\overline{\sigma}(f + g) = \overline{\sigma} f + \overline{\sigma} g$.
(iii) $\overline{\sigma}(fg) = (\overline{\sigma} f) \cdot (\overline{\sigma} g)$.

Definiţia 17. Polinomul $f \in R[X_1, X_2, \dots, X_n]$ se numeşte **simetric** dacă pentru orice $\sigma \in S_n$ avem $\overline{\sigma} f = f$.

Observaţia 18. Conform observaţiei 16 (i), polinomul $f \in R[X_1, X_2, \dots, X_n]$ este simetric dacă şi numai dacă avem $\overline{\tau} f = f$ pentru orice transpoziţie $\tau \in S_n$.

Observaţia 19. Mai mult, întrucât $S_n = \langle (1,2), (1,3), \dots, (1,n) \rangle$, polinomul $f \in R[X_1, X_2, \dots, X_n]$ este simetric dacă şi numai dacă avem $\overline{(1,j)} f = f$ pentru orice $j \in \{2, 3, \dots, n\}$.

Propoziţia 20. Mulţimea polinoamelor simetrice din $R[X_1, X_2, \dots, X_n]$ este un subinel al lui $R[X_1, X_2, \dots, X_n]$.

Propoziţia 21. Următoarele polinoame din $R[X_1, X_2, \dots, X_n]$ sunt simetrice:

$s_1 = X_1 + X_2 + \cdots + X_n$,
$s_2 = X_1X_2 + X_1X_2 + \cdots + X_1X_n + \cdots + X_{n-1}X_n$,
....
$s_k = X_1X_2 \dots X_k + X_1X_2 \dots X_{k-1}X_{k+1} \cdots + X_{n-k+1}X_{n-k+2} \dots X_n$,
....
$s_n = X_1X_2 \dots X_n$.

Definiţia 22. Polinoamele din propoziţia anterioară se numesc **polinoamele simetrice fundamentale în nedeterminatele** $X_1, X_2, \dots, X_n$.

Pe mulţimea $\mathcal{M}$ a monoamelor din $R[X_1, X_2, \dots, X_n]$, considerăm relaţia $M_1 \sim M_2$ dacă şi numai dacă M_1 şi M_2 au aceeaşi parte literală. Constatăm (temă!) că $\sim$ este o relaţie de echivalenţă. Notăm $\mathcal{N} = \mathcal{M}/\sim$. În mod nonstandard, vom folosi pentru clasa monomului $aX_1^{i_1}X_2^{i_2} \dots X_n^{i_n}$ tot notaţia $aX_1^{i_1}X_2^{i_2} \dots X_n^{i_n}$. Introducem pe $\mathcal{N}$ următoarea relaţie: $aX_1^{i_1}X_2^{i_2} \dots X_n^{i_n} < bX_1^{j_1}X_2^{j_2} \dots X_n^{j_n}$ dacă şi numai dacă există $r \in \{1, 2, \dots, n\}$ astfel încât $i_1 = j_1$, $i_2 = j_2, \dots, i_{r-1} = j_{r-1}$ şi $i_r < j_r$. Constatăm (temă!) că ,,$<$" este o relaţie de ordine strictă.

Definiţia 23. Relaţia de ordine asociată relaţiei ,,$<$" prezentate mai sus se numeşte relaţia de **ordine lexicografică** pe $\mathcal{N}$.

Observaţia 24. Relaţia de ordine lexicografică este o relaţie de ordine totală pe $\mathcal{N}$.

Definiţia 25. Fie $f \in R[X_1, X_2, \dots, X_n] \setminus \{0\}$. Monomul din scrierea lui f care este maxim în ordinea lexicografică se numeşte **termenul principal** al lui f

Vom nota termenul principal al lui $f \in R[X_1, X_2, \dots, X_n] \setminus \{0\}$ cu $\mathrm{lt}(f)$.

Lema 26. Fie M_1, M_2 monoame nenule din $R[X_1, X_2, \ldots, X_n]$ astfel încât $M_1 < M_2$. Atunci:
a) Pentru orice monom nenul $N \in R[X_1, X_2, \ldots, X_n]$ avem $M_1 N < M_2 N$.
b) Dacă $N_1, N_2 \in R[X_1, X_2, \ldots, X_n]$ sunt monoame nenule astfel încât $N_1 < N_2$, atunci $M_1 N_1 < M_2 N_2$.

Corolarul 27. Dacă $f, g \in R[X_1, X_2, \ldots, X_n] \setminus \{0\}$, atunci $\operatorname{lt}(fg) = (\operatorname{lt} f) \cdot (\operatorname{lt} g)$.

Lema 28. Dacă $f \in R[X_1, X_2, \ldots, X_n] \setminus \{0\}$ este polinom simetric, iar $\operatorname{lt} f = aX_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$, atunci $i_1 \geq i_2 \geq \ldots \geq i_n$.

Teorema fundamentală a polinoamelor simetrice. Pentru orice polinom simetric $f \in R[X_1, X_2, \ldots, X_n]$ există şi este unic $g \in R[Y_1, Y_2, \ldots, Y_n]$ astfel încât $f = g(s_1, s_2, \ldots, s_n)$, unde $s_1, s_2, \ldots, s_n$ sunt polinoamele simetrice fundamentale în variabilele $X_1, X_2, \ldots, X_n$.

O formulare mai puţin precisă dar mai uşor de reţinut pentru această teoremă este:

Teorema fundamentală a polinoamelor simetrice. Orice polinom simetric se scrie în mod unic ca polinom de polinoamele simetrice fundamentale.

Demonstraţie:
Existenţa: Notăm cu $\mathcal{T}$ mulţimea acelor polinoame simetrice din $R[X_1, X_2, \ldots, X_n]$ care nu se scriu ca polinom de polinoamele simetrice fundamentale. Presupunem că $\mathcal{T}$ este nevidă; fie $f \in \mathcal{T}$. Scriind f ca sumă de componente omogene, constatăm că măcar una dintre aceste componente, fie ea f_q, se află în $\mathcal{T}$. Notăm cu $\mathcal{T}_q$ submulţimea (nevidă!) a lui $\mathcal{T}$ alcătuită din polinoamele omogene de grad q din $\mathcal{T}$, iar cu $\mathcal{L}$ mulţimea termenilor principali ai polinoamelor din $\mathcal{T}_q$. Atunci, $\mathcal{L}/\sim$ este o submulţime nevidă şi finită a mulţimii total ordonate $\mathcal{N}$, deci ea admite un cel mai mic element. Fie $M = aX_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ acest element, iar $g \in \mathcal{T}_q$ un polinom care are termenul principal egal cu M. Atunci, $g - as_1^{i_1 - i_2} s_2^{i_2 - i_3} \ldots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n}$ se află în $\mathcal{T}_q$ şi are termenul principal mai mic decât M, contradicţie.
Unicitatea: Presupunem că polinomul simetric $f \in R[X_1, X_2, \ldots, X_n]$ se scrie în două moduri distincte, $g(s_1, s_2, \ldots, s_n)$ şi $h(s_1, s_2, \ldots, s_n)$ ca polinom de polinoamele simetrice fundamentale. Atunci, $g(s_1, s_2, \ldots, s_n) - h(s_1, s_2, \ldots, s_n) = 0$ cu $g - h \neq 0$. Dacă $g - h = \sum a_{i_1, i_2, \ldots, i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$,

obţinem

$$\sum a_{i_1,i_2,\ldots,i_n} s_1^{i_1} s_2^{i_2} \ldots s_n^{i_n} = 0. \tag{1}$$

Cum $\mathrm{lt}(a_{i_1,i_2,\ldots,i_n} s_1^{i_1} s_2^{i_2} \ldots s_n^{i_n}) = a_{i_1,i_2,\ldots,i_n} X_1^{i_1+i_2+\ldots+i_n} X_2^{i_2+i_3+\ldots+i_n} \ldots X_n^{i_n}$, constatăm că aceşti termeni principali sunt distincţi doi câte doi. Prin urmare, cel mai mare în ordine lexicografică dintre aceşti termeni maximi nu se va reduce, ceea ce arată că relaţia (1) este contradictorie. $\square$

Algoritm de scriere a polinoamelor simetrice ca polinoame de polinoamele simetrice fundamentale:

Input: Polionomul simetric $f \in R[X_1, X_2, \ldots, X_n]$

$g = 0$;
while ($f \neq 0$) do
{
$aX_1^{i_1} X_2^{i_2} \ldots X_n^{i_n} = \mathrm{lt}\ f$;
$f = f - a s_1^{i_1-i_2} s_2^{i_2-i_3} \ldots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}$;
$g = g + aY_1^{i_1-i_2} Y_2^{i_2-i_3} \ldots Y_{n-1}^{i_{n-1}-i_n} Y_n^{i_n}$
}

Output: Polinomul $g \in R[Y_1, Y_2, \ldots, Y_n]$ cu proprietatea $f = g(s_1, s_2, \ldots, s_n)$.

Este uşor de constatat că polinoamele $p_t = X_1^t + X_2^t + \cdots + X_n^t \in R[X_1, X_2, \ldots, X_n]$ sunt simetrice. Ele au următoarele proprietăţi calculatorii interesante:

Formulele lui Newton.
(i) Pentru $k > n$, $p_k - p_{k-1}s_1 + p_{k-2}s_2 - \cdots + (-1)^n p_{k-n} s_n = 0$.
(ii) Pentru $k \leq n$, $p_k - p_{k-1}s_1 + p_{k-2}s_2 - \cdots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0$.
Demonstraţie: (i) Din relaţiile $X_i^n - s_1 X_i^{n-1} + \cdots + (-1)^{n-1} s_{n-1} X_i + (-1)^n s_n = 0$, $1 \leq i \leq n$, obţinem că $X_i^k - s_1 X_i^{k-1} + \cdots + (-1)^{n-1} s_{n-1} X_i^{k-n+1} + (-1)^n s_n X_i^{k-n} = 0$ pentru orice $k > n$. Sumând aceste relaţii obţinem relaţia dorită.
(ii) Pentru $k = n$, formula se obţine cu calculele de la punctul (i). Pentru $k < n$, arătăm mai întâi că dacă un polinom $f \in R[X_1, \ldots, X_n]$ este omogen de grad $q < n$ şi are proprietatea că atunci când dăm valoarea zero la oricare $n - q$ dintre nedeterminatele $X_1, \ldots, X_n$, polinomul (în celelalte q nedeterminate) care rezultă se anulează, atunci $f = 0$. Într-adevăr, dacă f ar fi nenul, el s-ar scrie ca o sumă de termeni nenuli de

forma $aX_{i_1}^{k_1}\cdots X_{i_s}^{k_s}$ cu $k_j \geq 1$ pentru orice $1 \leq j \leq s$ şi $k_1+\ldots+k_s = q$. De aici rezultă în particular că $s \leq q$. Alegând un astfel de termen şi făcând X_i zero pentru orice $i \notin \{i_1,\ldots,i_s\}$, obţinem un polinom nenul, contradicţie.

Considerăm acum polinomul simetric $f(X_1,\ldots,X_n) = p_k - s_1p_{k-1} + \cdots + (-1)^{k-1}s_{k-1}p_1 + (-1)^k ks_k$ pentru $k < n$. Avem că f este polinom omogen de grad k. Dar $f(X_1,\ldots,X_k,0,\ldots 0) = p'_k - s'_1p'_{k-1} + \cdots + (-1)^{k-1}s'_{k-1}p'_1 + (-1)^k ks'_k$, unde $s'_j = s_j(X_1,\ldots,X_k,0,\ldots 0)$ şi $p'_j = p_j(X_1,\ldots,X_k,0,\ldots 0)$. Cum $s'_1,\ldots,s'_k$ sunt polinoamele simetrice fundamentale în nedeterminatele $X_1,\ldots,X_k$, rezultă din cazul $k = n$ considerat la început că avem $f(X_1,\ldots,X_k,0,\ldots 0) = 0$. Cum f este polinom simetric, obţinem că polinomul care rezultă atunci când dăm valoarea zero la oricare $n-k$ dintre nedeterminatele $X_1,\ldots,X_n$ este nul. Aceasta arată că $f = 0$.

Bibliografie

[1] C. Băeţica, S. Dăscălescu, C. Boboc, G. Mincu, *Probleme de algebră*, Ed. Universităţii din Bucureşti, 2006.
[2] T. Dumitrescu, *Algebra*, Ed. Universităţii din Bucureşti, 2006.
[3] I. D. Ion, N. Radu, *Algebra*, Ed. Universităţii din Bucureşti, 1981.
[4] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei*, Ed. Academiei, Bucureşti, 1986.