Polynômes invariants sous le groupe alterné

Soient A un anneau commutatif unitaire et $n \geq 2$ un entier. Le groupe symétrique $\mathfrak{S}_n$ agit sur l'anneau de polynômes $A[X_1, \ldots, X_n]$ en permutant les variables, et un polynôme invariant pour cette action est dit *symétrique*. Un polynôme qui est invariant pour l'action restreinte du groupe alterné $\mathfrak{A}_n$ est dit *alterné* ; donc tout polynôme symétrique est alterné. Le théorème fondamental des fonctions symétriques dit que l'anneau des polynômes symétriques est engendré par les fonctions symétriques élémentaires $S_1^n, \ldots, S_n^n$. Qu'en est-il pour l'anneau des polynômes alternés ? Son calcul est classique lorsque A est le corps des nombres complexes, ou d'ailleurs n'importe quel anneau dans lequel 2 est inversible ; mais il est plus original sur un anneau de base quelconque. On peut trouver ce développement dans le livre [S], page 602.

Ce développement peut être utilisé dans les leçons :

Groupes opérant sur un ensemble. Exemples et applications.
Groupes finis. Exemples et applications.
Groupe des permutations d'un ensemble fini. Applications.
Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.

1 Cas où 2 est inversible dans A

Rappelons que la fonction symétrique élémentaire de degré i en n variables est définie par

$$S_i = \sum_{\{\alpha_1 < \cdots < \alpha_i\}} X_{\alpha_1} \ldots X_{\alpha_i} \ ,$$

où la somme est étendue à toutes les parties ordonnées de i éléments de $\{1, \ldots, n\}$. Nous la notons S_i plutôt que S_i^n, car dans ce complément le nombre de variables sera toujours n. Nous introduisons aussi le polynôme de Vandermonde défini par

$$V_n = \prod_{i>j} (X_i - X_j) \ .$$

Ce polynôme est invariant par les permutations paires, et une permutation impaire change V_n en $-V_n$. Ainsi, sur un corps de caractéristique différente de 2, c'est un polynôme alterné, non symétrique. Pour déterminer tous les polynômes alternés, nous aurons besoin de quelques remarques sur les calculs dans $A[X_1, \ldots, X_n]$ et plus particulièrement sur la divisibilité par les polynômes $X_i - X_j$. Lorsque A est un anneau factoriel, par exemple un corps, il est clair que ces polynômes sont des irréductibles distincts. En conséquence, si un polynôme en n variables est divisible par tous les $X_i - X_j$ il est divisible par le polynôme de Vandermonde. En fait, si A est quelconque (pas nécessairement factoriel ni même intègre), il est facile de vérifier par des calculs directs que cette affirmation reste vraie :

Lemme 1 *Soit A un anneau commutatif et unitaire, et $F \in A[X_1, \ldots, X_n]$. Alors,*
(i) *$X_i - X_j$ est régulier dans $A[X_1, \ldots, X_n]$, pour tous i, j. De manière équivalente, le polynôme de Vandermonde V_n est régulier.*

(ii) *Si* $F(..., X, ..., X, ...) = 0$, *l'indéterminée* X *étant aux places* i *et* j, *alors* F *est divisible par* $X_i - X_j$.
(iii) *Si* F *est divisible par tous les polynômes* $X_i - X_j$ *pour* $i > j$, *il est divisible par le polynôme de Vandermonde.*

Nous utiliserons fréquemment le fait général et élémentaire suivant : un polynôme à coefficients dans un anneau R, de coefficient dominant régulier dans R, est régulier.

Preuve : (i) La remarque que l'on vient de faire, avec $R = A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ et $X = X_i$, nous dit que le polynôme $X_i - X_j$ est polynôme en X_i de coefficient dominant égal à 1, donc il est régulier dans $A[X_1, \ldots, X_n]$. Le résultat en découle pour V_n, car un produit d'éléments réguliers est régulier.
(ii) En faisant agir une permutation σ qui envoie i sur 1 et j sur 2, on se ramène au cas $i = 1$, $j = 2$, ce qui simplifie les notations. Effectuons la division euclidienne de F, vu comme un polynôme en X_1 à coefficients des polynômes en les autres variables, par $X_1 - X_2$. On trouve $F = (X_1 - X_2)Q + R$ où R est un polynôme constant en X_1, c'est-à-dire $R = R(X_2, X_3, \ldots)$. Lorsqu'on spécialise X_1 et X_2 en X comme indiqué, on trouve $0 = 0 + R(X, X_3, \ldots)$. Comme X est une indéterminée, ceci donne $R = 0$ de sorte que $X_1 - X_2$ divise F.
(iii) Les couples d'entiers (i, j) tels que $1 \leq j < i \leq n$ sont en nombre fini égal à $N = n(n-1)/2$. Munissons l'ensemble de ces couples de l'ordre lexicographique, et pour tout $k \leq N$, notons E_k l'ensemble des k premiers couples. On va montrer par récurrence sur k qu'il existe un polynôme $Q_k \in A[X_1, \ldots, X_n]$ tel que

$$F = \left(\prod_{(i,j) \in E_k} (X_i - X_j) \right) Q_k \ .$$

Pour $k = 1$, c'est une simple conséquence de l'hypothèse. Supposons maintenant que cette propriété est vraie pour un entier $k \leq N - 1$. Notons (u, v) le $k + 1$-ème couple d'entiers et Π le produit des $X_i - X_j$ avec $(i, j) \in E_k$. On sait que $X_u - X_v$ ne divise pas Π, mais $X_u - X_v$ divise F par hypothèse. Donc lorsqu'on fait $X_u = X_v$, le produit Π ne s'annule pas, et est régulier d'après le point (i), mais F s'annule. Il s'ensuit que Q_k s'annule. D'après le point (ii), il existe un polynôme Q_{k+1} tel que $Q_k = (X_u - X_v)Q_{k+1}$ et la propriété est vraie pour $k + 1$. L'assertion à démontrer est le cas $k = N$. □

Lemme 2 *Soit* A *un anneau commutatif et unitaire,* B *la* A*-algèbre des polynômes symétriques en* $X_1, \ldots, X_n$ *et* C *la* B*-algèbre des polynômes alternés. Alors il existe un* B*-automorphisme d'algèbres involutif*

$$\begin{array}{ccc} C & \to & C \\ F & \mapsto & \overline{F} \end{array}$$

défini en choisissant une permutation impaire quelconque σ *et en posant* $\overline{F} = \sigma F$. *Le polynôme* $\overline{F}$ *est appelé le* conjugué *de* F. *De plus,* F *est symétrique si et seulement si* $\overline{F} = F$.

En particulier, on a $\overline{V}_n = -V_n$.

Preuve : Soit F un polynôme alterné, σ une permutation impaire et $\overline{F} = \sigma F$. Si σ' est une autre permutation impaire, la permutation $\sigma^{-1}\sigma'$ est paire donc $(\sigma^{-1}\sigma')F = F$, de sorte que $\sigma' F = \sigma(\sigma^{-1}\sigma')F = \sigma$. Ceci montre que $\overline{F}$ est indépendant du choix de la permutation impaire σ. Par ailleurs, si τ est une permutation paire, alors $\sigma^{-1}\tau\sigma$ l'est aussi et donc

$$\tau\overline{F} = \sigma(\sigma^{-1}\tau\sigma F) = \sigma F = \overline{F} \ .$$

Ceci montre que $\overline{F}$ est alterné. Il est immédiat de vérifier que $\overline{\overline{F}} = F$ et que F est symétrique si et seulement si $\overline{F} = F$. □

Nous avons en main les outils pour démontrer le résultat suivant :

Théorème 1 *Soit A un anneau commutatif et unitaire tel que 2 est inversible dans A. Alors l'anneau des polynômes alternés est engendré par les fonctions symétriques élémentaires et le polynôme de Vandermonde. Plus précisément, notons $B = A[S_1, ..., S_n]$ l'algèbre des polynômes symétriques et $\Delta_n \in B$ le polynôme égal au carré du polynôme de Vandermonde. Alors, l'anneau des polynômes alternés est isomorphe comme B-algèbre à $B[T]/(T^2 - \Delta_n)$, par un isomorphisme qui envoie V_n sur la classe de T.*

L'expression du polynôme Δ_n nous est familière : ce n'est rien d'autre que le discriminant du polynôme $\prod_{i=1}^n (T - X_i)$, vu comme polynôme en T.

Preuve : Si F est un élément de C, on note $B \cdot F$ le sous-B-module qu'il engendre. Si F est régulier, le morphisme surjectif de B-modules $B \to B \cdot F$, $b \mapsto bF$ est injectif, donc c'est un isomorphisme. Dans C, les éléments 1 et V_n sont réguliers (voir lemme 1(i)), donc les sous-modules $B \cdot 1$ et $B \cdot V_n$ sont isomorphes à B.

Ces sous-modules sont en somme directe, car si $P + V_n R = 0$, alors en passant au conjugué on trouve $P - V_n R = 0$, dont on déduit $P = R = 0$.

Nous allons vérifier qu'ils engendrent C. Soit F un polynôme alterné et $\overline{F}$ son conjugué, comme défini dans le lemme 1. On considère les deux polynômes alternés $P = F + \overline{F}$ et $Q = F - \overline{F}$. Pour calculer $\overline{F}$, on peut utiliser n'importe quelle permutation impaire σ. Si on choisit $\sigma = (ij)$, on obtient

$$Q = F - \sigma F = F(..., X_i, ..., X_j, ...) - F(..., X_j, ..., X_i, ...)$$

donc $Q(..., X, ..., X, ...) = 0$, l'indéterminée X étant aux places i et j. D'après le point (ii) du lemme ci-dessus, on en déduit que Q est divisible par $X_i - X_j$. Comme ceci est vrai pour tous i, j, d'après le point (ii) du lemme on trouve que Q est divisible par le polynôme de Vandermonde : il existe un polynôme R tel que $Q = V_n R$. Voyons maintenant que P et R sont symétriques. Pour P c'est clair, car $\overline{P} = \overline{F} + F = P$. Par ailleurs, on a $\overline{Q} = \overline{F} - F = -Q$ et comme $\overline{V}_n = -V_n$, on trouve $V_n \overline{R} = V_n R$. D'après le point (i) du lemme, V_n est régulier, donc $\overline{R} = R$, et R est symétrique. Comme $F = \frac{1}{2}(P + Q) = \frac{1}{2}P + \frac{1}{2}V_n R$, on obtient bien que $B \cdot 1$ et $B \cdot V_n$ engendrent C. On a montré que l'algèbre C est engendrée par les fonctions symétriques élémentaires et le polynôme V_n.

Il nous reste à définir un isomorphisme $B[T]/(T^2 - \Delta_n) \simeq C$. Définissons un morphisme de B-algèbres $f : B[T] \to C$ par $f(T) = V_n$. Comme l'image de $T^2 - \Delta_n$ par f est $(V_n)^2 - \Delta_n = 0$, alors f induit un morphisme $\widetilde{f} : B[T]/(T^2 - \Delta_n) \to C$. Le B-module $B[T]/(T^2 - \Delta_n)$ est libre de rang 2 avec pour base 1 et l'image de T, et $\widetilde{f}$ envoie cette base sur la base $\{1, V_n\}$ donc c'est un isomorphisme. □

2 Cas général

Le 2 qui pose problème s'explique bien sûr par le fait que c'est l'indice de $\mathfrak{A}_n$ dans $\mathfrak{S}_n$. Introduisons le polynôme symétrique

$$\Theta_n = \prod_{i>j}(X_i + X_j) \ .$$

Lorsque 2 n'est pas inversible, il n'est plus vrai que V_n engendre l'anneau des polynômes alternés : en fait, si A est de caractéristique 2, on a $+1 = -1$ donc $V_n = \Theta_n$ est symétrique. On va maintenant s'affranchir de l'hypothèse $2 \in A^\times$.

Pour n'importe quel anneau unitaire A, il y a un morphisme $\mathbb{Z} \to A$, qui à n associe $n1$. En prenant les images des coefficients par ce morphisme, on peut voir tout polynôme P à coefficients dans l'anneau des entiers $\mathbb{Z}$ comme un polynôme à coefficients dans A. Pour simplifier, on le note encore par la même lettre P, lorsque l'anneau dans lequel on considère les coefficients de P est clair d'après le contexte.

Considérons d'abord V_n et Θ_n à coefficients dans $\mathbb{Z}$. D'après notre remarque introductive, lorsqu'on réduit modulo 2 pour obtenir des polynômes à coefficients dans le corps fini $\mathbb{F}_2$ on a :

$$V_n + \Theta_n = 2\Theta_n = 0 \ .$$

Il s'ensuit qu'il existe un polynôme W_n à coefficients dans $\mathbb{Z}$ tel que $2W_n = V_n + \Theta_n$. Nous appellerons ce polynôme W_n le *polynôme de Vandermonde modifié*. Pour tout anneau A, on peut le voir comme un polynôme à coefficients dans A. Nous allons démontrer un analogue du théorème 1, valable pour n'importe quel anneau commutatif, en remplaçant V_n par W_n.

Exemple 1 *Lorsque $n = 2$, on trouve :*

$$W_2 = \frac{1}{2}\big((Y - X) + (Y + X)\big) = Y \ .$$

Lorsque $n = 3$, on trouve après un bref calcul :

$$W_3 = \frac{1}{2}\big((Z-Y)(Z-X)(Y-X)+(Z+Y)(Z+X)(Y+X)\big) = YZ^2+XY^2+ZX^2+XYZ \ .$$

Il sera utile de collecter deux petits renseignements sur W_n :

Lemme 3 *Soit A un anneau commutatif unitaire, et*

$$W_n = \frac{1}{2}\left(\prod_{i>j}(X_i - X_j) + \prod_{i>j}(X_i + X_j)\right)$$

le polynôme de Vandermonde modifié. Alors,
(i) *W_n est régulier dans $A[X_1, \ldots, X_n]$.*
(ii) *Le conjugué de W_n est $\overline{W}_n = \Theta_n - W_n = W_n - V_n$.*

Preuve : On démontre le point (i) par récurrence sur $n \geq 2$. Pour $n = 2$ le résultat est clair. Pour $n \geq 3$, on calcule le coefficient dominant de W_n vu comme polynôme en X_n. Pour obtenir des termes de degré maximal en X_n, lorsqu'on développe le produit qui définit V_n, on doit retenir X_n dans chacun des facteurs $(X_n - X_i)$ pour $n > i$. Le coefficient devant X_n est donc

$$\prod_{n>i>j} (X_i - X_j) \ ,$$

c'est-à-dire V_{n-1}. De même, le coefficient dominant de Θ_n est Θ_{n-1}, de sorte que le coefficient dominant de W_n est W_{n-1}. D'après l'hypothèse de récurrence, W_{n-1} est régulier dans $A[X_1, \dots, X_{n-1}]$, et ceci implique que W_n est régulier dans $A[X_1, \dots, X_n]$.

Pour démontrer le point (ii), on raisonne d'abord dans l'anneau des polynômes à coefficients dans $\mathbb{Z}$. Une permutation impaire σ envoie $2W_n = V_n + \Theta_n$ sur $-V_n + \Theta_n = 2(\Theta_n - W_n)$, en d'autres termes,

$$\overline{W}_n = \Theta_n - W_n = W_n - V_n \ .$$

En prenant les images par le morphisme $\mathbb{Z} \to A$, ces expressions restent valables dans l'anneau A. $\square$

Nous introduisons enfin le polynôme $\Gamma_n := W_n \overline{W}_n$. Ce polynôme est clairement symétrique, et en utilisant le fait que $\overline{V}_n = -V_n$ et $\overline{\Theta}_n = \Theta_n$, on trouve $\Theta_n = W_n + \overline{W}_n$. En remplaçant Γ_n par sa valeur de définition, il vient l'identité :

$$W_n^2 - \Theta_n W_n + \Gamma_n = 0 \ .$$

Les polynômes Θ_n et Γ_n sont appelés la *trace* et la *norme* de W_n.

Théorème 2 *Soit A un anneau commutatif et unitaire. Alors l'anneau des polynômes alternés est engendré par les fonctions symétriques élémentaires et le polynôme de Vandermonde modifié W_n. Plus précisément, notons $B = A[S_1, ..., S_n]$ l'algèbre des polynômes symétriques et Θ_n, Γ_n les éléments de B introduits ci-dessus. Alors, l'anneau des polynômes alternés est isomorphe comme B-algèbre à $B[T]/(T^2 - \Theta_n T + \Gamma_n)$, par un isomorphisme qui envoie W_n sur la classe de T.*

Preuve : Notons $B \cdot 1$ et $B \cdot W_n$ les sous-B-modules de C engendrés par 1 et W_n. Comme 1 et W_n sont réguliers (lemme 3), ces deux sous-modules sont isomorphes à B. De plus ils sont en somme directe : si $P + W_n R = 0$, alors en passant au conjugué on trouve $P + (W_n - V_n)R = 0$. En soustrayant ces égalités, on trouve $-V_n R = 0$. Comme V_n est régulier d'après le point (i) du lemme 1, il vient $R = 0$, puis $P = 0$.

Nous allons vérifier que $B \cdot 1$ et $B \cdot W_n$ engendrent C. Soit F un polynôme alterné et posons $Q = F - \overline{F}$. En procédant comme dans la preuve du théorème 1, on montre que Q est divisible par V_n, donc il existe un polynôme R tel que $Q = V_n R$. Ce polynôme est symétrique. Le polynôme $P = F - W_n R$ vérifie

$$\overline{P} = \overline{F} - \overline{W}_n R = (F - V_n R) - (W_n - V_n)R = F - W_n R = P \ ,$$

donc il est symétrique également. Finalement, on a obtenu $F = P + W_n R$ avec P et R symétriques, d'où le résultat d'engendrement annoncé.

Pour finir, définissons un morphisme de B-algèbres $f : B[T] \to C$ par $f(T) = W_n$. D'après la définition de Γ_n, l'image de $T^2 - \Theta_n T + \Gamma_n$ par f est $(W_n)^2 - \Theta_n W_n + \Gamma_n = 0$. Ainsi f induit un morphisme $\widetilde{f} : B[T]/(T^2 - \Theta_n T + \Gamma_n) \to C$. Le B-module

$B[T]/(T^2 - \Theta_n T + \Gamma_n)$ est libre de rang 2 avec pour base 1 et l'image de T, et $\widetilde{f}$ envoie cette base sur la base $\{1, W_n\}$ donc c'est un isomorphisme. $\square$

Bibliographie :

[AB] ARNAUDIÈS, BERTIN, Groupes, Algèbres et Géométrie, tome II, *Ellipses.*

Calcul des polynômes invariants sous le groupe alterné sur le corps des complexes :

[Gob] GOBLOT, Algèbre commutative, *Masson.*

Preuve du théorème des fonctions symétriques avec une récurrence *simple* (on le trouve partout avec une récurrence double) :

[LS] LEICHTNAM, SCHAUER, Exercices corrigés de Mathématiques posés aux oraux X-ENS, Algèbre I, p. 53, *Ellipses.*

[S] A. SZPIRGLAS, Mathématiques algèbre L3, Cours complet avec 400 tests et exercices corrigés, *Pearson.*