# POLYNÔMES INVARIANTS SOUS L'ACTION DU GROUPE ALTERNÉ

OLIVIER SERMAN

On considère ici l'algèbre des polynômes invariants sous l'action du groupe alterné $\mathfrak{A}_n$. La première partie, où on décrit cette algèbre, est un grand classique, et se trouve un peu partout dans la littérature [1]. Dans la seconde, on étudie la factorialité de cet anneau : on montre qu'il est factoriel pour $n \geqslant 5$, en utilisant (comme on l'aura deviné) la simplicité du groupe alterné.

On désigne par $k$ un corps de caractéristique différente de 2, et par $n$ un entier $\geqslant 2$.

## 1. Polynômes invariants sous le groupe alterné

**1.1.** Rappelons que le groupe symétrique $\mathfrak{S}_n$ agit sur l'algèbre $k[X_1, \ldots, X_n]$ des polynômes à $n$ indéterminées de la façon suivante : $\sigma \in \mathfrak{S}_n$ envoie $P \in k[X_1, \ldots, X_n]$ sur le polynôme $\sigma P$ défini par

$$\sigma P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

On dit qu'un polynôme $P$ est symétrique si $\sigma P = P$ pour tout $\sigma \in \mathfrak{S}_n$. Le théorème des polynômes symétriques affirme que tout polynôme symétrique s'écrit comme un unique polynôme en les polynômes symétriques élémentaires $s_1, \ldots, s_n$. Autrement dit, l'algèbre des polynômes symétriques, que l'on note $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$, est isomorphe à l'algèbre $k[s_1, \ldots, s_n]$.

Si $\varepsilon \colon \mathfrak{S}_n \to \{\pm 1\}$ désigne la signature, on dit que $P$ est *antisymétrique* si $\sigma P = \varepsilon(\sigma) P$ pour tout $\sigma \in \mathfrak{S}_n$.

Un exemple de polynôme antisymétrique est fourni par le polynôme $V$ défini comme [2]

$$V = \prod_{i<j} (X_i - X_j).$$

**Lemme 1.2.** *Tout polynôme antisymétrique est le produit de $V$ et d'un polynôme symétrique.*

*Démonstration.* Soit $P$ un polynôme antisymétrique. Puisque les $X_i - X_j$, $i < j$ sont des irréductibles deux à deux premiers entre eux dans l'anneau factoriel $k[X_1, \ldots, X_n]$, il s'agit de montrer que $X_i - X_j$ divise $P$ pour tout $i < j$. Pour cela, effectuons la division euclidienne (dans $k[X_1, \ldots, \hat{X}_i, \ldots, X_n][X_i]$) de $P$ par $X_i - X_j$, possible puisque $X_i - X_j$ est unitaire. Il existe donc $Q \in k[X_1, \ldots, \hat{X}_i, \ldots, X_n][X_i]$ et $R \in k[X_1, \ldots, \hat{X}_i, \ldots, X_n]$ tels que

$$P = (X_i - X_j)Q + R.$$

Faisons maintenant $X_i = X_j$ dans l'égalité précédente. Comme $P$ est antisymétrique, le polynôme $P(\ldots, X_j, \ldots, X_j, \ldots)$ (où $X_j$ est à la $i$-ème et à la $j$-ème place) est nul. On en déduit que $R = 0$, i.e. $X_i - X_j | P$ pour tout $X_i - X_j, i < j$. On a donc $V | P$. Il est alors immédiat que le polynôme $Q$ tel que $P = VQ$ est symétrique. □

On s'intéresse à l'algèbre $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ des polynômes *invariants sous l'action du groupe alterné*, i.e. des polynômes $P \in k[X_1, \ldots, X_n]$ tels que $\sigma P = P$ pour tout $\sigma \in \mathfrak{A}_n$.

**Théorème 1.3.** *Tout polynôme $P$ invariant sous $\mathfrak{A}_n$ s'écrit sous la forme $P = A + BV$ où $A$ et $B$ sont deux polynômes symétriques uniquement déterminés.*

---

*Date*: 7 juin 2015.

1. Il existe des références où ces polynômes invariants sous $\mathfrak{A}_n$ sont appelés « polynômes alternés ». Cette appellation est très discutable, et je m'abstiendrai de l'utiliser.
2. Vérifiez-le !

*Démonstration.* Soit $P$ un polynôme invariant sous $\mathfrak{A}_n$. L'unicité d'une telle écriture est presque immédiate. Néanmoins, il convient d'en écrire les détails, car cela guide la démonstration de l'existence de cette écriture. Soit donc $P = A + BV$ avec $A, B$ deux polynômes symétriques. Appliquons la transposition $\tau = (1,2)$ à cette égalite. Il vient $\tau P = \tau A + \tau B \tau V = A - BV$. On a donc

$$\begin{cases} P = A + BV \\ \tau P = A - BV. \end{cases}$$

On en déduit que $A$ est égal à $\frac{1}{2}(P + \tau P)$ et $B$ au quotient de $\frac{1}{2}(P - \tau P)$ par $V$.

Démontrons maintenant l'existence de cette décomposition. L'orbite de $P$ sous $\mathfrak{S}_n$ ne prend que deux valeurs (éventuellement égales) $P$ et $Q = \tau P$, où $\tau$ désigne n'importe quelle permutation impaire. Il suffit alors de remarquer d'une part que

$$P = \frac{1}{2}(P + Q) + \frac{1}{2}(P - Q),$$

et d'autre part que le polynôme $A = \frac{1}{2}(P + Q)$ est symétrique, tandis que le polynôme $\frac{1}{2}(P - Q)$, qui est antisymétrique, s'écrit (d'après le lemme précédent) comme produit de $V$ et d'un polynôme symétrique $B$. On a donc écrit $P$ sous la forme attendue

$$P = A + BV$$

avec $A$ et $B$ deux polynômes symétriques. □

On peut reformuler cet énoncé en une description de l'algèbre des polynômes invariants sous $\mathfrak{A}_n$ comme algèbre quotient d'une algèbre de polynômes. Pour cela, notons que le carré

$$\Delta = V^2 = \prod_{i<j} (X_i - X_j)^2$$

du polynôme $V$ est évidemment symétrique, et donc appartient à l'algèbre $k[s_1, \ldots, s_n]$. Remarquons que $\Delta$ n'est autre que le *discriminant* de l'équation $\prod_i (T - X_i) \in k[X_1, \ldots, X_n][T]$.

**Corollaire 1.4.** *La sous-algèbre $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ de $k[X_1, \ldots, X_n]$ formée des polynômes invariants sous l'action de $\mathfrak{A}_n$ est isomorphe à l'algèbre*

$$k[s_1, \ldots, s_n][T]/(T^2 - \Delta).$$

*Démonstration.* On montre un tel résultat en exhibant un morphisme surjectif de $k[s_1, \ldots, s_n]$ sur $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$, dont on calcule ensuite le noyau.

Le théorème précédent nous invite à considérer le morphisme

$$\varphi \colon k[s_1, \ldots, s_n, T] \longrightarrow k[X_1, \ldots, X_n]^{\mathfrak{A}_n},$$

qui envoie chaque $s_i$ (vu comme une indéterminée [3]) sur le polynôme symétrique $s_i$ dans $k[X_1, \ldots, X_n]$, et $T$ sur $V$. Cette application est bien définie (car $s_1, \ldots, s_n$ et $V$ sont invariants sous $\mathfrak{A}_n$).

Sa surjectivité découle du lemme précédent : un polynôme $P$ invariant sous $\mathfrak{A}_n$ s'écrit sous la forme $A + BV$ avec $A$ et $B$ symétriques. Mais alors $A$ et $B$ sont des polynômes en les $s_i$, i.e. $A = R_1(s_1, \ldots, s_n)$ et $B = R_2(s_1, \ldots, s_n)$. Autrement dit,

$$P = \varphi(R_1 + TR_2).$$

Il reste donc à déterminer le noyau de $\varphi$. Clairement $T^2 - \Delta \in \ker \varphi$. On va montrer que $\ker \varphi$ est précisement l'idéal engendré par $T^2 - \Delta$. Soit donc $Q \in \ker \varphi$. Effectuons sa division euclidienne (dans $k[s_1, \ldots, s_n][T]$) par $T^2 - \Delta$. On a

$$Q = (T^2 - \Delta)R + S, \text{ avec } \deg_T(S) \leqslant 1.$$

3. Il aurait peut-être été préférable de ne pas utiliser la même notation pour les indéterminées et pour leurs « évaluations » dans $k[X_1, \ldots, X_n]$. On aurait alors établi l'isomorphisme

$$k[X_1, \ldots, X_n]^{\mathfrak{A}_n} \simeq k[Y_1, \ldots, Y_n, T]/(T^2 - \Delta)$$

(où $\Delta \in k[Y_1, \ldots, Y_n]$ désigne le polynôme tel que $\Delta(s_1, \ldots, s_n) = \prod_{i<j}(X_i - X_j)^2$) en considérant l'application $\varphi \colon k[Y_1, \ldots, Y_n][T] \to k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ défini par $Y_i \mapsto s_i$ et $T \mapsto V$.

En écrivant $S = S_0 + TS_1$ avec $S_0, S_1 \in k[s_1, \ldots, s_n]$, on obtient dans $k[X_1, \ldots, X_n]$

$$S_0(s_1, \ldots, s_n) + VS_1(s_1, \ldots, s_n) = 0.$$

D'après le lemme, cela entraîne $S_0 = S_1 = 0$, comme attendu. □

**Remarque 1.5.** L'algèbre des polynômes invariants sous $\mathfrak{A}_n$ sur un corps de caractéristique 2 admet également une description explicite, que l'on peut trouver dans Revoy, Anneau des invariants du groupe alterné, Bull. Sci. Math. (2) 106 (1982), no 4, 427–431.

## 2. Factorialité de l'anneau $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$

Pour aller plus loin, nous allons étudier la factorialité de l'algèbre des polynômes invariants sous $\mathfrak{A}_n$.

**2.1.** L'intégrité de cette algèbre est immédiate : en effet, c'est par définition une sous-algèbre de $k[X_1, \ldots, X_n]$ ! On en donne cependant dans la proposition 2.5 une autre démonstration, en utilisant la description comme anneau quotient obtenue en 1.4. Cet autre argument, qui repose sur l'irréductibilité du discriminant (dans $k[s_1, \ldots, s_n]$), est tout à fait au niveau de l'agrégation et peut constituer un excellent développement [4]. La suite va sans doute au-delà, sans pour autant sortir du programme de ce concours. Elle fournit notamment une belle application de la simplicité de $\mathfrak{A}_n$ (pour $n \geqslant 5$). C'est surtout l'occasion d'un premier contact avec les multiples subtilités entourant la notion de factorialité.

**2.2.** Montrons l'irréductibilité du discriminant $\Delta$ dans $k[s_1, \ldots, s_n]$. Pour cela, commençons par établir le lemme suivant [5] :

**Lemme 2.3.** *Soit $P \in k[X_1, \ldots, X_n]$ un polynôme symétrique. S'il existe $i \neq j$ tels que $X_i - X_j$ divise $P$, alors $\Delta$ divise $P$.*

*Démonstration.* Le polynôme $P$ étant symétrique, il revient au même de supposer que $X_i - X_j$ divise $P$ pour tous $i \neq j$.

Montrons que $(X_1 - X_2)^2$ divise $P$. On peut écrire $P$ sous la forme

$$P = (X_1 - X_2)^2 R(X_1, \ldots, X_n) + (X_1 - X_2) S(X_2, X_3, \ldots, X_n)$$

où $R \in k[X_1, \ldots, X_n]$ et $S \in k[X_2, \ldots, X_n]$. Il s'agit de montrer que $S$ est nul. Pour ce faire, on applique la transposition $\tau = (1, 2)$ à l'identité précédente. Il vient

$$P = \tau P = (X_1 - X_2)^2 R(X_2, X_1, X_3, \ldots, X_n) + (X_2 - X_1) S(X_1, X_3, \ldots, X_n),$$

d'où l'on déduit que $(X_1 - X_2)^2$ divise $(X_1 - X_2)(S(X_2, X_3, \ldots) + S(X_1, X_3, \ldots))$, ce qui entraîne

$$(X_1 - X_2) | S(X_2, X_3, \ldots, X_n) + S(X_1, X_3, \ldots, X_n).$$

En faisant $X_1 = X_2$, on obtient $S(X_2, X_3, \ldots, X_n) = 0$, i.e. $S = 0$. Le polynôme $P$ est donc divisible par $(X_1 - X_2)^2$.

On conclut en notant que l'invariance de $P$ sous $\mathfrak{S}_n$ entraîne aussitôt que $(X_i - X_j)^2$ divise également $P$ pour tous $i < j$. Ces polynômes étant deux à deux premiers entre eux, on obtient que $P$ est divisible par $\prod_{i<j} (X_i - X_j)^2 = \Delta$. □

**Proposition 2.4.** *Le polynôme $\Delta$ est irréductible dans $k[s_1, \ldots, s_n]$.*

---

4. Attention tout de même à bien garder en tête que, l'intégrité de cet anneau étant immédiate, il faut présenter l'irréductibilité du discriminant comme un résultat intéressant en lui-même (ce qui est le cas !), et remarquer qu'elle permet de retrouver l'intégrité de l'algèbre quotient $k[s_1, \ldots, s_n]/(T^2 - \Delta)$ *sans savoir a priori qu'elle est isomorphe à* $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$, et par un argument particulièrement *instructif.*

5. Signalons au passage que le cas $n = 2$ constitue le déjà très bon exercice suivant : montrer qu'un polynôme symétrique $P \in k[X, Y]$ divisible par $X - Y$ est aussi divisible par $(X - Y)^2$.

*Démonstration.* Soit $\Delta = P(s_1, \ldots, s_n)Q(s_1, \ldots, s_n)$ une décomposition de $\Delta = \prod_{i<j}(X_i - X_j)^2$ en produit de deux polynômes symétriques.

Considérons cette égalité dans l'anneau $k[X_1, \ldots, X_n]$. On a en particulier que $X_1 - X_2$ divise $P(s_i)$ ou $Q(s_i)$.

Supposons que $X_1 - X_2$ divise le polynôme $P(s_i)$. Puisque $P(s_i)$ est un polynôme symétrique, le lemme précédent assure qu'il est divisible par $\Delta$, et $Q(s_i)$ est alors inversible.

Le polynôme $\Delta$ est donc bien irréductible dans $k[s_1, \ldots, s_n]$. □

On peut maintenant donner l'argument (particulièrement instructif) évoqué plus haut pour établir directement l'intégrité du quotient $k[s_1, \ldots, s_n]/(T^2 - \Delta)$.

**Proposition 2.5.** *L'anneau $k[s_1, \ldots, s_n][T]/(T^2 - \Delta)$ est intègre.*

*Démonstration.* Puisque $k[s_1, \ldots, s_n][T]$ est factoriel, l'intégrité du quotient $k[s_i][T]/(T^2-\Delta)$ équivaut à l'irréductibilité du polynôme $T^2 - \Delta$ dans $k[s_1, \ldots, s_n, T]$. Comme ce polynôme est primitif dans $k[s_i][T]$, il suffit de vérifier qu'il est irréductible sur le corps des fractions $k(s_1, \ldots, s_n)$. Puisque c'est un polynôme de degré 2, il suffit de vérifier qu'il n'y a pas de racine, autrement dit qu'on ne peut trouver deux polynômes $P$ et $Q$ dans $k[s_1, \ldots, s_n]$ premiers entre eux tels que

$$\Delta = \left(\frac{P}{Q}\right)^2.$$

L'irréductibilité de $\Delta$ (dans $k[s_1, \ldots, s_n]$) montre que c'est impossible [6]. □

**2.6.** L'anneau des polynômes invariants sous $\mathfrak{A}_n$ est un anneau intègre et noethérien [7]. En particulier, tout élément y admet une décomposition en produits d'irréductibles. La factorialité de cet anneau équivaut donc à l'unicité de cette décomposition.

Si $n = 2$ le groupe alterné est trivial et il n'y a rien à montrer. On va distinguer les cas $n \geqslant 5$ et $n = 3, 4$.

Le lemme clé suivant permet d'associer à un polynôme $p$ de $k[X_1, \ldots, X_n]$ un polynôme divisible par $p$ et invariant sous $\mathfrak{A}_n$, qui soit « le plus petit possible » [8] :

**Lemme 2.7.** *Soit $n \geqslant 5$. Soit $p \in k[X_1, \ldots, X_n]$ un polynôme irréductible. Soit $\Omega = \{p_1, \ldots, p_k\}$ un système de représentants des polynômes irréductibles contenus dans l'orbite $\mathrm{Orb}_{\mathfrak{A}_n}(p)$ de $p$ sous $\mathfrak{A}_n$. Le polynôme*

$$\pi = \prod_{q \in \Omega} q$$

*est alors invariant sous l'action de $\mathfrak{A}_n$, et est divisible par $p$. De plus, tout polynôme invariant sous $\mathfrak{A}_n$ et divisible par $p$ (dans $k[X_1, \ldots, X_n]$) est divisible par $\pi$.*

*Démonstration.* Une permutation paire $\sigma \in \mathfrak{A}_n$ induit une permutation de $\Omega$, et envoie donc $\pi$ sur un polynôme qui lui est associé. On a ainsi une application $\chi \colon \mathfrak{A}_n \to k^*$ telle que

$$\sigma\pi = \chi(\sigma)\pi \quad \text{pour tous } \sigma \in \mathfrak{A}_n.$$

Cela implique aussitôt que $\chi$ est un morphisme de groupes de $\mathfrak{A}_n$ dans $k^*$ (soit encore un *caractère* de $\mathfrak{A}_n$). Mais, puisqu'on a supposé $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple (et non abélien), et n'admet donc aucun morphisme non trivial vers $k^*$. Il en résulte que $\pi$ est invariant sous $\mathfrak{A}_n$. C'est évidemment un multiple de $p$.

6. Il ne faut surtout pas se priver de relever la ressemblance frappante avec la démonstration de l'irrationalité de $\sqrt{2}$, qu'on n'aura pas manqué de reconnaître.

7. On peut également noter que cet anneau est *intégralement clos*. Tout anneau factoriel est intégralement clos, mais la réciproque est fausse. On obtient d'ailleurs ici, pour $n = 3, 4$ et $k = \mathbf{C}$ (par exemple) des exemples d'anneaux intégralement clos non factoriels.

8. Le polynôme $\prod_{\sigma \in \mathfrak{A}_n} \sigma p$ satisfait bien les deux conditions requises. Mais associer à $p$ ce produit est trop grossier : dans le cas extrême où $p$ est déjà invariant sous $\mathfrak{A}_n$, on obtient le polynôme $q = p^{n!/2}$, alors que $p$ convient également. Le but du lemme est de montrer comment associer à tout polynôme $p$ le plus petit polynôme (au sens de la division) vérifiant les deux conditions souhaitées.

Si $r$ est un polynôme invariant sous $\mathfrak{A}_n$ et divisible par $p$, il est clair que tout $\sigma p \in \mathrm{Orb}_{\mathfrak{A}_n}(p)$ divise $r$. Ainsi $\pi$ divise $r$. (Cette dernière propriété montre que $\pi$ est uniquement déterminé, à multiplication par un inversible près.) $\square$

**Théorème 2.8.** *Si $n \geqslant 5$, l'anneau $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ des polynômes invariants sous le groupe alterné $\mathfrak{A}_n$ est factoriel.*

*Démonstration.* Il suffit de montrer que tout élément irréductible est premier.

Soit donc $a \in k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ un élément irréductible. Il se décompose (dans l'anneau factoriel $k[X_1, \ldots, X_n]$) de manière unique comme produit

$$a = u \prod_{i \in I} p_i^{n_i}$$

d'éléments $p_i \in k[X_1, \ldots, X_n]$ irréductibles et deux à deux premiers entre eux et d'un inversible $u \in k^*$. L'invariance de $a$ sous $\mathfrak{A}_n$ montre que pour tout $i \in I$ et pour tout $\sigma \in \mathfrak{A}_n$, $\sigma p_i$ divise $a$, et que de plus les multiplicités de $p_i$ et $\sigma p_i$ dans $a$ coïncident. En particulier, si $\pi_i$ désigne le polynôme invariant associé à $p_i$ par le lemme 2.7 (de sorte que $\pi_i$ est le produit d'une famille de représentants des polynômes irréductibles apparaissant dans l'orbite $\mathrm{Orb}_{\mathfrak{A}_n}(p_i)$ de $p_i$), alors $\pi_i^{n_i}$ divise $a$. On a en fait

$$a = u' \prod_{j \in J} \pi_j^{n_j}$$

avec $u' \in k^*$, et $J \subset I$. D'après le lemme, chaque $\pi_j$ est invariant sous l'action du groupe alterné[9], et l'irréductibilité de $a$ dans $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ assure donc qu'un seul $\pi_i$ apparaît dans le produit précédent, et avec multiplicité 1.

Autrement dit, la décomposition de $a$ en produits d'irréductibles dans $k[X_1, \ldots, X_n]$ s'écrit

$$(*) \qquad a = u \prod_{q \in \Omega} q$$

où $\Omega$ désigne un ensemble d'irréductibles deux à deux non associés et deux à deux conjugués sous l'action de $\mathfrak{A}_n$.

On est maintenant en mesure de montrer que $a$ est premier. Soient $b, c \in k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ tels que $a$ divise $bc$. Dans $k[X_1, \ldots, X_n]$, cette égalité assure que, si $q$ désigne un irréductible divisant $a$, $q$ divise $b$ ou $c$. Il résulte alors de l'égalité $(*)$ que $a$ divise $b$ ou $c$.

On a donc montré que tout irréductible est premier, comme attendu. $\square$

**2.9.** Il reste à examiner les cas $n = 3$ et $n = 4$. Dans ces deux cas, le lemme 2.7 tombe en défaut. La démonstration de cet énoncé repose en effet sur l'absence de morphisme $\mathfrak{A}_n \to k^*$ non trivial (garantie dès que $\mathfrak{A}_n$ est simple). Si $n = 3$, $\mathfrak{A}_3$ est le groupe cyclique $\mathbf{Z}/3\mathbf{Z}$, qui peut s'envoyer injectivement dans $k^*$ (pourvu que $k$ contienne une racine cubique de l'unité non triviale). Si $n = 4$, $\mathfrak{A}_4$ s'envoie surjectivement sur $\mathbf{Z}/3\mathbf{Z}$, qui à nouveau peut s'envoyer injectivement dans $k^*$ (sous la même condition). Notons tout de même que si cette condition sur le corps $k$ n'est pas remplie, on a :

**Proposition 2.10.** *Si $n = 3$ ou $4$, et si $k$ est un corps dont la seule racine cubique de l'unité est $1$ (par exemple, $k = \mathbf{R}$ ou $\mathbf{Q}$), alors l'anneau $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ est factoriel.*

*Démonstration.* Il suffit de remarquer que le lemme 2.7 est encore vrai dans ce cas, puisqu'il n'y a pas de morphisme non trivial de $\mathfrak{A}_n$ dans $k^*$. $\square$

**Proposition 2.11.** *Si $n = 3, 4$, et si $k$ contient une racine cubique de l'unité non triviale, alors l'anneau $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ n'est pas factoriel*[10].

9. *C'est exactement là qu'intervient la simplicité de $\mathfrak{A}_n$, ou, plus exactement, l'absence de morphisme non trivial de $\mathfrak{A}_n$ dans $k^*$.*

10. Le groupe des classes de diviseurs de cet anneau est en fait d'ordre 3 (voir remarque 2.12).

*Démonstration.* Il suffit de montrer que chacun des anneaux considérés contient un élément irréductible non premier.

Soit $\zeta \in k$ une racine cubique de l'unité non triviale.

Si $n = 3$, considérons les polynômes $p_1 = X_1 + \zeta X_2 + \zeta^2 X_3$ et $p_2 = X_1 + \zeta^2 X_2 + \zeta X_3$, et leur produit [11] $a = p_1 p_2$. Ce polynôme est invariant sous l'action de $\mathfrak{A}_3$, et on vérifie aisément qu'il est irréductible dans $k[X_1, X_2, X_3]^{\mathfrak{A}_3}$.

Remarquons alors que les polynômes $b_1 = p_1^3$ et $b_2 = p_2^3$ sont également invariants sous $\mathfrak{A}_3$. Il n'y a plus qu'à constater que, dans $k[X_1, X_2, X_3]^{\mathfrak{A}_3}$, $a$ divise leur produit $b_1 b_2$, mais ne divise aucun des deux : $a \in k[X_1, X_2, X_3]^{\mathfrak{A}_3}$ est donc un élément irréductible mais non premier [12].

Si $n = 4$ on procède de la même manière, en se rappelant que $\mathbf{Z}/3\mathbf{Z}$ apparaît ici comme le quotient de $\mathfrak{A}_4$ par son sous-groupe dérivé $D(\mathfrak{A}_4) = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Les polynômes $q_{12} = X_1X_2 + X_3X_4$, $q_{13} = X_1X_3 + X_2X_4$, et $q_{14} = X_1X_4 + X_2X_3$ sont invariants sous l'action de $D(\mathfrak{A}_4)$. On considère alors les polynômes

$$p_1 = q_{12} + \zeta q_{13} + \zeta^2 q_{14}, \text{ et } p_2 = q_{12} + \zeta^2 q_{13} + \zeta q_{14},$$

et leur produit $a = p_1 p_2$. On vérifie que ce produit est irréductible dans $k[X_1, X_2, X_3, X_4]^{\mathfrak{A}_4}$. On conclut comme dans le cas $n = 3$, en constatant qu'il divise le produit des deux polynômes invariants $b_1 = p_1^3$ et $b_2 = p_2^3$, mais ne divise aucun des deux. □

**Remarque 2.12.** Voici quelques remarques précisant le défaut de factorialité constaté dans la proposition précédente. L'objet construit pour mesurer le manque de factorialité d'un anneau $A$ est son *groupe des classes de diviseurs*, souvent noté $\mathrm{Cl}(A)$. Définir ce groupe des classes de diviseurs nous emmènerait bien trop loin [13]. Signalons simplement que, dans les cas considérés dans la proposition, ce groupe est d'ordre 3, et est engendré par (la classe de) l'idéal $I = (a, b_1)$ (où $a$ et $b_1$ sont les polynômes introduits au cours de la démonstration précédente).

Précisons ici à titre de curiosité les raisons qui font que cet idéal est bien d'ordre 3. Montrons d'abord que son cube est trivial : $I^3 = (a^3, a^2 b_1, a b_1^2, b_1^3)$ est le produit de l'idéal principal $(b_1)$ et de l'idéal $J = (b_2, a^2, a b_1, b_1^2)$, qui n'est visiblement contenu dans aucun idéal principal fractionnaire ne contenant pas l'anneau $k[X_i]^{\mathfrak{A}_n}$ (en effet, dire que $J$ est contenu dans l'idéal divisoriel $(\frac{\alpha}{\beta})$ implique en particulier que $\alpha$ divise $\beta b_2$ et $\beta b_1^2$, et donc aussi $\beta$, de sorte que $(\frac{\alpha}{\beta})$ contient l'anneau entier).

Il n'est pas plus difficile de vérifier que $I$ est non trivial. Il faut montrer qu'il n'est pas principal, ce qui est clair, et qu'il est contenu dans un idéal principal fractionnaire ne contenant pas $k[X_i]^{\mathfrak{A}_n}$. Il suffit pour cela de remarquer qu'il est contenu dans l'idéal fractionnaire $(\frac{a}{b_2})$ engendré par $\frac{a}{b_2}$ (ce qui résulte des égalités $a = b_2 \frac{a}{b_2}$ et $b_1 = a^2 \frac{a}{b_2}$) [14].

---

11. Mais d'où une telle idée peut-elle bien sortir ? Il est en fait naturel de partir de polynômes mettant en défaut le lemme 2.7, comme $p_1$ et $p_2$ (en effet, le polynôme $\pi_i$ associé à $p_i$ suivant le lemme 2.7 est (associé à) $p_i$, qui n'est pas invariant sous $\mathfrak{A}_3$). On trouve de tels polynômes en diagonalisant l'action de $\mathfrak{A}_3$ : en fait $p_1$ et $p_2$ sont des vecteurs propres de $(1,2,3) \in \mathfrak{A}_3$. L'idée est alors de considérer un polynôme invariant sous $\mathfrak{A}_3$, mais qui ne peut s'écrire sous la forme $(*)$ rencontrée au cours de la démonstration du théorème 2.8. Le produit $p_1 p_2$ remplit ces conditions.

12. Il n'est pas difficile de voir que $b_1$ et $b_2$ définissent deux irréductibles de $k[X_1, X_2, X_3]^{\mathfrak{A}_3}$, et que l'égalité

$$a^3 = b_1 b_2$$

montre alors que l'unicité de la décomposition en produit d'irréductibles n'a pas lieu dans l'anneau considéré. Notons que $a$ est symétrique (et s'écrit $a = s_1^2 - 3s_2$), tandis que $b_1$ et $b_2$ ne le sont pas (on a $(1,2)b_1 = b_2$).

13. On pourra consulter Bourbaki, *Algèbre commutative VII*, ou bien Samuel, *Lectures on unique factorisation domains* (ou encore Fossum, *The divisor class group of a Krull domain*).

14. En fait $I$ est même égal à l'intersection $(\frac{a}{b_2}) \cap k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ de cet idéal fractionnaire avec l'anneau des polynômes invariants sous $\mathfrak{A}_n$ (l'intersection étant prise dans le corps des fractions de cet anneau). Soit en effet $p \in k[X_1, X_2, X_3]^{\mathfrak{A}_3}$ appartenant à l'idéal fractionnaire $(\frac{a}{b_2})$. Un tel polynôme est un multiple de $p_1$ (dans $k[X_1, X_2, X_3]$) : il existe un polynôme $q$ tel que $p = p_1 q$. Soit $\sigma = (1,2,3)$ le cycle tel que $\sigma p_1 = \zeta^2 p_1$. Alors $q$ vérifie l'identité $\sigma q = \zeta q$ (on dit que $q$ est un *semi-invariant*). Il suffit alors de décrire l'ensemble des polynômes vérifiant cette relation. La donnée des trois vecteurs propres $p_1$, $p_2$ et $p_0 = X_1 + X_2 + X_3$ correspondant à l'action de $\sigma$ sur les polynômes homogènes de degré 1 suggère d'écrire $q$ sous la forme $p = \sum a_{ijk} p_0^i p_1^j p_2^k$.

En conclusion, voici le joli théorème auquel on est parvenu :

**Théorème 2.13.** *Soit $n \geqslant 3$.*

*Si $n \geqslant 5$ ou si $k$ ne contient pas de racine cubique de l'unité non triviale, alors l'anneau $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$ des polynômes invariants sous $\mathfrak{A}_n$ est factoriel.*

*Dans les autres cas, il ne l'est pas.*

**Remarque 2.14.** On a en particulier obtenu un exemple naturel de $\mathbf{R}$-algèbre factorielle $A = \mathbf{R}[X_1, X_2, X_3]^{\mathbf{Z}/3\mathbf{Z}}$ (ou $\mathbf{R}[X_1, X_2, X_3, X_4]^{\mathfrak{A}_4}$) dont l'algèbre complexifiée $A \otimes_{\mathbf{R}} \mathbf{C}$ n'est pas factorielle.

## 3. Pour aller plus loin

Je ne résiste pas à l'envie de dire un mot de la géométrie à peine cachée derrière l'étude précédente. Plaçons nous sur le corps des nombres complexes $\mathbf{C}$. Le groupe symétrique $\mathfrak{S}_n$ opère sur $\mathbf{C}^n$ par permutation des coordonnées. Considérons le quotient (ensembliste)

$$\mathbf{C}^n/\mathfrak{S}_n.$$

Cet ensemble est naturellement muni d'une topologie quotient, dont on vérifie qu'elle est séparée (cela résulte des bonnes propriétés de l'action de $\mathfrak{S}_n$ sur $\mathbf{C}^n$). En fait on peut vérifier que ce quotient est homéomorphe à $\mathbf{C}^n$, un homéomorphisme étant obtenu à partir de l'application $\varphi = (s_1, \ldots s_n)$ (où les $s_i$ sont les fonctions symétriques élémentaires, vues comme applications $\mathbf{C}^n \to \mathbf{C}$) :

$$\begin{array}{cccc} \varphi & : & \mathbf{C}^n & \longrightarrow & \mathbf{C}^n \\ & & (x_1, \ldots, x_n) & \longmapsto & (x_1 + \ldots + x_n, \ldots, x_1 \cdots x_n). \end{array}$$

On a évidemment $\varphi \circ \sigma = \varphi$ pour tout $\sigma \in \mathfrak{S}_n$, de sorte que $\varphi$ passe au quotient :

$$\begin{tikzcd} \mathbf{C}^n \arrow[r, "\varphi"] \arrow[d] & \mathbf{C}^n \\ \mathbf{C}^n/\mathfrak{S}_n. \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

On vérifie que $\tilde{\varphi}$ est un homéomorphisme [15].

L'analogie entre cet isomorphisme $\mathbf{C}^n/\mathfrak{S}_n \xrightarrow{\sim} \mathbf{C}^n$ (donné par les fonctions symétriques) et l'isomorphisme $k[s_1, \ldots, s_n] \xrightarrow{\sim} k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ n'est pas fortuite.

Considérons alors l'action de $\mathfrak{A}_n$ sur $\mathbf{C}^n$. On a de même un espace quotient $\mathbf{C}^n/\mathfrak{A}_n$, que l'on peut réaliser comme un fermé de $\mathbf{C}^{n+1}$ en considérant l'image de l'application $\psi = (\varphi, v) \colon \mathbf{C}^n \to \mathbf{C}^n \times \mathbf{C}, x \mapsto (\varphi(x), v(x))$, où $v \colon \mathbf{C}^n \to \mathbf{C}$ est l'application $(x_i)_i \mapsto \prod_{i<j}(x_i - x_j)$.

De plus, $\mathbf{C}^n/\mathfrak{A}_n$ est naturellement muni d'une action de $\mathbf{Z}/2\mathbf{Z}$, ou, autrement dit, d'une involution $\iota$, telle que le quotient

$$p \colon \mathbf{C}^n/\mathfrak{A}_n \to (\mathbf{C}^n/\mathfrak{A}_n)/\iota \simeq \mathbf{C}^n/\mathfrak{S}_n \simeq \mathbf{C}^n$$

fasse de $\mathbf{C}^n/\mathfrak{A}_n$ est un *revêtement (ramifié) double* de $\mathbf{C}^n$. Les « mauvais » points de $\mathbf{C}^n$ sont ceux qui ont un seul antécédent : ils forment ce qu'on appelle le *lieu de branchement* de $p$. Sa préimage dans $\mathbf{C}^n/\mathfrak{A}_n$ est appelée *lieu de ramification.*

Comment décrire ce lieu de branchement ? Par définition, il est constitué des points $(a_1, \ldots, a_n)$ dont la préimage par $\varphi$ ne contient qu'une orbite sous $\mathfrak{A}_n$. On a déjà remarqué (cf. footnote 15) que cette préimage est l'ensemble des $(x_1, \ldots, x_n)$ où les $x_i$ sont exactement

---

La semi-invariance de $q$ montre que $a_{ijk} = 0$ si $2j + k \neq 1 \mod 3$, ce qui permet d'écrire $q$ sous la forme $q = p_2 r + p_1^2 s$ avec $r, s$ polynômes invariants sous $\mathfrak{A}_3$. D'où finalement $p = p_1 q = p_1 p_2 r + p_1^3 s \in (a, b_1) = I$.

15. Par exemple en remarquant que la préimage par $\varphi$ d'un point $(a_1, \ldots, a_n)$ est exactement l'ensemble des $(x_1, \ldots, x_n)$ tels que $\prod(X - x_i) = X^n - a_1 X + \cdots + (-1)^n a_n$, qui est toujours non vide (d'où la surjectivité), et qui détermine bien une unique orbite sous $\mathfrak{S}_n$ (d'où l'injectivité de $\tilde{\varphi}$). La continuité de $\tilde{\varphi}$ est automatique (par définition de la topologie quotient). Il reste à montrer qu'elle est ouverte. Cela peut se voir à la main, ou bien en montrant que $\varphi$ est un difféomorphisme local (le calcul du jacobien de $\varphi$ étant un exercice non trivial).

les racines de $\Pi_{(a_i)}(X) = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n$. Dire qu'ils sont tous conjugués sous $\mathfrak{A}_n$ signifie que ce polynôme a au moins une racine double, autrement dit que son discriminant $\Delta = \prod_{i<j}(x_i - x_j)^2$ est nul. En se rappelant que $\Delta$ est un polynôme en les $s_i$, on voit que le lieu de branchement est une hypersurface de $\mathbf{C}^n$ : c'est le lieu des zéros de $\Delta$. Ce lieu de branchement est aussi l'image par $\varphi$ de l'hyperplan $x_1 = x_2$ de $\mathbf{C}^n$. C'est donc un fermé « irréductible »[16]. Cet énoncé topologique est à rapprocher de l'irréductibilité de $\Delta$ dans $k[s_1, \ldots, s_n]$ (cf. proposition 2.4).

Le lieu de ramification lui est homéomorphe. Il est donc également irréductible. On retrouve ainsi l'irréductibilité de $T$ dans l'anneau quotient $k[s_1 \ldots, s_n, T]/T^2 - \Delta$.

On peut également s'intéresser au lieu de ramification de la projection $\mathbf{C}^n \to \mathbf{C}^n/\mathfrak{A}_n$ (qui est le lieu des points de $\mathbf{C}^n$ au voisinage desquels $\mathbf{C}^n \to \mathbf{C}^n/\mathfrak{A}_n$ n'est pas un homéomorphisme local). C'est un fermé de codimension au moins 2 : il ne peut être défini par une seule équation. Dans le cas $n = 3$, on peut aussi remarquer que le fermé de $\mathbf{C}^3/\mathfrak{A}_3$ défini par les équations de l'idéal $I = (a, b_1)$ évoqué dans la remarque 2.12 est l'image de l'hyperplan de $\mathbf{C}^3$ d'équation $x_1 + \zeta x_2 + \zeta^2 x_3 = 0$.

16. pour la topologie de Zariski ! Rappelons qu'un espace topologique non vide $X$ est dit irréductible si l'intersection de deux ouverts non vides de $X$ est toujours non vide, soit encore si on ne peut pas le recouvrir par deux fermés propres $F, F' \subsetneq X$.