MAT4111

Premier semestre — 2020–2021

Fiche 1: Compléments sur les anneaux (1ère partie)

Polynômes en n indéterminées

1. *Fonctions polynomiales.* Soient k un corps infini et $n \in \mathbb{N}^*$.

(a) Soient $I_1, \dots, I_n$ des parties infinies de k. Montrer que si $P \in k[X_1,...,X_n]$ vérifie $P(x_1,...,x_n) = 0$ pour tout $(x_1,...,x_n) \in \prod_{i=1}^n I_i$, alors $P = 0$.

(b) Montrer que k^n n'est pas une réunion finie d'hypersurfaces.

(c) Soient $A, B \in M_n(k)$ deux matrices de taille n à coefficient dans k. On souhaite montrer que AB et BA ont le même polynôme caractéristique. Étant donné $\ell \in \{0, \dots, n-1\}$, on note f_ℓ le coefficient de X^ℓ dans la différence $(\chi_{AB} - \chi_{BA})(X)$, où $A \in M_n(k)$ est fixée. En particulier, f_ℓ est une fonction polynomiale en les coefficients $(b_{i,j})$ de B. On note $F_\ell \in k[X_{ij} : 1 \leq i, j \leq n]$ son polynôme associé.

(i) Montrer que si B est inversible, alors $\chi_{AB} = \chi_{BA}$ et donc $f_\ell = 0$.

(ii) En déduire la nullité du produit $F_\ell \det \in k[X_{ij} : 1 \leq i, j \leq n]$ pour tout $\ell \in \{0, \dots, n-1\}$.

(iii) Conclure.

2. *Non-intégrité des fonctions polynomiales à coefficients dans un corps fini.* Soit k un corps fini de cardinalité q. En particulier k est l'ensemble des racines du polynôme $X^q - X$. Soit $\varphi : k[X_1, \dots, X_n] \to F(k^n, k)$ le morphisme associant à un polynôme la fonction polynomiale correspondante.

(a) Montrer que $\ker(\varphi) = (X_1^q - X_1, \dots, X_n^q - X_n)$.

(b) Montrer que φ est surjective.

3. *Ensemble algébrique réduit à un point.* Soit A un anneau commutatif. Montrer que pour tout $(a_1, \dots, a_n) \in A^n$, l'idéal des polynômes de $A[X_1, \dots, X_n]$ qui s'annulent en $(a_1, \dots, a_n)$ est $(X_1 - a_1, \dots, X_n - a_n)$. Cet idéal est-il maximal ?

⋆ **4.** *Déterminant circulant.* Une permutation $\sigma \in \mathbb{S}_n$ est dite *cyclique* si elle appartient au sous-groupe engendré par le n-cycle $(1, \dots, n)$. Soit $M \in M_n(\mathbb{C}[X_1, \dots, X_n])$ telle que $M_{i,j} = X_{\sigma^{i-1}(j)}$ pour tous $i, j \in \{1, \dots, n\}$, où $\sigma \in \mathbb{S}_n$ est l'unique permutation cyclique telle que $\sigma(1) = n$. On pose $f = \sum_{\ell=0}^{n-1} X_{\ell+1} T^\ell \in \mathbb{C}[X_1, \dots, X_n][T]$. On se propose de calculer le déterminant de M.

(a) On définit $J \in M_n(k)$ tel que $J_{i,j} = \delta_{i+1,j}$, pour tous $i \in \{1, \dots, n-1\}$ et $j \in \{1, \dots, n\}$, et $J_{n,j} = \delta_{1,j}$, pour tout $j \in \{1, \dots, n\}$. Montrer que $M = f(J)$.

(b) Soit $\xi = e^{2i\pi/n}$. Pour $0 \leq r \leq n-1$, on pose $U_r = \sum_{\ell=0}^{n-1} \xi^{r\ell} e_{1+\ell}$, où e_ℓ est le ℓ-ème vecteur de la base canonique de k^n. Montrer que U_r est un vecteur propre de J associé à la valeur propre ξ^r.

(c) En déduire que $\det(M) = \prod_{r=0}^{n-1} f(\xi^r) = \prod_{r=0}^{n-1} \sum_{\ell=0}^{n-1} \xi^{r\ell} X_{\ell+1}$.

Séries formelles

5. *Éléments inversibles.* Soit A un anneau commutatif. On note $A[[X]]$ l'anneau des séries formelles à coefficients dans A, c'est-à-dire l'ensemble des expressions de la forme $\sum_{\ell\geq 0} a_\ell X^\ell$ avec $(a_\ell)_{\ell\in\mathbb{N}} \in A^{\mathbb{N}}$, muni de l'addition terme à terme et de la multiplication de Cauchy définie par

$$\Big(\sum_{\ell\geq 0} a_\ell X^\ell\Big)\Big(\sum_{\ell\geq 0} b_\ell X^\ell\Big) = \Big(\sum_{\ell\geq 0}\Big(\sum_{j=0}^{\ell} a_j b_{\ell-j}\Big)X^\ell\Big).$$

(a) Montrer qu'une série formelle $\sum_{\ell\geq 0} a_\ell X^\ell$ est inversible si et seulement si a_0 est inversible dans A.

(b) Montrer que $A[[X]]$ est un anneau local si et seulement si A est un anneau local (en particulier $K[[X]]$ est local pour tout corps K).

6. *Valuation, division euclidienne et conséquences.* Soit K un corps. La valuation d'une série formelle non nulle $a = \sum_{\ell\geq 0} a_\ell X^\ell \in K[[X]]$ est définie par

$$v(a) = \min\{\ell \in \mathbb{N} : a_\ell \neq 0\}.$$

On pose $v(0) = +\infty$.

(a) Montrer que pour tout $a, b \in K[[X]]$ on a $v(a+b) \geq \min(v(a), v(b))$ et $v(ab) = v(a) + v(b)$, et que a est inversible si et seulement si $v(a) = 0$.

(b) Soient $a = \sum_{\ell\geq 0} a_\ell X^\ell$ et $b = \sum_{\ell\geq 0} b_\ell X^\ell$ deux séries formelles de $K[[X]]$, avec $b \neq 0$. Montrer qu'il existe $q, r \in K[[X]]$ tels que $a = bq + r$ avec $v(r) < v(b)$ ou $r = 0$. *Indication :* on pourra prendre $r = \sum_{\ell=0}^{v(b)-1} a_\ell X^\ell$.

(c) Montrer que $K[[X]]$ est principal.

(d) Montrer que tout idéal non nul de $K[[X]]$ est de la forme (X^n) pour un certain entier n.

Polynômes symétriques et relations entre les racines et les coefficients

7. *Polynômes alternés et symétriques.*

(a) Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$ tel que pour tout couple (i, j) avec $i < j$ on ait

$$P(X_1, \dots, X_i, \dots, X_{j-1}, X_i, X_{j+1}, \dots, X_n) = 0.$$

Montrer que $\prod_{i<j}(X_j - X_i)$ divise P.

(b) Soit $P \in \mathbb{Z}[X, Y]$ symétrique tel que $(X - Y)|P$. Montrer que $(X - Y)^2|P$.

8. *Polynômes symétriques homogènes.* Soit A un anneau commutatif intègre. Exprimer $\sum_{i\neq j} X_i^2 X_j$ et $\sum_{i<j}(X_i X_j)^2$ dans $A[X_1, \dots, X_n]$ avec $n = 3$ ou $n = 4$, comme polynômes en les polynômes symétriques élémentaires.

9. Soit A un anneau commutatif intègre et

$$I = \big\{(i, j, k) \in [\![1, n]\!]^3 : i \neq j, i \neq k, j \neq k\big\}.$$

Exprimer $\sum_{(i,j,k)\in I} X_i X_j X_k^2$ comme polynôme en les polynômes symétriques élémentaires.

10. *Formules de Newton.* Soit A un anneau commutatif intègre de caractéristique plus grande que n. Pour tout $\ell \in \mathbb{N}^*$, on note $S_\ell = \sum_{i=1}^n X_i^\ell$ la ℓ-ème somme de Newton dans $A[X_1, \ldots, X_n]$, et pour $\ell \in \{1, \ldots, n\}$, σ_ℓ le ℓ-ème polynôme symétrique élémentaire en $X_1, \ldots, X_n$. Soit $P(T) = \prod_{i=1}^n (1 - TX_i) \in A[X_1, \ldots, X_n][T]$.

(a) Montrer que

$$P(T) = 1 + \sum_{\ell=1}^{n} (-1)^\ell \sigma_\ell T^\ell \quad \text{et} \quad -T\frac{P'(T)}{P(T)} = \sum_{i=1}^{n} \frac{TX_i}{1 - TX_i} = \sum_{\ell \in \mathbb{N}^*} S_\ell T^\ell.$$

(b) En déduire les *identités de Newton* :

(i) si $1 \leq \ell \leq n$, alors $S_\ell + \sum_{i=1}^{\ell-1} (-1)^i \sigma_i S_{\ell-i} + (-1)^\ell \ell \sigma_\ell = 0$,

(ii) si $\ell \geq n$, alors $S_\ell + \sum_{i=1}^{n} (-1)^i \sigma_i S_{\ell-i} = 0$.

(c) En déduire que $A[X_1, \ldots, X_n]^{\mathbb{S}_n} = A[S_1, \ldots, S_n]$.

(d) On va considérer l'application suivante. Soient $A, B \in M_n(\mathbb{C})$. Montrer que A et B ont le même polynôme caractéristique si et seulement si pour tout $\ell \in \{1, \ldots, n\}$, $\mathrm{tr}(A^\ell) = \mathrm{tr}(B^\ell)$.

(e) En déduire que A est nilpotente si et seulement si pour tout $\ell \in \{1, \ldots, n\}$, $\mathrm{tr}(A^\ell) = 0$.

11. *Discriminant d'une équation cubique.* Soient K un corps et $(\alpha_i)_{1 \leq i \leq 3}$ les racines du polynôme cubique $X^3 + pX + q \in K[X]$. Déterminer en fonction de p et q

(a) $\sum_{i=1}^3 \alpha_i^6$,

(b) Le discriminant $\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2$.

12. *Orbite et stabilisateur.* Soit A un anneau commutatif intègre et $N \geq 4$ entier. Déterminer l'orbite et le stabilisateur des polynômes suivants dans $A[X_1, \ldots, X_N]$ sous l'action de $\mathbb{S}_N$: X_1X_2, $X_2X_3X_4$, $X_1X_2 + X_3X_4$.

13. *Signature d'une permutation.* Soit $n \geq 2$. On rappelle que la *signature* $\epsilon(\sigma)$ de la permutation $\sigma \in \mathbb{S}_n$ est la parité de son nombre d'inversions, *i.e.*

$$\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

On note $\delta = \prod_{1 \leq i < j \leq n} (X_j - X_i) \in \mathbb{Z}[X_1, \ldots, X_n]$.

(a) Soit $\sigma \in \mathbb{S}_n$, déterminer $\sigma \cdot \delta$.

(b) En déduire que la signature est un morphisme de groupes $\mathbb{S}_n \to \{\pm 1\}$. En particulier, la parité du nombre de transpositions dans toute décomposition de σ donnée ne dépend pas de la décomposition.

⋆ **14.** *Opérations sur les entiers algébriques.* On appelle *entier algébrique* un nombre complexe qui est racine d'un polynôme unitaire à coefficients entiers. On note $\mathbb{A}$ l'ensemble des entiers algébriques, on va montrer dans cet exercice que c'est un anneau.

(a) Montrer que $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.

(b) Soient $P, Q \in \mathbb{Z}[X]$ deux polynômes unitaires de degré n et m respectivement et de racines complexes $(a_i)_{1 \leq i \leq n}$ et $(b_j)_{1 \leq j \leq m}$. On pose

$$S = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (X - a_i - b_j) \quad \text{et} \quad T = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (X - a_i b_j).$$

Montrer que le polynôme symétrique

$$\tilde{S}(B_1, \ldots, B_m) = \prod_{j=1}^{m} P(X - B_j)$$

est à coefficients dans $\mathbb{Z}[X]$. En déduire que $S \in \mathbb{Z}[X]$.

(*c*) Soit $\tilde{P} \in \mathbb{Z}[X, Y]$ l'homogénéisé de P. Montrer que $T = \prod_{j=1}^{m} \tilde{P}(X, b_j)$. Avec un raisonnement similaire à celui de la question précédente, montrer que $T \in \mathbb{Z}[X]$.

(*d*) En déduire que $\mathbb{A}$ est un sous-anneau de $\mathbb{C}$.

(*e*) Déterminer un polynôme unitaire à coefficients dans $\mathbb{Z}[X]$ dont $\sqrt{3} + \sqrt{7}$ est racine.