# Autour du problème de Nœther concernant les groupes alternés

Rapport du stage effectué sous la direction de Mathieu Florence,

maître de conférence à l'Institut de Mathématiques de Jussieu.

Sylvain Gaulhiac

*Juin 2013*

## Introduction

Soit $k$ un corps et $G$ un groupe fini. Considérons alors l'action régulière du groupe $G$ sur l'ensemble des indéterminées $\{X_g\}_{g\in G}$ ( ie pour $g,h \in G$ : $g.X_h = X_{gh}$ ). Soit $k(G) = k(\{X_g\})^G$ le corps des points fixes sous cette action. C'est une extension du corps $k$. Le problème de Nœther de $G$ sur $k$ consiste à savoir si l'extension de corps $k(G)/k$ est rationnelle, autrement dit si elle est transcendante pure, c'est-à-dire engendrée par un nombre fini d'éléments qui forment une famille algébriquement libre sur $k$. Nous savons que ce problème admet une réponse positive pour les groupes symétriques $S_n$ (quel que soit le corps $k$) ou pour tout groupe abélien fini sur $\mathbb{C}$. Il est également connu que la réponse est négative pour certains groupes (même si le corps $k$ est algébriquement clos). Cependant le problème reste ouvert pour la plupart des groupes.

Par ailleurs, pour tout entier naturel $n \leqslant 1$ les groupes $S_n$ et $A_n$ agissent aussi sur $k(X_1,\dots,X_n)$ en permuttant les indéterminées $X_1,\dots,X_n$. Notons alors respectivement $k(X_1,\dots,X_n)^{S_n}$ et $k(X_1,\dots,X_n)^{A_n}$ les sous-corps des points fixes pour ces actions. Ce sont des extensions de k, et nous pouvons donc nous demander si elles sont rationnelles (c'est en fait le problème de Nœther, sauf que ce n'est plus l'action régulière que l'on considère). La réponse est 'oui' pour le groupe symétrique $S_n$ (pour tout entier naturel $n$ et tout corps $k$) car il est connu que $k(X_1,\dots,X_n)^{S_n} = k(\sigma_1,\dots,\sigma_n)$ où $\sigma_i$ est le polynôme élémentaire de degré $i$ en les $X_1,\dots,X_n$. Nous savons aussi que la réponse est positive pour les groupes alternés $A_n$ avec $n \leqslant 5$, mais le problème reste ouvert lorsque $n > 5$.

L'article est structuré comme suit. Dans la section 1, nous montrerons le résultat principal de ce texte (théorme 1.7) qui est le suivant : si $n \geqslant 2$ est un entier pair et $k$ un corps de caractéristique différente de 2, alors il y a un isomorphisme de corps

$$k(X_1,\dots,X_{n+1})^{A_{n+1}} \cong k(X_1,\dots,X_n)^{A_n}(X)$$

où $X$ est une indéterminée. Ce résultat est déjà connu mais la présente démonstration est inédite, et plus élémentaire que celle déjà existante dans [Plans].
Dans la section 2, nous donnerons une application de ce résultat pour montrer que l'extension $k(X_1,\dots,X_5)^{A_5}/k$ est rationnelle. Enfin dans la section 3 nous verrons comment à partir de là il est possible de revenir au problème de Noether.

# 1. Première partie

## 1.1. Résultats préliminaires.

Dans toute cette partie on considère un corps $k$ de caractéristique différente de 2. Notons $\overline{k}$ sa clôture algébrique.

Lemme 1.1. *Soit $n \geqslant 3$ un entier impair et $P \in k[X]$ un polynôme de degré $n$ unitaire, séparable dont on note $x_1, \ldots, x_n$ ses racines dans $\overline{k}$. Pour $1 \leqslant i \neq j \leqslant n$ posons $u_{ij} := \frac{1}{x_i - x_j}$ et $u_{ii} = 0$. Soit $\mathcal{M}_\mathcal{P}$ la matrice de terme général $u_{ij}$, c'est une matrice antisymétrique (donc de rang pair) de taille $n$. Supposons que $\mathrm{rg}(\mathcal{M}_\mathcal{P}) = n-1$, que la somme des composantes d'un vecteur non nul du noyau ne soit pas nulle et qu'aucune de ces composantes ne soit nulle.*
*Alors il existe de manière unique des polynômes unitaires $R, Q \in k[X]$ tels que :*

(1) $\deg(Q) = \deg(R) = n-1$
(2) *$P$ et $R$ sont premiers entre eux.*
(3) $P'Q - Q'P = R^2$ $(*)$

**Démonstration.** Cherchons $\frac{Q}{P}$ et $\frac{R}{P}$ sous leur forme développée en éléments simples :

$$\frac{Q}{P} = \sum_{i=1}^{n} \frac{\alpha_i}{X - x_i},\ \alpha_i \in k(x_1, \ldots, x_n)$$

$$\frac{R}{P} = \sum_{i=1}^{n} \frac{\beta_i}{X - x_i},\ \beta_i \in k(x_1, \ldots, x_n)$$

L'égalité $(*)$ est équivalente à

$$\left(\frac{Q}{P}\right)' = -\left(\frac{R}{P}\right)^2$$

En utilisant l'unicité de la décomposition en éléments simples on voit après calculs que cette égalité est équivalente à : Pour tout $1 \leqslant i \leqslant n$,

$$\begin{cases} 2\beta_i \Sigma_{j=1}^{n} u_{ij}\beta_j = 0 \\ \alpha_i = {\beta_i}^2 \end{cases}$$

Or $\mathrm{car}(k) \neq 2$ et aucun des $\beta_i$ ne doit être nul, car sinon $x_i$ est aussi une racine de $R$ et ainsi $P$ et $R$ ne sont pas premiers entre eux. On est donc amené à résoudre le système : Pour tout $1 \leqslant i \leqslant n$,

$$\begin{cases} \Sigma_{j=1}^{n} u_{ij}\beta_j = 0 \\ \alpha_i = {\beta_i}^2 \end{cases}$$

Par conséquent le vecteur des $\beta_i$ (noté ß) doit être dans $\ker(\mathcal{M}_\mathcal{P})$. Or ce noyau est une droite vectorielle d'après les hypothèses, et le fait d'imposer $Q$ unitaire détermine alors de manière unique les $\alpha_i$, donc aussi ß au signe près.
Réciproquement, les polynômes $Q$ et $R$ ainsi construits vérifient l'égalité $(*)$, $Q$ est unitaire et $R$ est premier avec $P$ car aucun des $\beta_i$ n'est nul (d'après les hypothèses sur $\mathcal{M}_\mathcal{P}$). Comme $\sum_{i=1}^{n} \beta_i \neq 0$, $R$ est bien de degré $n-1$, donc $Q$ l'est aussi. Par conséquent le polynôme $P'Q - Q'P$ est unitaire, et l'on peut ainsi choisir ß tel que $R$ soit unitaire, ce qui détermine ce dernier de manière unique.
On a donc des uniques polynômes $Q, R \in k(x_1, \ldots, x_n)[X]$ qui vérifient les

conditions de l'énoncé dans le corps $k(x_1, \ldots, x_n)$. Il nous reste à montrer qu'ils sont à coefficients dans $k$.

Soit $g \in \mathrm{Gal}(k(x_1, \ldots, x_n)/k)$. En appliquant $g$ à l'égalité polynomiale $(*)$ (ie en appliquant $g$ à chaque coefficient) on obtient : $g(P)'g(Q) - g(Q)'g(P) = g(R)^2$. Or comme $P \in k[X]$ on a $g(P) = P$. De là,

$$P'g(Q) - g(Q)'P = g(R)^2$$

Or $g(Q), g(R) \in k(x_1, \ldots, x_n)[X]$ vérifient les conditions de l'énoncé, et par unicité on a : $\begin{cases} g(Q) = Q \\ g(R) = R \end{cases}$
Cela montre donc que :

$$Q \in k[X]$$

$$R \in k[X].$$

□

*Remarque* 1.2. La condition de non annulation des composantes d'un vecteur non nul du noyau de $\mathcal{M}_{\mathcal{P}}$ est vérifiée lorsque $P$ est irréductible dans $k[X]$. En effet soit $G$ le groupe de Galois de l'extension $k \subset k(x_1, \ldots, x_n)$. Puisque $P$ est irréductible, l'action de $G$ sur les racines $x_i$ est transitive. Par unicité de la décomposition en éléments simples de $\frac{R}{P}$, on voit aisément que si $g \in G$, $g(\beta_i) = \beta_j$ dès que $g(X_i) = X_j$. Par transitivité de l'action de $G$ sur les $x_i$, la nullité d'un seul des $\beta_i$ entraîne la nullité de tous les $\beta_i$, ce qui est impossible.

*Remarque* 1.3. Les conditions sur la non nullité des composantes d'un vecteur non nul du noyau ainsi que la non nullité de la somme de ces composantes se traduisent par des expressions symétriques en les $\beta_i$, donc en les $x_i$, donc également en les coefficients de $P$. De là il existe un polynôme $H$ universel en les coefficients de $P$ tel que si un $P$ donné n'annule pas ce polynôme (on dit alors que $P$ est $H$-général), alors ces conditions sont vérifiées.

Lemme 1.4. *Soit $n \geqslant 2$ un entier pair et $Q \in k[X]$ un polynôme de degré $n$ unitaire, séparable ne s'annulant pas sur $k$ tout entier (cela est en particulier vérifié lorsque $k$ est infini) dont on note $x_1, \ldots, x_n$ ses racines dans $\overline{k}$. Soit $x \in k$ tel que $Q(x) \neq 0$. Pour $1 \leqslant i \neq j \leqslant n$ posons $u_{ij} := \frac{1}{x_i - x_j}$ et $u_{ii} = 0$. Soit $\mathcal{M}_{\mathcal{Q}}$ la matrice de terme général $u_{ij}$, c'est une matrice antisymétrique (donc de rang pair) de taille $n$. Supposons qu'elle soit inversible. Si $v$ désigne le vecteur de taille $n$ qui ne contient que des* 1*, supposons également que ${\mathcal{M}_{\mathcal{Q}}}^{-1}.v$ n'ait aucune composante nulle.*
*Alors il existe de manière unique des polynômes unitaires $R, P \in k[X]$, tels que :*

(1) $\deg(P) = n + 1$ *et* $\deg(R) = n$
(2) $P(x) = 0$
(3) $Q$ *est premier avec* $R$ *ainsi qu'avec* $P$.
(4) $P'Q - Q'P = R^2$ $(*)$

**Démonstration.** Cherchons $\frac{P}{Q}$ et $\frac{R}{Q}$ sous leur forme développée en éléments simples :

$$\frac{P}{Q} = X + b + \sum_{i=1}^{n} \frac{\alpha_i}{X - x_i},\ b,\ \alpha_i \in k(x_1, \ldots, x_n)$$

$$\frac{R}{Q} = 1 + \sum_{i=1}^{n} \frac{\beta_i}{X - x_i},\ \beta_i \in k(x_1, \ldots, x_n)$$

L'égalité $(*)$ est équivalente à

$$\left(\frac{P}{Q}\right)' = \left(\frac{R}{Q}\right)^2$$

En utilisant l'unicité de la décomposition en éléments simples on voit après calculs que cette égalité est équivalente à : Pour tout $1 \leqslant i \leqslant n$,

$$\begin{cases} 2\beta_i.(1 + \Sigma_{j=1}^{n} u_{ij}\beta_j) = 0 \\ \alpha_i = -{\beta_i}^2 \end{cases}$$

Or aucun des $\beta_i$ ne doit être nul, car sinon $x_i$ est aussi une racine de $R$ et ainsi $Q$ et $R$ ne sont pas premiers entre eux. On est donc amené à résoudre le système : Pour tout $1 \leqslant i \leqslant n$,

$$\begin{cases} 1 + (\Sigma_{j=1}^{n} u_{ij}\beta_j) = 0 \\ \alpha_i = -{\beta_i}^2 \end{cases}$$

Par conséquent le vecteur des $\beta_i$ (noté ß) doit vérifier $\mathcal{M}_{\mathcal{Q}}.ß = -v$ ie $ß = -{\mathcal{M}_{\mathcal{Q}}}^{-1}.v$. Cela détermine de manière unique les $\beta_i$ et les $\alpha_i$. Par ailleurs le fait d'imposer $P(x) = 0$ détermine de manière unique $b$, et l'on construit de cette manire des polynômes $P$ et $R$ uniques.
Réciproquement, les polynômes $P$ et $R$ ainsi construits vérifient l'égalité $(*)$ ainsi que $P(x) = 0$, sont respectivement de degré $n + 1$ et $n$, sont unitaires, $R$ est premier avec $Q$ car aucun des $\beta_i$ n'est nul (d'après les hypothèses sur ${\mathcal{M}_{\mathcal{Q}}}^{-1}.v$) et $Q$ est premier avec $P$ car aucun des $\alpha_i$ n'est nul puisqu'aucun des $\beta_i$ ne l'est.
On a donc des uniques polynômes $R, P \in k(x_1, \ldots, x_n)[X]$ qui vérifient les conditions de l'énoncé dans le corps $k(x_1, \ldots, x_n)$. Il nous reste à montrer qu'ils sont à coefficients dans $k$.

Soit $g \in \mathrm{Gal}(k(x_1, \ldots, x_n)/k)$. En appliquant $g$ à l'égalité polynomiale $(*)$ (ie en appliquant $g$ à chaque coefficient) on obtient : $g(P)'g(Q) - g(Q)'g(P) = g(R)^2$. Or comme $Q \in k[X]$ on a $g(Q) = Q$. De là,

$$g(P)'Q - Q'g(P) = g(R)^2$$

Or $g(P), g(R) \in k(x_1, \ldots, x_n)[X]$ vérifient les conditions de l'énoncé, dont en particulier $g(P)(x) = 0$ et par unicité l'on a : $\begin{cases} g(P) = P \\ g(R) = R \end{cases}$
Cela montre donc que :

$$P \in k[X]$$

$$R \in k[X].$$

□

1.2. Résultat concernant le discriminant.

Rappelons tout d'abord quelques propriétés concernant le résultant de deux polynômes. Si $P$, $Q$ et $R$ sont des polynômes de $k[X]$ avec $\deg(P) = p \geqslant 1$ et $\deg(Q) = q \geqslant 1$, et $\lambda, \mu \in k$, alors :

$$\begin{aligned}\mathrm{res}(P,Q) &= (-1)^{pq}\mathrm{res}(Q,P)\\ \mathrm{res}(P,QR) &= \mathrm{res}(P,Q).\mathrm{res}(P,R)\\ \mathrm{res}(\lambda P,\mu Q) &= \lambda^q\mu^p\mathrm{res}(P,Q)\end{aligned}$$

Si $P$ est de coefficient dominant $a_p$ et que $\{\alpha_1,\ldots,\alpha_p\}$ est l'ensemble de ses racines dans $\overline{k}$, alors :

$$\mathrm{res}(P,Q) = a_p^q \prod_{1\leqslant i\leqslant p} Q(\alpha_i)$$

Définition 1.5. *Si $P$ est un polynôme de $k[X]$ de coefficient dominant $a_p$ avec $\deg(P) = p \geqslant 2$, on définit le discriminant de $P$ comme :*

$$\Delta(P) = (-1)^{\frac{p(p-1)}{2}} a_p^{-1}.\mathrm{res}(P,P')$$

*Par ailleurs si $\{\alpha_1,\ldots,\alpha_p\}$ est l'ensemble de ses racines dans $\overline{k}$, alors :*

$$\Delta(P) = a_p^{2p-2} \prod_{1\leqslant i<j\leqslant p} (\alpha_i-\alpha_j)^2$$

Proposition 1.6. *Soit $n \geqslant 2$ un entier pair. Supposons que l'on ait des polynômes $P,Q,R \in k[T]$ unitaires tels que $Q\wedge R = 1$, $Q$ séparable, $\deg(P) = n+1$, $\deg(Q) = \deg(R) = n$ , et qui vérifient l'égalité : $P'Q - Q'P = R^2$. Si $X$ désigne une indéterminée, posons : $\widetilde{P}(T) := P(T) - XQ(T) \in k(X)[T]$.*
*Alors il existe $S \in k(X)$ tel que :*

$$\Delta(\widetilde{P}) = S^2.\Delta(Q)$$

**Démonstration.** Posons :

$$U(X) := \mathrm{res}(P - XQ, R) \in k(X)$$

En vertu des propriétés sur le résultant, on a :

$$\begin{aligned}U^2(X) &= \mathrm{res}(P-XQ,R^2) = \mathrm{res}(P-XQ,P'Q-Q'P)\\ &= \mathrm{res}(P-XQ,P'Q-Q'P+Q'(P-XQ))\\ &= \mathrm{res}(P-XQ,P'Q-TQQ') = \mathrm{res}(P-XQ,Q).\mathrm{res}(P-XQ,P'-XQ')\\ &= (-1)^{\frac{n(n+1)}{2}}\mathrm{res}(P,Q)\Delta(\widetilde{P}).\end{aligned}$$

Posons maintenant: $V(X) := \mathrm{res}(Q,R) \in k(X)$

$$\begin{aligned}V^2 &= \mathrm{res}(Q,R^2) = \mathrm{res}(Q,P'Q-Q'P)\\ &= \mathrm{res}(Q,-Q'P) = \mathrm{res}(Q,Q'P)\\ &= \mathrm{res}(Q,P).\mathrm{res}(Q,Q')\\ &= (-1)^{\frac{n(n-1)}{2}}\mathrm{res}(P,Q).\Delta(Q).\end{aligned}$$

Puisque $Q$ est séparable $\Delta(Q)$ est non nul, et en regroupant ces deux égalités l'on obtient : $U^2 = \frac{V^2}{\Delta(Q)}\Delta(\widetilde{P})$.

Puisque $Q$ et $R$ sont premiers entre eux $V$ est non nul, et en posant $S = \frac{U}{V} \in k(X)$ l'on obtient finalement :

$$\Delta(\widetilde{P}) = S^2.\Delta(Q)$$

□

1.3. Exemple.

Nous allons ici donner un exemple de polynômes $P$, $Q$ et $R$ qui illustrent à la fois le lemme 1.1 et le lemme 1.4, mais qui nous sera surtout utile par la suite pour démontrer le théorème principal. Supposons aussi que $\mathrm{car}(k) > 3n-6$. Soit $n \geqslant 3$ un entier impair. Posons :

$$\begin{cases} P(X) = X^n - X \\ Q(X) = X^{n-1} - \left(\frac{n-2}{n}\right)^2 \\ R(X) = X^{n-1} + \frac{n-2}{n} \end{cases}$$

Le lecteur pourra aisément vérifier que $P'Q - Q'P = R^2$. Montrons maintenant que ces polynômes vérifient toutes les conditions des lemmes 1.1 et 1.4. Tout d'abord il est évident que $P$ et $Q$ sont unitaires séparables, que $\deg(P) = n$ et $\deg(Q) = \deg(R) = n-1$. Comme aucun de ces trois polynômes n'a de racine commune avec un autre, alors $P \wedge R = Q \wedge R = Q \wedge P = 1$. Il nous reste à vérifier les conditions sur les matrices $\mathcal{M}_{\mathcal{P}}$ et $\mathcal{M}_{\mathcal{Q}}$.
Soit $z$ une racine primitive $n-1^{ieme}$ de l'unité. Alors $0, 1, z, z^2, \ldots, z^{n-2}$ sont les racines de $P$. Comme $\mathcal{M}_{\mathcal{P}}$ est antisymétrique elle est de rang pair, donc $\mathrm{rg}(\mathcal{M}_{\mathcal{P}}) \leqslant n-1$. Pour montrer que $\mathrm{rg}(\mathcal{M}_{\mathcal{P}}) = n-1$ il suffit donc de montrer que la sous-matrice $\widetilde{\mathcal{M}_{\mathcal{P}}}$ carrée de taille $n-1$ obtenue à partir de $\mathcal{M}_{\mathcal{P}}$ en enlevant la première ligne et la première colonne est inversible. Pour $1 \leqslant i \leqslant n-2$ posons : $a_i := (1-z^i)^{-1}$ et $a_0 := 0$. La matrice $\widetilde{\mathcal{M}_{\mathcal{P}}}$ est formée des lignes $(a_0, \ldots, a_{n-2}), z(a_{n-2}, a_0, \ldots, an-3), z^2(a_{n-3}, a_{n-2}, a_0, \ldots, a_{n-4}), \ldots$.
Par conséquent le déterminant de $\widetilde{\mathcal{M}_{\mathcal{P}}}$ est égal à une racine de l'unité près au déterminant de la matrice circulante :

$$\mathcal{A} := \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}.$$

Or les valeurs propres de $\mathcal{A}$ sont les

$$\lambda_k := \sum_{i=0}^{n-2} a_i (z^k)^i = \sum_{i=1}^{n-2} \frac{(z^k)^i}{1-z^i}\ ,\ 0 \leqslant k \leqslant n-2$$

donc

$$\det(\mathcal{A}) = \prod_{k=0}^{n-2} \lambda_k.$$

Or on peut remarquer que $\lambda_k = \mathrm{Tr}(\frac{z^k}{1-z})$, la trace étant prise par rapport au polynôme $(X^{n-1}-1)/(X-1)$. Remarquons aussi que pour $i \geqslant 1$ :

$$\mathrm{Tr}(\frac{z^{i+1}}{1-z}) - \mathrm{Tr}(\frac{z^i}{1-z}) = \mathrm{Tr}(-z^i) = 1.$$

Ainsi il suffit de connaître $\mathrm{Tr}(\frac{1}{1-z})$ pour pouvoir calculer le déterminant.

$$\begin{aligned}\frac{X^{n-1}-1}{X-1}-(n-1) &= \sum_{k=0}^{n-2}(X^k-1)\\ &= (X-1)\sum_{k=1}^{n-2}\sum_{j=0}^{k-1}X^j\\ &= (X-1)\sum_{j=0}^{n-2}(n-2-j)X^j.\end{aligned}$$

Ainsi dans la $k$-algèbre $\frac{k[X]}{(\frac{X^{n-1}-1}{X-1})}$, $(1-X)$ est inversible, avec :

$$(1-X)^{-1}=\sum_{j=0}^{n-2}\left(\frac{n-2-j}{n-1}\right)X^j$$

De là :

$$\mathrm{Tr}(\frac{1}{1-z})=\frac{(n-2)^2}{n-1}-\sum_{j=1}^{n-2}\left(\frac{n-2-j}{n-1}\right)=\sum_{j=1}^{n-2}\frac{j}{n-1}=\frac{n-2}{2}$$

On en déduit que :

$$\det(\mathcal{A})=\frac{(n-2)n(n+2)(n+4)\dots(3n-6)}{2^{n-1}}\neq 0.$$

Ainsi $\widetilde{\mathcal{M}_{\mathcal{P}}}$ est inversible, et donc

$$\mathrm{rg}(\mathcal{M}_{\mathcal{P}})=n-1.$$

Comme $\mathcal{M}_{\mathcal{Q}}$ est égale à un multiple scalaire près à $\widetilde{\mathcal{M}_{\mathcal{P}}}$, alors l'on en déduit également que $\mathcal{M}_{\mathcal{Q}}$ est inversible.
En outre le fait qu'un vecteur non nul du noyau de $\mathcal{M}_{\mathcal{P}}$ n'ait aucune composante nulle et que la somme de ses composantes soit non nulle est équivalent au fait que $R$ soit premier avec $P$ et de degré $n-1$. Or cela est vérifié. De même le fait qu'aucune composante du vecteur ${\mathcal{M}_{\mathcal{Q}}}^{-1}.v$ ne soit nulle est équivalent au fait que $Q$ et $R$ soient premiers entre eux, ce qui est bien le cas ici.

### 1.4. Démonstration du théoème principal.

Théorème 1.7. *Soit $k$ un corps de caratéristique différente de 2 et $n\geqslant 2$ un entier pair. Si $X, X_1, \dots, X_{n+1}$ sont des indéterminées, alors on a un isomorphisme de corps :*

$$k(X_1,\dots,X_{n+1})^{A_{n+1}}\cong k(X_1,\dots,X_n)^{A_n}(X)$$

**Démonstration.** Dans toute cette démonstration nous utiliserons à plusieurs reprises l'exemple précédent où nous avions besoin que $\mathrm{car}(k)>3n-6$. Cependant je pense que l'on peut trouver des exemples appropriés dès lors que $\mathrm{car}(k)\neq 2$, et je me permettrai de le supposer par la suite. Posons:

$$L_n := k(X_1,\dots,X_n)^{S_n}$$
$$K_n := k(X_1,\dots,X_n)^{A_n}.$$

Définissons :

$$Q(T) := \prod_{i=1}^{n}(T - X_i)$$

C'est un polynôme de $L_n[T]$ car ses coefficients sont des expressions symétriques en ses racines $X_1, \ldots, X_n$. Montrons que $Q$ vérifie toutes les conditions du lemme 1.4 : $Q$ est unitaire, séparable, de degré $n$, et par ailleurs toutes les conditions requises concernant $\mathcal{M}_{\mathcal{Q}}$ sont ici a fortiori vérifiées car elles le sont pour $\mathcal{M}_{\mathcal{Q}}$ dans l'exemple 1.3 (cela a été montré plus haut). De plus $Q(0) \neq 0$, donc $Q$ vérifie toutes les conditions du lemme 1.4. On peut ainsi construire de manière unique les polynômes associés $P, R \in L_n[T]$ en imposant $P(0) = 0$.
Définissons alors :

$$\widetilde{P}(T) = P(T) - XQ(T) \in L_n(X)[T]$$

Soient $Y_1, \ldots, Y_{n+1}$ les racines de $P$ dans $\overline{L_n(X)}$, ie : $\widetilde{P}(T) = \prod_{i=1}^{n+1}(T - Y_i)$. Posons :

$$L_{n+1} := k(Y_1, \ldots, Y_{n+1})^{S_{n+1}}$$

$$K_{n+1} := k(Y_1, \ldots, Y_{n+1})^{A_{n+1}}.$$

$\widetilde{P} \in L_{n+1}[T]$ et ses coefficients engendrent même $L_{n+1}$. Comme l'on a aussi $P \in L_n(X)[T]$, alors :

$$L_{n+1} \subset L_n(X).$$

Montrons maintenant que $\widetilde{P}$ vérifie toutes les conditions du lemme 1.1 en tant qu'élément de $L_n(X)[T]$. $\widetilde{P}$ est unitaire de degré $n+1$, et séparable (car $P$ est séparable dans l'exemple 1.3, donc ici $P$ est également séparable, et comme $P$ est obtenu à partir de $\widetilde{P}$ en posant $X = 0$, alors $\widetilde{P}$ l'est aussi). Par ailleurs toutes les conditions requises concernant $\mathcal{M}_{\widetilde{\mathcal{P}}}$ sont ici vérifiées car elles le sont pour $\mathcal{M}_{\mathcal{P}}$ dans l'exemple 1.3 (et l'on utilise à nouveau le même argument pour passer à $\mathcal{M}_{\widetilde{\mathcal{P}}}$).

Or $Q, R \in L_n[T]$, donc $Q, R \in L_n(X)[T]$. Par ailleurs $Q$ est unitaire, $\deg(Q) \leqslant n$ et $\deg(R) \leqslant n$ et $\widetilde{P}' - Q'\widetilde{P} = P'Q - Q'P = R^2$ donc $\widetilde{P}$, $Q$ et $R$ vérifient l'égalité $(*)$. Comme $P$ et $R$ sont premiers entre eux, alors a fortiori $\widetilde{P}$ et $R$ le sont aussi. Ainsi par unicité $Q$ et $R$ sont les solutions du lemme 1.1 appliqué à $\widetilde{P}$ considéré comme élément de $L_n(X)[T]$. Or comme $L_{n+1} \subset L_n(X)$, les solutions du lemme 1.1 appliqué à $\widetilde{P}$ considéré comme élément de $L_{n+1}[T]$ sont aussi les solutions dans $L_n(X)[T]$. Ainsi on a : $Q \in L_{n+1}[T]$. En prenant $T = 0$ on obtient $\widetilde{P}(0) = -XQ(0) \in L_{n+1}$, et donc $X \in L_{n+1}$. Comme les coefficients de $Q$ engendrent $L_n$ et sont dans $L_{n+1}$ et que par ailleurs $X \in L_{n+1}$, alors :

$$L_n(X) \subset L_{n+1}$$

De là :

$$L_n(X) = L_{n+1} := L.$$

Considérons les extensions $L \subset K_n(X)$ et $L \subset K_{n+1}$. Comme $A_n \lhd S_n$ et $A_{n+1} \lhd S_{n+1}$, alors la théorie de Galois nous indique que ces extensions sont galoisiennes finies, et que leurs groupes de Galois sont respectivement isomorphes à $S_n/A_n$ et $S_{n+1}/A_{n+1}$. Or le degré d'une extension galoisienne finie est égale au cardinal de

son groupe de Galois. Par conséquent : $[L : K_n(X)] = [L : K_{n+1}] = 2$. Posons maintenant :

$$\sqrt{\Delta(Q)} = \prod_{1 \leqslant i < j \leqslant n} (X_i - X_j)$$

$$\sqrt{\Delta(\widetilde{P})} = \prod_{1 \leqslant i < j \leqslant n+1} (Y_i - Y_j)$$

Cette notation est pertinente car $\sqrt{\Delta(Q)}^2 = \Delta(Q)$ et $\sqrt{\Delta(\widetilde{P})}^2 = \Delta(\widetilde{P})$. On a $\sqrt{\Delta(Q)} \in K_n(X) \setminus L$ et $\sqrt{\Delta(\widetilde{P})} \in K_{n+1} \setminus L$, et comme les extensions sont de degré 2 on obtient : $\begin{cases} K_{n+1} = L(\sqrt{\Delta(\widetilde{P})}) \\ K_n(X) = L(\sqrt{\Delta(Q)}) \end{cases}$. Or d'après la proposition 1.6 il existe $S \in K_n(X)$ tel que $\Delta(\widetilde{P}) = S^2.\Delta(Q)$. De là $\sqrt{\Delta(\widetilde{P})} = \pm S.\sqrt{\Delta(Q)}$. Ainsi $K_{n+1} \subset K_n(X)$, et en considérant les degrés on obtient finalement :

$$K_{n+1} = K_n(X).$$

Afin de conclure il reste à montrer que la famille $(Y_1, \ldots, Y_{n+1})$ est algébriquement libre sur $k$. Notons $\mathrm{degtr_k}(l)$ le degré de transcendance d'une extension $k \subset l$, c'est-à-dire le nombre maximum d'éléments de $l$ algébriquement indépendants sur $k$. Les extensions $K_n(X) \subset k(X_1, \ldots, X_n)(X)$ et $K_{n+1} \subset k(Y_1, \ldots, Y_{n+1})$ sont algébriques (car finies). Or les extensions algébriques conservent le degré de transcendance et ainsi l'on a :

$$\begin{aligned} \mathrm{degtr_k}(k(Y_1, \ldots, Y_{n+1})) &= \mathrm{degtr_k}(K_{n+1}) \\ &= \mathrm{degtr_k}(K_n(X)) \\ &= \mathrm{degtr_k}(k(X_1, \ldots, X_n)(X)) \\ &= n + 1. \end{aligned}$$

Par conséquent la famille $(Y_1, \ldots, Y_{n+1})$ est algébriquement libre sur $k$, ce qui termine la preuve du théorème.

□

## 2. Application

Le but de cette section est de montrer à l'aide du théorème principal (1.7) que si $k$ est un corps de caractéristique différente de 2, alors l'extension $k(X_1, \ldots, X_5)^{A_5}/k$ est rationnelle. Le lemme 2.1 et les deux propositions (2.2) et (2.3) que l'on utilise pour cela sont essentiellement repris de [Haj].

Lemme 2.1. *Soit $k$ un corps, $n \in \mathbb{N}$ et $k(X_1, \ldots, X_n)$ une extension rationnelle de $k$ de degré de transcendance $n$. Soient $Y_1, \ldots, Y_n$ définies par :*

$$Y_i = \prod_{j=1}^{n} X_j^{n_{ji}} \ , n_{ji} \in \mathbb{Z}$$

*Soit $\mathcal{N}$ la matrice des $n_{ji}$. Si $\det(\mathcal{N}) = d \neq 0$, alors :*

$$[k(X_1, \ldots, X_n) : k(Y_1, \ldots, Y_n)] = |d|.$$

**Démonstration.** Par le théorème de la base adaptée, il existe des matrices $\mathcal{P}, \mathcal{S} \in \mathrm{GL}_n(\mathbb{Z})$ telles que $\mathcal{PNS}$ soit une matrice diagonale. Ainsi par un changement de variable approprié on peut supposer que $\mathcal{N}$ est diagonale, et dans ce cas le résultat est immédiat. □

PROPOSITION 2.2. *L'extension $k(X_1, X_2, X_3)^{A_3}/k$ est rationnelle.*

**Démonstration.** Soit $K := k(X_1, X_2, X_3)$.

Supposons dans un premier temps que $\mathrm{car}(k) \neq 3$. Soit $\widetilde{k}$ le corps de décomposition du polynôme $T^3 - 1 \in k[T]$ et $\omega \in \widetilde{k}$ tel que $T^3 - 1 = (T-1)(T-\omega)(T-\omega^2)$. Soit $\widetilde{K} := K(\omega)$. L'action de $A_3$ sur $K$ peut être étendue sur $\widetilde{K}$ en fixant $\omega$. Nous savons que $A_3$ est engendré par $\sigma := (1,2,3)$. Pour $1 \leqslant j \leqslant 3$ posons $x_j := X_1 + \omega^j X_2 + \omega^{2j} X_3$. Le lecteur vérifiera aisément que $\widetilde{K} = \widetilde{k}(x_1, x_2, x_3)$ (on utilise le fait que $\mathrm{car}(k) \neq 3$) et que $\sigma(x_j) = \omega^{-j} x_j$. Soient :

$$\begin{cases} Y_1 := \frac{{x_1}^2}{x_2} \\ Y_2 := \frac{{x_2}^2}{x_1} \\ Y_3 := x_3 \end{cases}$$

On remarque facilement que $Y_1, Y_2, Y_3$ sont dans $\widetilde{K}^{A_3} = \widetilde{K}^{\sigma}$. De plus,

$$\det \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 3 = |A_3|.$$

D'après le lemme 2.1 on a donc : $[\widetilde{K} : \widetilde{k}(Y_1, Y_2, Y_3)] = 3$. Or $\widetilde{k}(Y_1, Y_2, Y_3) \subset \widetilde{K}^{A_3}$, et la théorie de Galois (plus précisément le lemme d'Artin) nous indique que $[\widetilde{K} : \widetilde{K}^{A_3}] = 3$. Ainsi $\widetilde{K}(Y_1, Y_2, Y_3) = \widetilde{K}^{A_3}$. Si $\omega \in k$ alors $\widetilde{k} = k$ et le résultat est montré. Sinon, il suffit de remarquer que $Y_1$ et $Y_2$ sont conjuguées vis-à-vis de la substitution $\omega \leftrightarrow \omega^2$. Ainsi l'on peut écrire

$$Y_1 = \omega Z_1 + \omega^2 Z_2 + Z_3 \ , \ Y_2 = \omega^2 Z_1 + \omega Z_2 + Z_3$$

avec $Z_1, Z_2, Z_3 \in K$. On obtient alors $\widetilde{K}^{A_3} = \widetilde{k}(Z_1, Z_2, Y_3)$ avec $Z_1, Z_2, Y_3 \in K$. Puis comme $\widetilde{K} = K(\omega)$ et $\widetilde{k} = k(\omega)$ et que $A_3$ n'agit pas sur $\omega$, alors on conclut que $K^{A_3} = k(Z_1, Z_2, Y_3)$.

Supposons maintenant que $\mathrm{car}(k) = 3$. Soit $\rho := \sigma - \mathrm{id}$. Pour $0 \leqslant j \leqslant 2$ posons $x_j := \rho^j(X_1)$. Le lecteur vérifiera aisément que $K = k(x_0, x_1, x_2)$ et que

$$\sigma : \ x_0 \mapsto x_0 + x_1 \ , \ x_1 \mapsto x_1 + x_2 \ , \ x_2 \mapsto x_2 \ .$$

Soit $x := {x_1}^2 + x_0 x_2 - x_1 x_2$. Remarquons que $K = k(x, x_1, x_2)$ et que

$$\sigma : \ x \mapsto x \ , \ x_1 \mapsto x_1 + x_2 \ , \ x_2 \mapsto x_2 \ .$$

Par conséquent

$$K^{A_3} = K^{\sigma} = k(x, x_2, x_1(x_1 + x_2)(x_1 + 2x_2)),$$

d'où la rationalité.

□

PROPOSITION 2.3. *Si $\mathrm{car}(k) \neq 2$, alors l'extension $k(X_1, \ldots, X_4)^{A_4}/k$ est rationnelle.*

**Démonstration.** Soit $K := k(X_1, \ldots, X_4)$.
$A_4$ est généré par :

$$\begin{cases} \alpha := (1,2) \circ (3,4) \\ \beta := (1,3) \circ (2,4) \\ \sigma := (1,2,3) \end{cases}$$

Définissons :

$$\begin{cases} s := X_1 + X_2 + X_3 + X_4 \\ z_1 := X_1 + X_2 - X_3 - X_4 \\ z_2 := X_1 - X_2 + X_3 - X_4 \\ z_3 := X_1 - X_2 - X_3 + X_4 \end{cases}$$

On vérifie aisément que $K = k(s, z_1, z_2, z_3)$ (pour cela on utilise $\mathrm{car}(k) \neq 2$), que $s$ est laissé stable par $\alpha, \beta$ et $\sigma$, et que :

$$\begin{cases} \alpha : \ z_1 \mapsto z_1 \ , \ z_2 \mapsto -z_2 \ , \ z_3 \mapsto -z_3 \\ \beta : \ z_1 \mapsto -z_1 \ , \ z_2 \mapsto z_2 \ , \ z_3 \mapsto -z_3 \\ \sigma : \ z_1 \mapsto -z_3 \ , \ z_2 \mapsto z_1 \ , \ z_3 \mapsto -z_2 \end{cases}$$

Posons maintenant :

$$\begin{cases} Y_1 := \frac{z_1 z_3}{z_2} \\ Y_2 := \sigma(Y_1) = \frac{z_2 z_3}{z_1} \\ Y_3 := \sigma^2(Y_1) = \frac{z_1 z_2}{z_3} \end{cases}$$

Or,

$$\left| \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & -1 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \right| = 4 = |\langle \alpha, \beta \rangle|.$$

D'après le lemme 2.1 on a donc : $[K : k(s, Y_1, Y_2, Y_3)] = 4$.
Or $k(s, Y_1, Y_2, Y_3) \subset K^{\langle \alpha, \beta \rangle}$, et la théorie de Galois nous indique que $[K : K^{\langle \alpha, \beta \rangle}] = 4$. Ainsi $k(s, Y_1, Y_2, Y_3) = K^{\langle \alpha, \beta \rangle}$. En remarquant que

$$\sigma : \ s \mapsto s \ , \ Y_1 \mapsto Y_2 \mapsto Y_3 \mapsto Y_1$$

on a : $K^{A_4} = K^{\langle \alpha, \beta, \sigma \rangle} = [k(s)](Y_1, Y_2, Y_3)^{\sigma}$.
Or la proposition 2.2 nous indique que l'extension $[k(s)](Y_1, Y_2, Y_3)^{\sigma}/k(s)$ est rationnelle, donc il en est de même pour l'extension $K^{A_4}/k$.

□

Théorème 2.4. *Si* $\mathrm{car}(k) \neq 2$*, alors l'extension* $k(X_1, \ldots, X_5)^{A_5}/k$ *est rationnelle.*

**Démonstration.** D'après la proposition précédente (2.3), l'extension $k(X_1, \ldots, X_4)^{A_4}/k$ est rationnelle, et d'après le théorème principal (1.7) l'extension $k(X_1, \ldots, X_5)^{A_5}/k(X_1, \ldots, X_4)^{A_4}$ est rationnelle, d'où le résultat. □

## 3. Vers le problème de Nœther

Dans cette dernière partie nous allons revenir au problème de Nœther. Rappelons que l'on note : $k(A_n) := k(\{X_g\}_{g \in A_n})^G$ le corps des points fixes résultant de l'*action régulière* de $A_n$ sur $\{X_g\}_{g \in A_n}$, et non plus de l'action de permutation sur

$\{X_1, \ldots, X_n\}$ (on note $k(X_1, \ldots, X_n)^{A_n}$ le corps des points fixes sous cette action).

Nous avons vu que si $n \geqslant 2$ est un entier pair, alors l'extension $k(X_1, \ldots, X_{n+1})^{A_{n+1}}/k(X_1, \ldots, X_n)^{A_n}$ est rationnelle. Le but de cette partie est de montrer à partir de ce résultat que l'extension $k(A_{n+1})/k(A_n)$ est elle-aussi rationnelle. Pour cela on utilisera le *Lemme sans nom* (théorème 3.4) que l'on montrera à partir du *Lemme de Speiser* (Proposition 3.1). Nous ne donnerons pas ici la démonstration du *Lemme de Speiser* car elle est assez longue, mais elle figure entièrement dans [Haz] où l'on voit que ce lemme résulte d'un cas particulier de l'équivalence de Morita.

PROPOSITION 3.1. *(Lemme de Speiser) Soit $k \subset l$ une extension finie galoisienne de groupe de Galois $G$. Soit $X$ un $l$-espace vectoriel muni d'une action $l/k$-semi-linéaire de $G$. Alors on a un isomorphisme de $l$-espaces vectoriels (qui respecte l'action de $G$):*

$$l \bigotimes_k X^G \to X$$

$$\lambda \otimes x \mapsto \lambda x$$

DÉFINITION 3.2. *Soit $V$ un $k$-espace vectoriel de dimension finie dont la famille $(e_1, \ldots, e_n)$ est une base. On note alors $k(V) := k(x_1, \ldots, x_n)$ où $(x_1, \ldots, x_n)$ est une famille de taille $n$ algébriquement libre sur $k$ (cela définit $k(V)$ à isomorphisme de corps près). Si de plus $V$ est une représentation linéaire d'un groupe $G$ sur $k$, alors en identifiant $x_i$ avec $e_i$ (pour $1 \leqslant i \leqslant n$) on a une action de $G$ sur le corps $k(V)$.*

*Remarque* 3.3. On pourrait définir de manière plus rigoureuse $k(V)$ en utilisant l'algèbre symétrique, mais cela n'est pas nécessaire ici.

THÉORÈME 3.4. *(Lemme sans nom) Soit $G$ un groupe fini, et $V$ et $W$ deux représentations fidèles de $G$ sur le corps $k$, de dimensions respectives $n$ et $m$ (en tant que $k$-espaces vectoriels). Alors si $x_1, \ldots, x_m$ et $t_1, \ldots, t_n$ sont des indéterminées, on a un isomorphisme de $k$-algèbres :*

$$k(V)^G(x_1, \ldots, x_m) \cong k(W)^G(t_1, \ldots, t_n).$$

**Démonstration.** Posons :

$$L := k(V)$$

$$K := k(V)^G$$

Comme $G$ agit par automorphismes de corps sur $k(V)$, alors d'après le lemme d'Artin l'extension $K \subset L$ est galoisienne finie de groupe de Galois $G$.
$L \bigotimes_k W$ est un $L$-espace vectoriel muni d'une action $L/K$-semi-linéaire de $G$. Ainsi, en notant $N := (L \bigotimes_k W)^G$ ($N$ est alors un $K$-espace vectoriel) on a d'après le lemme de Speiser un isomorphisme de $L$ espaces vectoriels :

$$L \bigotimes_k W \sim L \bigotimes_K N.$$

Nous savons par ailleurs que : $k(V \bigoplus W) \sim k(V)(W \bigotimes_k k(V))$.

Or,

$$\begin{aligned} k(V)(W \bigotimes_k k(V)) &= L(W \bigotimes_k L) \\ &\sim L(N \bigotimes_K L) \\ &= L(N \bigotimes_k L) \\ &\sim k(V \bigoplus N) \\ &= k(V)(N) \end{aligned}$$

Ainsi l'on a : $k(V \bigoplus W) \sim k(V)(x_1, \ldots, x_m)$ pour une certaine famille $(x_1, \ldots, x_m)$ algébriquement libre sur $k(V)$, et sur laquelle $G$ agit trivialement. On en déduit donc que :

$$k(V \bigoplus W)^G \sim k(V)^G(x_1, \ldots, x_m).$$

En reprenant alors le même raisonnement mais en interchangeant le rôle de $V$ et $W$ on obtient :

$$k(V \bigoplus W)^G \sim k(W)^G(t_1, \ldots, t_n).$$

où $t_1, \ldots, t_n$ sont des indéterminées. On a finalement le résultat voulu.

□

Corollaire 3.5. *Si $n \geqslant 2$ est un entier pair et que la caractéristique de $k$ ne divise pas $n!$ , alors l'extension $k(A_{n+1})/k(A_n)$ est rationnelle.*

**Démonstration.** La représentation régulière $V$ de $S_n$ contient la représentation naturelle $k^n$ comme facteur direct, et puisque la caractéristique de $k$ ne divise pas $n!$ (ce qui entraîne la complète réductibilité de la représentation), on peut écrire $V = k^n \bigoplus W$ avec $W$ sous-espace stable par $S_n$ donc aussi par $A_n$. La démonstration du *Lemme sans nom* (3.4) entraîne alors que $k(A_n)$ est transcendant pur sur $k(X_1, \ldots, X_n)^{A_n}$, et d'après le théorème principal (1.7) on obtient le résultat. □

Corollaire 3.6. *Si la caractéristique de $k$ est différente de 2 et 3 alors l'extension $k(A_5)/k$ est rationnelle, c'est-à-dire que le problème de Nœther admet une réponse positive pour $A_5$ sur $k$.*

**Démonstration.** C'est une conséquence du théorème 2.4 et du *Lemme sans nom* (3.4). □

Remerciements. Je tiens à remercier vivement Mathieu Florence mon maître de stage pour le temps qu'il m'a consacré, et grâce à qui j'ai pu apprendre beaucoup de choses.

## Bibliographie

[Mes] J-F. Mestre..— *Extensions régulières de $Q(T)$ de groupe de Galois $\widetilde{A}_n$*, Journal of Algebra 131 (1991) 483-495.

[Plans] B. Plans..— *On Nœther's problem for central extensions of symetric and alternating groups*, Journal of Algebra 321 (2009), 3704-3713.

[Haj] M. Hajja..— *The alternating functions of three and of four variables*, Algebras, Groups and Geometries 6 (1989), 49-54.

[Haz] M. Haziza.— *Équivalence de Morita et Descente Galoisienne*, Sujet de TER proposé par Mathieu Florence (2013).

Sylvain Gaulhiac, Etudiant en mathmatiques à l'Ecole Normale Supérieure de Cachan Antenne de Bretagne.