Notations. A sera un anneau commutatif unitaire, $\mathbb{K}$ un corps.
$n \in \mathbb{N}$, $n \geq 2$ et pour $i \in \mathbb{N}^n$, $i = (i_1, \dots, i_n)$, on note $|i| = \sum_{j=1}^{n} i_j$.

I POLYNÔMES À n INDÉTERMINÉES

1 L'algèbre $A[X_1, \dots, X_n]$

Déf 1: On appelle polynôme à n indéterminées sur A toute famille presque nulle d'éléments de A indexées par $\mathbb{N}^n$.
On écrit alors $P = (a_i)_{i \in \mathbb{N}^n}$ un tel polynôme. ([RDO], 6.7.1)
On note, pour $k \in [\![1,n]\!]$, X_k le polynôme défini par :
$(X_k)_i = 1$ si $i = (0, \dots, 0, \underset{k}{1}, 0, \dots, 0)$ et $(X_k)_i = 0$ sinon.
L'ensemble des polynômes à n indéterminées à coefficients dans A est noté $A[X_1, \dots, X_n]$.

Déf 2: Soient $P = (a_i)_{i \in \mathbb{N}^n}$, $Q = (b_i)_{i \in \mathbb{N}^n} \in A[X_1, \dots, X_n]$ et $\lambda \in A$.
On définit une addition : $P + Q = (a_i + b_i)_{i \in \mathbb{N}^n}$
une multiplication : $PQ = \left(\sum_{k+l=i} a_k b_l\right)_{i \in \mathbb{N}^n}$
une multiplication par un scalaire : $\lambda P = (\lambda a_i)_{i \in \mathbb{N}^n}$. ([RDO], 6.7.2 et 3)

Thm 3. Muni de ces opérations, $A[X_1, \dots, X_n]$ est une A-algèbre commutative. ([RDO], 6.7.3)

Thm 4:
Dans $A[X_1, \dots, X_n]$, tout polynôme peut s'exprimer d'une et une seule façon comme combinaison linéaire de la famille $(X_1^{i_1} \dots X_n^{i_n})_{(i_1, \dots, i_n) \in \mathbb{N}^n}$.
Les coefficients de la combinaison linéaire sont ceux du polynôme. ([RDO], 6.7.5)

Rq 5: On abandonne alors la notation $P = (a_i)_{i \in \mathbb{N}^n}$, au profit de $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n}$.

Prop 6: Propriété universelle ([SOB], p. 171)
Soit R une A-algèbre et $(x_1, \dots, x_n) \in R^n$.
Alors il existe un morphisme de A-algèbres $\Phi : A[X_1, \dots, X_n] \to R$, tel que $\forall i \in [\![1,n]\!]$, $\Phi(X_i) = x_i$.

Thm 7: Isomorphisme canonique ([RDO], 6.7.6)

$$\Phi : \left| \begin{array}{ccc} A[X_1, \dots, X_n] & \longrightarrow & (A[X_1, \dots, X_{n-1}])[X_n] \\ \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} & \longmapsto & \sum_{i_n=0}^{\infty} \left(\sum_{(i_1, \dots, i_{n-1}) \in \mathbb{N}^{n-1}} a_i X_1^{i_1} \dots X_{n-1}^{i_{n-1}} \right) X_n^{i_n} \end{array} \right.$$

est un isomorphisme de A-algèbres.

Ex 8: Le déterminant est un polynôme à plusieurs indéterminées.
De façon plus générale, les coefficients du polynôme caractéristique sont des polynômes à plusieurs indéterminées.

2 Degré et Polynômes homogènes ([RDO], 6.7.7-8, 6.8.1-3)

Déf 9: Degré partiel
Soit $q \in [\![1,n]\!]$, $P \in A[X_1, \dots, X_n]$. On appelle degré partiel de P en X_q le degré de ce polynôme comme élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$.
On le note $\deg_{X_q}(P)$.

Prop 10:
Soient $P, Q \in A[X_1, \dots, X_n]$, $q \in [\![1,n]\!]$.
On a : $\deg_{X_q}(P+Q) \leq \max\{\deg_{X_q}(P), \deg_{X_q}(Q)\}$
$\deg_{X_q}(PQ) \leq \deg_{X_q}(P) + \deg_{X_q}(Q)$ (avec égalité si A intègre).

Déf 11: Degré total
Soit $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$.
Si $P \neq 0$, on appelle degré total de P l'entier :
$\deg(P) = \max\{|i| \mid i \in \mathbb{N}^n, a_i \neq 0\}$
Si $P = 0$, on convient : $\deg(P) = -\infty$.

Prop 12:
Soient $P, Q \in A[X_1, \dots, X_n]$.
On a : $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$,
$\deg(PQ) \leq \deg(P) + \deg(Q)$ (avec égalité si A intègre).

Ex 13: Si $P = XYZ - X^2 + Y$, $\deg(P) = 3$, $\deg_X(P) = 2$ et $\deg_Y(P) = \deg_Z(P) = 1$.

Déf 14: Homogénéité.
Soit $p \in \mathbb{N}$; $P \in A[X_1, \dots, X_n]$ est p-homogène $\Leftrightarrow (|i| \neq p \Rightarrow a_i = 0)$.

Ex 15: $X^2 + XY$ est 2-homogène.

Prop 16: Si P est p-homogène et Q q-homogène, PQ est $(p+q)$-homogène.

Terminologie des polynômes homogènes de degré ≤ 2 :
- degré 0 : constantes
- degré 1 : formes linéaires
- degré 2 : formes quadratiques

Prop 17:
On note M_k l'ensemble des polynômes k-homogènes de $A[X_1,\dots,X_n]$.
Soit $P \in A[X_1,\dots,X_n]$, P s'écrit de manière unique $P = \sum_{k\in\mathbb{N}} P_k$ comme somme d'éléments de M_k.

Thm 18: Molien ([LEI], p. 95) DÉVELOPPEMENT N°1.
Soit G un sous-groupe fini de $GL_n(\mathbb{C})$, $(e_1,\dots,e_n)$ une base de $\mathbb{C}^n$.
Pour $g : e_i \mapsto \sum_{j=1}^n u_{ji} e_j$, $g \in G$, on définit $\tau_g : \begin{array}{l} \mathbb{C}[X_1,\dots,X_n] \to \mathbb{C}[X_1,\dots,X_n] \\ P(X_1,\dots,X_n) \mapsto P\left(\sum_{j=1}^n u_{j1}e_j,\dots,\sum_{j=1}^n u_{jn}e_j\right) \end{array}$
Alors $\tau_{g|A_k} \in \mathrm{Aut}(A_k)$ et pour cette action, on note $a_k(G) = \dim(A_k^G)$.
On a alors : $\frac{1}{\#G}\sum_{g\in G} \frac{1}{\det(\mathrm{Id}-gZ)} = \sum_{k=0}^{\infty} a_k(G) Z^k$ dans $\mathbb{C}[[Z]]$.

Déf 19: Polynôme dérivé partiel
On appelle polynôme dérivé partiel de $P \in A[X_1,\dots,X_n]$ selon X_q, le polynôme dérivé de P comme élément de $A[X_1,\dots,X_{q-1},X_{q+1},\dots,X_n][X_q]$. On le note $\partial P/\partial X_q$.

Thm 20: Euler
Soit K corps commutatif de caractéristique nulle, $P \in K[X_1,\dots,X_n]$.
On a : P est p-homogène $\Leftrightarrow \sum_{q=1}^n X_q \frac{\partial P}{\partial X_q} = pP$.

3 Propriétés arithmétiques ([RDO], 6.9)

Prop 21:
Si A est intègre, alors $A[X_1,\dots,X_n]$ est intègre
Si A est factoriel, alors $A[X_1,\dots,X_n]$ est factoriel.

C-Ex 22: Si $n \geq 2$, $K[X_1,\dots,X_n]$ n'est pas principal, car (X_1,X_2) ne l'est pas.

Conséquences de la factorialité de $A[X_1,\dots,X_n]$:
→ Existence d'une décomposition unique en produit de polynômes irréductibles non-associés.
→ Existence du PGCD et du PPCM
→ Le théorème de Gauss y est valide (mais pas Bezout : $UX_1+VX_2=1$ est impossible : évaluer en $X_1=0$ et $X_2=0$).

Prop 23:
Soit $A \in K[X_1,\dots,X_n]$, $B \in K[X_1,\dots,X_{n-1}]$.
On a : $X_n - B$ divise $A \Leftrightarrow A(X_1,\dots,X_{n-1},B(X_1,\dots,X_{n-1})) = 0$.

Ex 24: Dans $\mathbb{Q}[X,Y,Z]$, $X+Y+Z$ divise $X^3+Y^3+Z^3+mXYZ \Leftrightarrow m=-3$.

Cor 25:
$A \in K[X_1,\dots,X_n]$ est divisible par $\prod_{1\leq i<j\leq n}(X_i-X_j)$
$\Leftrightarrow \forall 1\leq i<j\leq n$, A est divisible par (X_i-X_j).

II FONCTIONS POLYNÔMES

1 Définition & Prolongement des identités

Déf 26: ([RDO], 6.7.9)
Pour $P = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1,\dots,i_n} X_1^{i_1}\dots X_n^{i_n} \in A[X_1,\dots,X_n]$, on définit $\tilde{P} : \begin{array}{l} A^n \mapsto A \\ (x_1,\dots,x_n) \to \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1,\dots,i_n} x_1^{i_1}\dots x_n^{i_n} \end{array}$.
$\tilde{P}$ est appelée fonction polynôme associée.

Lem 27: ([RDO], 6.7.9)
On suppose A intègre infini.
Soient $(A_i)_{1\leq i\leq n}$ des sous-ensembles infinis de A, $P \in A[X_1,\dots,X_n]$.
Si $P \neq 0$, alors il existe une infinité de points de $\prod_{i=1}^n A_i$ en lesquels $\tilde{P}$ prend une valeur non-nulle.

Thm 28: ([RDO], 6.7.9)
Si A est intègre infini,
Alors $\tilde{\Psi} : P \mapsto \tilde{P}$ est un isomorphisme de $A[X_1,\dots,X_n]$ sur l'algèbre des fonctions polynomiales de n variables sur A.

Rq 29: Dans ce cas, on peut faire l'abus d'écriture $P = \tilde{P}$.

Déf 30: ([GOB], p. 172)
Une identité entre m polynômes $F_1,\dots,F_m$ de $A[X_1,\dots,X_n]$ est une égalité de la forme $G(F_1(X_1,\dots,X_n),\dots,F_m(X_1,\dots,X_n)) = 0$,
où $G(Y_1,\dots,Y_m) \in A[Y_1,\dots,Y_m]$

Prop 31: Prolongement des identités ([GOB], p. 173)
On suppose A intègre de cardinal infini.
Soient $P_1,\dots,P_m \in A[X_1,\dots,X_n]$, puis pour $j \in [\![1,m]\!]$, $V(P_j) = \{(x_1,\dots,x_n) \in A^n \mid P_j(x_1,\dots,x_n) = 0\}$
Soient $F_1, F_2 \in A[X_1,\dots,X_n]$ tels que :
$$\forall (x_1,\dots,x_n) \in A \setminus \left(\bigcup_{j=1}^m V(P_j)\right),\ F_1(x_1,\dots,x_n) = F_2(x_1,\dots,x_n).$$
Alors $F_1 = F_2$.

App 32: Soit $M, N \in \mathcal{M}_d(K)$, alors $\chi_{MN} = \chi_{NM}$. ([GOB], p. 173)

2 Sur des corps finis ([SER], p. 13-14)

Dans cette sous-partie, on pose $q = p^r$, où p est premier et $r \in \mathbb{N}^*$.

Thm 33: Chevalley-Warning DÉVELOPPEMENT N°2
Soient $P_1,\dots,P_s \in \mathbb{F}_q[X_1,\dots,X_n]$ tels que $\sum_{i=1}^s \deg(P_i) < n$;
On note $V = \{(x_1,\dots,x_n) \in \mathbb{F}_q^n \mid \forall i \in [\![1,s]\!],\ P_i(x_1,\dots,x_n) = 0\}$.
On a : $\#V \equiv 0 \ [\mathrm{mod}\ p]$.

Cor 34:
Si on suppose de plus que les $P_1, \dots, P_s$ sont sans terme constant, Alors ils ont un zéro commun non-trivial.

App 35:
Toute forme quadratique d'au moins 3 variables sur $\mathbb{F}_q$ a un zéro non trivial.

C-Ex 36: C'est faux en 2 variables : dans $\mathbb{F}_2$, $x^2+xy+y^2=0 \Rightarrow (x,y)=(0,0)$
C'est faux dans $\mathbb{Q}$: $x^2+y^2+z^2=0 \Rightarrow (x,y,z)=(0,0,0)$.

3 Sur les corps $\mathbb{R}$ et $\mathbb{C}$

Dans cette sous-partie, K désigne $\mathbb{R}$ ou $\mathbb{C}$.

Prop 37: ([GOB], p. 173)
Soient $F_1, F_2 \in K[X_1, \dots, X_n]$.
On suppose que $\tilde{F}_1$ et $\tilde{F}_2$ coïncident sur un ouvert non-vide de K^n.
Alors $F_1 = F_2$.

App 38: Théorème de Cayley-Hamilton
Notons $\mathcal{D}_n'(K)$ l'ensemble des matrices diagonalisables à valeurs propres distinctes dans $\mathcal{M}_n(K)$. $\mathcal{D}_n'(K)$ est ouvert.
L'identité $\chi_M(M) = 0$, vraie sur $\mathcal{D}_n'(K)$ se prolonge sur $\mathcal{M}_n(K)$.

III POLYNÔMES SYMÉTRIQUES ([RDO], 6.10)

1 Définition & Relation coefficients-racines.

Déf 39:
Le groupe $\mathfrak{S}_n$ agit sur $A[X_1, \dots, X_n]$ via $\tau : \left| \begin{array}{ccc} A[X_1,\dots,X_n] & \longrightarrow & A[X_1,\dots,X_n] \\ P(X_1,\dots,X_n) & \longmapsto & P(X_{\tau(1)},\dots,X_{\tau(n)}) \end{array} \right.$,
où $\tau \in \mathfrak{S}_n$.
$P \in A[X_1, \dots, X_n]$ est dit symétrique $\Leftrightarrow \forall \tau \in \mathfrak{S}_n$, $\tau(P) = P$.

Déf 40: Polynômes symétriques élémentaires.
Dans $A[X_1, \dots, X_n]$, les n polynômes σ_k ($k \in [\![1, n]\!]$) définis par :

$$\sigma_k = \sum_{1 \le i_1 < \dots < i_k \le n} X_{i_1} \dots X_{i_k}$$

sont symétriques ; on les appelle polynômes symétriques élémentaires.
Pour $k \in [\![1, n]\!]$, σ_k est k-homogène.

Prop 41:
Soit $P = \prod_{i=1}^{n} (Y - X_i) \in A[X_1, \dots, X_n, Y]$.
On a : $P = Y^n + \sum_{k=1}^{n} (-1)^k \sigma_k(X_1, \dots, X_n) Y^{n-k}$.

Rq 42: On retrouve alors la relation coefficients-racines dans $A[Y]$.

2 Structure des polynômes symétriques.

Déf 43: Poids
* On appelle poids du monôme $X_1^{i_1} \dots X_n^{i_n}$ l'entier $\sum_{k=1}^{n} k i_k$.
* Soit $P = \sum_{(i_1,\dots,i_n) \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$, $P \neq 0$.
On définit le poids de P par : $\pi(P) = \max \left\{ \sum_{k=1}^{n} k i_k \,\middle|\, (i_1, \dots, i_n) \in \mathbb{N}^n,\ a_i \neq 0 \right\}$.
Si $P = 0$, on convient $\pi(P) = -\infty$.

Prop 44: Ordre
Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique.
P a même degré partiel par rapport à chacune de ses indéterminées.
Ce degré partiel est appelé ordre de P, et noté $\omega(P)$.

Thm 45: Théorème de structure
Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique de poids π et d'ordre ω.
Il existe un unique polynôme $Q \in A[Y_1, \dots, Y_n]$, tel que :

$$P(X_1, \dots, X_n) = Q(\sigma_1, \dots, \sigma_n).$$

De plus, ce polynôme Q est de poids π et d'ordre ω.

Algorithme pour déterminer Q :
Soit $P \in A[X_1, \dots, X_n]$ symétrique, non-nul, et homogène : $P = \sum_{|i|=p} a_i X_1^{i_1} \dots X_n^{i_n}$.
Soit $k = (k_1, \dots, k_n)$ le plus grand (pour l'ordre lexicographique) n-uplet tel que $a_k \neq 0$, on note $k = \deglex(P)$.
Par l'absurde, on peut montrer $k_1 \geq \dots \geq k_n$.
On pose $R = P - a_k \sigma_1^{k_1 - k_2} \sigma_2^{k_2 - k_3} \dots \sigma_{n-1}^{k_{n-1} - k_n} \sigma_n^{k_n}$.
On vérifie que R est symétrique homogène.
De plus, on a deux cas :
* Soit $R = 0$, et le problème est réglé.
* Soit $R \neq 0$, et on montre que $\deglex(R) < \deglex(P)$.
Dans ce cas, on réitère le procédé sur R.

Il est manifeste qu'en un nombre fini d'opérations, le polynôme trouvé est nul puisque la suite des degrés pour l'ordre lexicographique décroît strictement.
Ainsi, l'algorithme termine en un temps fini.

Références :

[RDO] : E. Ramis - C. Deschamps - J. Odoux, Cours de mathématiques spéciales, Algèbre 1, 2e édition.

[LEI] : Éric Leichtnam, Mathématiques, Polytechnique ENS, Algèbre & Géométrie

[GOB] : Rémi Goblot, Algèbre commutative, 2e édition.

[SER] : Jean-Pierre Serre, Cours d'arithmétique, 4e édition.