

TD5 : Polynômes symétriques. Anneaux factoriels

Exercice 1 Soit $A[X_1, \dots, X_n]$ l'anneau de polynômes en X_1, \dots, X_n à coefficients dans un anneau intègre A . Le groupe symétrique \mathfrak{S}_n agit de manière naturelle sur $A[X_1, \dots, X_n]$. On désigne par $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ l'anneau des polynômes symétriques (c.à.d. invariants pour l'action de \mathfrak{S}_n) et par s_1, \dots, s_n les polynômes symétriques élémentaires.

Cet exercice suggère une méthode pratique pour présenter un polynôme $f \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ comme $f = g(s_1, \dots, s_n)$, où g est un polynôme en n variables à coefficients dans A .

1. Introduisons l'ordre *lexicographique* sur l'ensemble des monômes : $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n} > X_1^{j_1} X_2^{j_2} \dots X_n^{j_n}$ s'il existe $1 \leq k \leq n$ tel que $i_1 - j_1 = 0, \dots, i_{k-1} - j_{k-1} = 0, i_k - j_k > 0$. Si $f \in A[X_1, \dots, X_n]$, le monôme maximal parmi les monômes qui participent à l'expression de f comme une combinaison linéaire de monômes à coefficients non-nuls est dite *dominant pour f* . Montrer que si u et v sont les monômes dominants pour les polynômes f et g , respectivement, alors uv est le monôme dominant pour fg .
2. Soit $u = X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ et $H = \{\sigma \in \mathfrak{S}_n : \sigma u = u\}$. On écrit

$$S(u) = \sum_{\sigma \in R} \sigma u,$$

où R est un ensemble de représentants des classes d'équivalence à gauche \mathfrak{S}_n/H . Montrer que $S(u) = S(u_0)$, où u_0 est un monôme *monotone*, c.à.d. $u_0 = X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ avec $i_1 \geq i_2 \geq \dots \geq i_n \geq 0$. De plus, u_0 coïncide avec le monôme dominant pour $S(u)$.

3. Montrer que chaque $f \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ se représente uniquement sous la forme

$$f = \sum_{i=1}^m a_i S(u_i),$$

où $a_i \in A \setminus \{0\}$ et u_i sont des monômes monotones.

4. Soit $u = X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ un monôme monotone. On pose

$$g_u = s_1^{i_1 - i_2} s_2^{i_2 - i_3} \dots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n}.$$

Montrer que u est le monôme dominant pour g_u . (Indication : voir 1.) En déduire que $S(u)$ se représente uniquement sous la forme

$$S(u) = g_u + \sum_{w \in M_u} b_w g_w, \tag{1}$$

où $b_w \in A$ et M_u est l'ensemble des monômes monotones $w = X_1^{j_1} X_2^{j_2} \dots X_n^{j_n}$ tels que $u > w$ et $j_1 + \dots + j_n = i_1 + \dots + i_n$.

Exercice 2 En utilisant l'exercice 1 exprimer les polynômes suivants en fonction des polynômes symétriques élémentaires. (Remarque : Pour trouver b_w dans la formule (1) on applique la méthode des coefficients indéterminés.)

- (a) $S(X_1^3) \in \mathbb{Z}[X_1, \dots, X_n]$;
- (b) $X_1^2 X_2 + X_1 X_2^2 + X_1^2 X_3 + X_1 X_3^2 + X_2^2 X_3 + X_2 X_3^2 \in \mathbb{Z}[X_1, X_2, X_3]$;
- (c) $X_1^4 + X_2^4 + X_3^4 - X_1^2 X_2^2 - X_1^2 X_3^2 - X_2^2 X_3^2 \in \mathbb{Z}[X_1, X_2, X_3]$.

Exercice 3 Soit $f(X) = X^n + a_1 X^{n-1} + \dots + a_n \in \mathbb{C}[X]$. Rappelons que $f(X) = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$, où les nombres complexes $\alpha_1, \alpha_2, \dots, \alpha_n$ sont les racines de f . Soit $h \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$, où A est un sous-anneau de \mathbb{C} (exemples : $A = \mathbb{Z}, \mathbb{Z}[\sqrt{2}], \mathbb{Q}, \mathbb{R}$). Montrer que si $h \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ alors $h(\alpha_1, \alpha_2, \dots, \alpha_n) \in A$. (Indications : Utiliser les formules de Viète : $a_i = (-1)^i s_i(\alpha_1, \alpha_2, \dots, \alpha_n)$, $1 \leq i \leq n$.)

Exercice 4 1. Trouver la somme des carrés des racines du polynôme $3X^5 - X^3 + X + 2$.
 2. Trouver $\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3} + \frac{1}{\alpha_4}$, où α_i , $1 \leq i \leq 4$, sont les racines du polynôme $X^4 - X^2 - X - 1$.

Exercice 5 Trouver le polynôme de degré trois dont les racines sont :

- (a) les cubes des racines complexes du polynôme $X^3 - X - 1$;
- (b) les quatrième degrés des racines complexes du polynôme $2X^3 - X^2 + 2$.

Exercice 6 Soit A un anneau principal. Montrer que si I est un idéal premier et $I \neq \{0\}$ alors I est maximal et engendré par un élément irréductible.

Exercice 7 Dans un anneau factoriel montrer qu'un élément a est irréductible si et seulement si l'idéal engendré par a est premier.

Exercice 8 Pour A un anneau intègre, montrer que $A[X]$ est principal si et seulement si A est un corps. En particulier, on obtient que $\mathbb{Z}[X]$ n'est pas principal.

Exercice 9 Montrer que \mathbb{Z} est intégralement clos. (Un anneau intègre A est *intégralement clos* si chaque élément α appartenant à son corps de fractions K et étant racine d'un polynôme $X^n + a_1 X^{n-1} + \dots + a_n \in A[X]$, appartient à A). À quel type d'anneaux peut-on généraliser ce résultat ?

Exercice 10 Soit A un anneau commutatif. Montrez que les conditions suivantes sont équivalentes :

1. Chaque idéal de A est de type fini ;
2. Chaque suite croissante des idéaux de A est finie.
3. Chaque ensemble non-vidé des idéaux de A contient un élément maximal par inclusion.

Un anneau avec les conditions ci-dessus s'appelle anneau *noethérien*.

Exercice 11 Soit A un anneau intègre et noethérien. On suppose que chaque idéal maximal de A est principal. Montrez que :

1. A est factoriel ;
2. A est principal. (Indication : utiliser 1.)

Exercice 12 (Anneau des entiers quadratiques) Si A est un sous-anneau de \mathbb{C} et $\alpha \in \mathbb{C}$ on note $A[\alpha] = \{f(\alpha) : f \in A[X]\}$. Il est facile de voir que $A[\alpha]$ est un anneau. Soit d un nombre entier sans facteur carré.

1. Montrer que $\mathbb{Q}[\sqrt{d}]$ est un corps contenant \mathbb{Q} et $\mathbb{Q}[\sqrt{d}] = \mathbb{Q} + \mathbb{Q}\sqrt{d}$. En particulier, $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{d}] = 2$.
2. Un nombre $\alpha \in \mathbb{Q}[\sqrt{d}]$ est dit *entier* si $\mathbb{Z}[\alpha]$ est un \mathbb{Z} -module de type fini. Soit \mathcal{O}_d l'ensemble des tous nombres entiers dans $\mathbb{Q}[\sqrt{d}]$. Montrer que \mathcal{O}_d est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$ (appelé *anneau des entiers quadratiques*). (Indication : Rappelons que chaque sous-module d'un \mathbb{Z} -module de type fini est de type fini.)
3. Pour $\alpha = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ on note $N(\alpha) = a^2 - b^2d = (a + b\sqrt{d})(a - b\sqrt{d})$ et $T(\alpha) = 2a$.
 - (a) Montrer que l'application $\bar{} : \mathbb{Q}[\sqrt{d}] \rightarrow \mathbb{Q}[\sqrt{d}], a + b\sqrt{d} \rightarrow a - b\sqrt{d}$, est un automorphisme de corps.
 - (b) Montrer que l'application $N : \mathbb{Q}(\sqrt{d})^* \rightarrow \mathbb{Q}^*, \alpha \rightarrow N(\alpha)$, est un homomorphisme de groupes.
 - (c) Montrer que α est une racine du polynôme $f_{\alpha}(X) = X^2 - T(\alpha)X + N(\alpha) \in \mathbb{Q}[X]$.
 - (d) Montrer que $\alpha \in \mathcal{O}_d$ si et seulement si $f_{\alpha}(X) \in \mathbb{Z}[X]$. (Indication : Si $\alpha \in \mathcal{O}_d \setminus \mathbb{Z}$ alors α est une racine d'un polynôme $g(x) = x^n + a_1x^{n-1} + \dots + a_n \in \mathbb{Z}[x]$. On voit facilement que f_{α} divise g dans $\mathbb{Q}[X]$. Maintenant en utilisant le lemme de Gauss on montre que $f_{\alpha} \in \mathbb{Z}[X]$.)
 - (e) Montrer que $\mathcal{O}_d = \mathbb{Z}[\omega]$, où $\omega = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod{4}$ et $\omega = \sqrt{d}$ si $d \equiv 2$ ou $3 \pmod{4}$.
 - (f) Montrer que $\alpha \in \mathcal{O}_d$ est dans \mathcal{O}_d^* si et seulement si $N(\alpha) = \pm 1$. En déduire que \mathcal{O}_2^* est infini.
4. On considère le cas $d = -5$.
 - (a) Montrer que les nombres $3, 7, 1 + 2\sqrt{-5}$ et $1 - 2\sqrt{-5}$ sont irréductibles, deux à deux non-associés et non-premiers. (Indication : $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.)
 - (b) Déduire de (a) que l'anneau \mathcal{O}_{-5} n'est pas factoriel.

Exercice 13 Montrer que $\mathbb{Z}[i]$ est un anneau euclidien.

Exercice 14 Soit A un anneau commutatif euclidien. Montrer qu'il existe un élément x de A non inversible tel que, en notant π la projection $A \rightarrow A/(x)$, $\pi|_{A^\times \cup \{0\}}$ est surjective (où A^\times est l'ensemble des inversibles de A).

Exercice 15 Soit $A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

1. Trouver A^* .
2. En déduire que A n'est pas euclidien.
3. Montrer que A est quasi-euclidien c.à.d. si $a \in A$ et $b \in A \setminus \{0\}$ alors il existe des éléments q et r dans A tels que $a = bq + r$ ou $2a = bq + r$ et $r = 0$ ou $N(r) < N(b)$.
4. Montrer que $A \cong \mathbb{Z}[t]/(t^2 - t + 5)$. En déduire que l'idéal engendré par 2 est maximal dans A .
5. Montrer que A est principal.

Exercice 16 Soit A un anneau factoriel et k son corps des fractions.

1. Si P est un polynôme irréductible de $A[X]$ montrer qu'il est encore irréductible dans $k[X]$. La réciproque est-elle vraie ?
2. Montrer que le polynôme $X^2 + Y^2 + 1$ est irréductible dans $k[X, Y]$ dès que $\text{car}(k) \neq 2$.

Exercice 17 Soit $A = \mathbb{C}[X, Y]/(X^2 - Y^3)$

1. Montrer que A est intègre en exhibant un morphisme injectif $\phi : A \rightarrow \mathbb{C}[T]$.
2. Déterminez le corps des fractions de A .
3. Montrer que A n'est pas intégralement clos. L'anneau A est-il factoriel ?

Exercice 18

1. Soit $P \in \mathbb{C}[X, Y]$ un polynôme, montrer que l'idéal (P) n'est pas maximal dans $\mathbb{C}[X, Y]$.
2. Soient $A, B \in \mathbb{C}[X, Y]$, $B \neq 0$, montrer qu'il existe $Q, R \in \mathbb{C}[X, Y]$ et $P \in \mathbb{C}[X]$ avec $\deg_Y(R) < \deg_Y(B)$ tels que $P(X)A(X, Y) = B(X, Y)Q(X, Y) + R(X, Y)$.
3. Soit \mathcal{M} un idéal premier non principal de $\mathbb{C}[X, Y]$, montrer qu'il existe $a, b \in \mathbb{C}$ tels que $\mathcal{M} = (X - a, Y - b)$.
4. En déduire la liste des idéaux premiers de $\mathbb{C}[X, Y]$.
5. Pour un polynôme $P \in \mathbb{C}[X, Y]$ trouver la liste des idéaux premiers de $\mathbb{C}[X, Y]$ contenant P .