Polynômes symétriques et fractions rationnelles : correction

Exercice 1. La preuve du théorème donnée en cours est effective et fournit donc un algorithme pour écrire un polynôme symétrique comme polynôme en les polynômes symétriques élémentaires.
On prendra bien garde à ne pas confondre l'exposant n dans la notation

$$\Sigma_i^n = \sum_{1 \leq j_1 < \cdots < j_i \leq n} \mathrm{X}_{j_1} \cdots \mathrm{X}_{j_n}$$

avec une élévation à la puissance...

1. $\mathrm{P}(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) = \mathrm{X}^3\mathrm{Y} + \mathrm{X}\mathrm{Y}^3 + \mathrm{X}\mathrm{Z}^3 + \mathrm{X}^3\mathrm{Z} + \mathrm{Y}^3\mathrm{Z} + \mathrm{Y}\mathrm{Z}^3$. $\mathrm{P}(\mathrm{X}, \mathrm{Y}, 0) = \mathrm{X}^3\mathrm{Y} + \mathrm{X}\mathrm{Y}^3 = \mathrm{X}\mathrm{Y}(\mathrm{X}^2 + \mathrm{Y}^2) = \Sigma_2^2((\Sigma_1^2)^2 - 2\Sigma_2^2)$.
   Regardons alors $\mathrm{P}(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) - \Sigma_2^3((\Sigma_1^3)^2 - 2\Sigma_2^3) = -\mathrm{X}\mathrm{Y}\mathrm{Z}^2 - \mathrm{X}\mathrm{Y}^2\mathrm{Z} - \mathrm{X}^2\mathrm{Y}\mathrm{Z} = -\Sigma_3^3\Sigma_1^3$.
   On en déduit que $\mathrm{P} = \Sigma_2^3((\Sigma_1^3)^2 - 2\Sigma_2^3) - \Sigma_3^3\Sigma_1^3$.
2. $\mathrm{P} = \Sigma_3^3\Sigma_2^3 - (\Sigma_2^3)^2$.

Exercice 2.

1. Le fait que ii) implique i) ne pose pas de problème : il suffit de prendre la transposition (ij) pour σ. Dans l'autre sens, il suffit d'écrire σ comme un produit de transpositions et de se rappeler que $\epsilon(\sigma)$ est la parité du nombre de transpositions nécéssaires (indépendamment du choix d'une telle écriture).
2. Remarquons que dans la question précédente, il s'agit en fait de le vérifier pour des transpositions de la forme $(i, i+1)$. En écrivant $\sigma \in \mathfrak{S}_n$ comme produit de transpositions de la forme $(i, i+1)$, on vérifie que Δ est antisymétrique.
3. Soit P un polynôme antisymétrique dans $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Il s'agit de démontrer que $\mathrm{X}_i - \mathrm{X}_j$ divise P, ces polynômes étant irréductibles et premiers entre eux, leur produit Δ divisera alors P. Montrons-le pour $\mathrm{X}_1 - \mathrm{X}_2$, la preuve étant la même pour $\mathrm{X}_i - \mathrm{X}_j$.
   Si P est antisymétrique, alors chacune de ses composantes homogène l'est également, donc on peut supposer P antisymétrique homogène de degré d. On peut décomposer P de manière unique sous la forme

   $$\mathrm{P} = \sum_{k+l=d} \mathrm{P}_{k,l}\mathrm{X}_1^k\mathrm{X}_2^l \qquad (\mathrm{P}_{k,l} \in \mathrm{K}[\mathrm{X}_3, \ldots, \mathrm{X}_n]).$$

   On a $\mathrm{P}^{(1,2)} = -\mathrm{P}$, et donc $\mathrm{P}_{k,k} = 0$ et $\mathrm{P}_{k,l} = -\mathrm{P}_{l,k}$ pour $l \leq k$. On a donc

   $$\mathrm{P} = \sum_{\substack{k+l=d \\ k \neq l}} \mathrm{P}_{k,l}\mathrm{X}_1^l\mathrm{X}_2^k = \sum_{\substack{k+l=d \\ k > l}} \mathrm{X}_1^k\mathrm{X}_2^l(\mathrm{X}_1^{k-l} - \mathrm{X}_2^{k-l}),$$

   qui est donc divisible par $\mathrm{X}_1 - \mathrm{X}_2$. On peut donc écrire $\mathrm{P} = \mathrm{D}\overline{\mathrm{P}}$, et l'on a bien que $\overline{\mathrm{P}} \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est symétrique.
   Remarque. On a utilisé dans cette question l'hypothèse sur la caractéristique de K. Saurez-vous trouver où ?

Exercice 3.

1. Soit P un tel polynôme, et $\mathrm{Q} = \mathrm{P}^{(1,2)}$. Alors, si $\sigma \in \mathfrak{S}_n$, $\sigma = (1,2)\sigma'$, avec $\sigma' \in \mathfrak{A}_n$, et donc $\mathrm{P}^{\sigma} = (\mathrm{P}^{\sigma'})^{(1,2)} = \mathrm{P}^{(1,2)} = \mathrm{Q}$.
2. On vérifie que $\mathrm{P}+\mathrm{Q}$ est symétrique et $\mathrm{P}-\mathrm{Q}$ est antisymétrique. Par conséquent (souvenons-nous que K n'est pas de caractéristique 2), $\mathrm{P} = \frac{1}{2}((\mathrm{P}+\mathrm{Q}) + (\mathrm{P}-\mathrm{Q}))$, et comme $\mathrm{P}-\mathrm{Q}$ est divisible par Δ (avec un quotient symétrique), on a bien l'écriture recherchée. Inversement, si $\mathrm{P} = \mathrm{A} + \Delta\mathrm{B}$ avec A, B symétriques, on a $\mathrm{Q} = \mathrm{A} - \Delta\mathrm{B}$ et donc $\mathrm{A} = \frac{1}{2}(\mathrm{P}+\mathrm{Q})$ et $\mathrm{B} = \frac{1}{2}(\mathrm{P}-\mathrm{Q})$.
3. Soit φ le morphisme de K-algèbres de $\mathrm{K}[\mathrm{X}_1,\ldots,\mathrm{X}_n,\mathrm{T}]$ vers $\mathrm{K}[\mathrm{X}_1,\ldots,\mathrm{X}_n]$ qui envoie X_i sur Σ_i et T sur Δ. Il est évident que son image est formée de polynômes invariants sous $\mathfrak{A}_n$. Son image est même formée de tous les polynômes invariants sous $\mathfrak{A}_n$. En effet, celle-ci contient les polynômes symétriques élémentaires, donc tous les polynômes symétriques, ainsi que leur produit avec Δ, les polynômes antisymétriques. D'après la question précédente, elle contient tous les polynômes invariants sous $\mathfrak{A}_n$. L'ensemble des polynômes invariants sous $\mathfrak{A}_n$ est donc isomorphe à
$$\mathrm{K}[\mathrm{X}_1,\ldots,\mathrm{X}_n,\mathrm{T}]/\mathrm{Ker}\varphi.$$

Exercice 4.

1. Tout cela est évident.
2. Les morphismes φ et φ_f sont deux morphismes de corps de $\mathrm{K}(\mathrm{X})$ dans lui-même. Ils coïncident sur K (où ils valent l'identité) et sur X (qu'ils envoient tous deux sur f) : ils coïncident donc sur tout $\mathrm{K}(\mathrm{X})$, qui est le corps engendré par K et X.
3. Notons $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\mathrm{B} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Alors $\mathrm{AB} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$. Il suffit donc de vérifier que $\dfrac{af_{\mathrm{B}}(\mathrm{X})+b}{cf_{\mathrm{B}}(\mathrm{X})+d} = \dfrac{(aa'+bc')\mathrm{X}+(ab'+bd')}{(ca'+dc')f_{\mathrm{B}}(\mathrm{X})+(cb'+dd')}$.
4. Soit $v : \mathrm{K}(\mathrm{X}) \to \mathrm{Aut}_{\mathrm{K}}(\mathrm{K}(\mathrm{X})), f \mapsto \varphi_f$. C'est un anti-morphisme bien défini. De même, $w : \mathrm{GL}_2(\mathrm{K}) \to \mathrm{K}(\mathrm{X}), \mathrm{A} \mapsto f_{\mathrm{A}}$ est un morphisme (d'après la question précédente). Par conséquent, $u = v \circ w$ est un anti-morphisme bien défini.
5. Si $v(f) = \varphi_f = \mathrm{Id}_{\mathrm{K}(\mathrm{X})}$, il est clair que $f = \mathrm{X}$, car $\varphi_f(\mathrm{X}) = f(\mathrm{X})$. Le noyau de u est donc le noyau de w. Si $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans le noyau de w, on a $\frac{a\mathrm{X}+b}{c\mathrm{X}+d} = \mathrm{X}$, donc $a\mathrm{X}+b = c\mathrm{X}^2 + d\mathrm{X}$, d'où $b = c = 0$ et $a = d$, donc A est scalaire. Inversement, les matrices scalaires sont clairement dans le noyau de w. On a donc prouvé que le noyau de u était l'ensemble des matrices scalaires.
6. Calcul....
7. Soit $g/h \in \mathrm{L}(\mathrm{X})$ premiers entre eux tel que la fonction associée sur $\mathbf{P}^1(\mathrm{L})$ soit injective. Si h est constant, g/h est un polynôme dont la fonction polynomiale associée est injective. Si g est constant, h/g est un tel polynôme. Or, en caractéristique nulle et sur un corps algébriquement clos, seuls les polynômes de degré 1 vérifient cette propriété : en effet, si $\mathrm{P} \in \mathrm{L}[\mathrm{X}]$ définit une fonction injective, P n'a qu'une racine, donc il s'écrit $\mathrm{P} = \lambda(\mathrm{X}-\alpha)^n$. Si n était > 1, P' ne s'annulerait qu'en α, donc $\mathrm{P}-1$ et $\mathrm{P}' = (\mathrm{P}-1)'$ seraient premiers entre eux. $\mathrm{P}-1$ aurait donc n racines simples, ce qui contredit l'injectivité de P.

   On peut donc maintenant supposer que g et h ne sont pas constants. En particulier, ils ont tous deux une racine dans L, donc la fonction $(g/h)_{|\mathrm{L}}$ prend déjà les valeurs 0 et ∞. On a donc $(g/h)(\infty) \in \mathrm{L}^{\times}$, et g et h sont donc du même degré n.

Puisque 0 n'a qu'un antécédent, g n'a qu'une racine α, et donc $g = \lambda(\mathrm{X}-\alpha)^n$ avec $\lambda \neq 0$. De même, ∞ n'a qu'un antécédent (et ce n'est pas le même !) donc $h = \mu(\mathrm{X}-\beta)^n$, avec $\alpha \neq \beta$ et $\mu \neq 0$. Enfin, puisque $\frac{\lambda}{\mu} = \frac{g}{h}(\infty)$ n'a pas d'antécédent dans K, le polynôme $\lambda(\mathrm{X}-\alpha)^n - \mu(\mathrm{X}-\beta)^n$ n'a pas de racine dans K. Il est donc constant. En identifiant les termes dominants, on obtient $\lambda = \mu$. On a donc

$$\text{Constante} = n\lambda(\beta-\alpha)\mathrm{X}^{n-1} + \text{termes de degré} < n-1.$$

Si $n > 1$, l'identification des termes de degré $n-1$ donne donc $n\lambda(\beta-\alpha) = 0$, ce qui est exclu en caractéristique nulle. En conclusion, f et g sont de degré au plus un, et donc f/g est une homographie.

Remarquons que le résultat de cette question est faux en caractéristique $p > 0$, la fonction $\mathrm{X} \mapsto \mathrm{X}^p$ étant un contre-exemple. Le résultat principal de l'exercice, lui, reste vrai, mais la démonstration n'est plus la même.

8. Soit $\varphi_f \in \mathrm{Aut}_{\mathrm{K}}(\mathrm{K}(\mathrm{X}))$. Puisque φ_f est un automorphisme, il admet un automorphisme réciproque, qui d'après la question 2 est de la forme φ_g. Il existe donc $g \in \mathrm{K}(\mathrm{X})$ tel que $g \circ f = f \circ g = \mathrm{X}$. Les fractions rationnelles f et g définissent donc des fonctions réciproques, non seulement sur $\mathbf{P}^1(\mathrm{K})$ mais aussi sur $\mathbf{P}^1(\overline{\mathrm{K}})$. On peut alors appliquer la question précédente à $\mathrm{L} = \overline{\mathrm{K}}$: f est donc quotient de deux polynômes de degré un, premiers entre eux dans $\overline{\mathrm{K}}[\mathrm{X}]$, donc aussi dans $\mathrm{K}[\mathrm{X}]$ et f est de la forme $\frac{a\mathrm{X}+b}{c\mathrm{X}+d}$, et donc dans l'image de u. Comme le noyau de u est formé des homothéties, u est donc un anti-isomorphisme de $\mathrm{PGL}_2(\mathrm{K})$ dans $\mathrm{Aut}_{\mathrm{K}}(\mathrm{K}(\mathrm{X}))$. Comme tout groupe est anti-isomorphe à lui-même, on a bien l'isomorphisme demandé.

Exercice 5.

1. L'égalité $\mathrm{A}+\mathrm{B} = \mathrm{C}$ implique $\frac{\mathrm{C}}{\mathrm{C}'} = \frac{\mathrm{A}+\mathrm{B}}{\mathrm{A}'+\mathrm{B}'}$, que l'on peut aussi écrire

$$\mathrm{A}\left(\frac{\mathrm{A}'}{\mathrm{A}} - \frac{\mathrm{C}'}{\mathrm{C}}\right) = \mathrm{B}\left(\frac{\mathrm{C}'}{\mathrm{C}} - \frac{\mathrm{A}'}{\mathrm{A}}\right).$$

Rappelons que deux polynômes de $\mathbf{C}[\mathrm{X}]$ sont premiers entre eux si et seulement s'ils ont une racine commune. Les polynômes A, B et C sont donc non seulement premiers dans leur ensemble, mais aussi premiers entre eux deux à deux :si deux d'entre eux avaient une racine commune, cette racine serait aussi une racine du troisième, puisque $\mathrm{A}+\mathrm{B} = \mathrm{C}$.

Notons

$$\mathrm{A} = \alpha\prod_{i=1}^{n_{\mathrm{A}}}(\mathrm{X}-a_i)^{\alpha_i}, \mathrm{B} = \beta\prod_{i=1}^{n_{\mathrm{B}}}(\mathrm{X}-b_i)^{\beta_i}, \mathrm{C} = \gamma\prod_{i=1}^{n_{\mathrm{C}}}(\mathrm{X}-c_i)^{\gamma_i}$$

En décomposant en éléments simples, on obtient

$$\frac{\mathrm{A}'}{\mathrm{A}} = \sum_{i=1}^{n_{\mathrm{A}}}\frac{\alpha_i}{\mathrm{X}-a_i}, \frac{\mathrm{B}'}{\mathrm{B}} = \sum_{i=1}^{n_{\mathrm{B}}}\frac{\beta_i}{\mathrm{X}-b_i}, \frac{\mathrm{C}'}{\mathrm{C}} = \sum_{i=1}^{n_{\mathrm{C}}}\frac{\gamma_i}{\mathrm{X}-c_i}.$$

Un dénominateur commun à ces trois fractions rationnelles est le polynôme

$$\mathrm{U} = \prod_{i=1}^{n_{\mathrm{A}}}(\mathrm{X}-a_i)\prod_{i=1}^{n_{\mathrm{B}}}(\mathrm{X}-b_i)\prod_{i=1}^{n_{\mathrm{C}}}(x-c_i),$$

et donc il existe deux polynômes P et Q de $\mathbf{C}[\mathrm{X}]$ tels que

$$\frac{\mathrm{A}'}{\mathrm{A}} - \frac{\mathrm{C}'}{\mathrm{C}} = \frac{\mathrm{P}}{\mathrm{U}} \text{ et } \frac{\mathrm{C}'}{\mathrm{C}} - \frac{\mathrm{B}'}{\mathrm{B}} = \frac{\mathrm{Q}}{\mathrm{U}}.$$

De plus, comme $m = n_\mathrm{A} + n_\mathrm{B} + n_\mathrm{C}$, $\deg \mathrm{U} = m$. Comme les trois fractions rationnelles A'/A, B'/B et C'/C sont de degré -1, $\deg \mathrm{P}$ et $\deg \mathrm{Q}$ sont majorés par $m-1$.

Comme $\mathrm{AP} = \mathrm{BQ}$ et que A et B sont premiers entre eux, B divise P et A divise Q, donc $\deg \mathrm{A}$ et $\deg \mathrm{B}$ sont majorés par $m-1$. Comme $\mathrm{C} = \mathrm{A} + \mathrm{B}$, on a aussi $\deg \mathrm{C} \leq m-1$, d'où l'inégalité recherchée.

2. Soit P, Q, R trois polynômes non tous constants tels que $\mathrm{P}^n + \mathrm{Q}^n = \mathrm{R}^n$. Soit $\mathrm{D} = \mathrm{pgcd}(\mathrm{P}, \mathrm{Q}, \mathrm{R})$ et $\overline{\mathrm{P}}$, $\overline{\mathrm{Q}}$, $\overline{\mathrm{R}}$ tels que $\mathrm{P} = \overline{\mathrm{P}}\mathrm{D}$, $\mathrm{Q} = \overline{\mathrm{Q}}\mathrm{D}$ et $\mathrm{R} = \overline{\mathrm{R}}\mathrm{D}$. Ces trois derniers sont premiers entre eux dans leur ensemble et vérifient $\overline{\mathrm{P}}^n + \overline{\mathrm{Q}}^n = \overline{\mathrm{R}}^n$. Supposons qu'ils ne soient pas tous constants. On aurait alors d'après la question précédente $n \max(\deg \overline{\mathrm{P}}, \deg \overline{\mathrm{Q}}, \deg \overline{\mathrm{R}}) < \deg(\overline{\mathrm{PQR}})$, et donc $n \max(\deg \overline{\mathrm{P}}, \deg \overline{\mathrm{Q}}, \deg \overline{\mathrm{R}}) < 3 \max(\deg \mathrm{P}, \deg \mathrm{Q}, \deg \mathrm{R})$, ce qui est impossible si $n \geq 3$. Les trois polynômes $\overline{\mathrm{P}}$, $\overline{\mathrm{Q}}$ et $\overline{\mathrm{R}}$ sont donc constants, ce qui entraîne que P, Q et R sont tous égaux au produit de D et d'un scalaire dans $\mathbf{C}[\mathrm{X}]^\times = \mathbf{C}^*$.

3. Soit $\mathrm{A} = \mathbf{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{X}^n + \mathrm{Y}^n - 1)$ et K son corps des fractions. On note $\overline{\mathrm{X}}$ et $\overline{\mathrm{Y}}$ les images de X et Y dans $\mathrm{A} \subset \mathrm{K}$. Supposons par l'absurde qu'il existe un isomorphisme $\varphi : \mathrm{K} \to \mathbf{C}(\mathrm{T})$ et posons $\mathrm{R}_1 = \varphi(\overline{\mathrm{X}})$ et $\mathrm{R}_2 = \varphi(\overline{\mathrm{Y}})$. Puisque $\overline{\mathrm{X}}^n + \overline{\mathrm{Y}}^n = 1$, on doit avoir $\mathrm{R}_1^n + \mathrm{R}_2^n = 1$. En réduisant au même dénominateur $\mathrm{R}_1 = \mathrm{P}_1/\mathrm{Q}$ et $\mathrm{R}_2 = \mathrm{P}_2/\mathrm{Q}$, on a donc $\mathrm{P}_1^n + \mathrm{P}_2^n = \mathrm{Q}^n$. D'après la question précédente, on a donc un polynôme $\mathrm{T} \in \mathbf{C}[\mathrm{X}]$ tel que P_1, P_2 et R soient des multiples de T. Il s'ensuit que R_1 et R_2 sont des constantes. Comme $\overline{\mathrm{X}}$ et $\overline{\mathrm{Y}}$ engendrent l'anneau A (et donc le corps K), on a donc $\varphi(\mathrm{K}) \subset \mathbf{C}$, ce qui est une contradiction.

Exercice 6.

1. Dans le cas $n = d = 3$, les polynômes r_i sont :
   - $r_2 = \mathrm{X}_1^2\mathrm{X}_2 + \mathrm{X}_1\mathrm{X}_2^2 + \mathrm{X}_1^2\mathrm{X}_3 + \mathrm{X}_1\mathrm{X}_3^2 + \mathrm{X}_2^2\mathrm{X}_3 + \mathrm{X}_2\mathrm{X}_3^2$;
   - $r_3 = \mathrm{X}_1^3 + \mathrm{X}_2^3 + \mathrm{X}_3^3$.
2. On a $p_d = \sum_j \mathrm{X}_j^d = r_d$.
3. On a pour $k \geq 2$:

$$\begin{aligned}
p_k \Sigma_{d-k} &= \left(\sum_{j_0} \mathrm{X}_{j_0}^k\right) \cdot \left(\sum_{j_1 < \cdots < j_{d-k}} \mathrm{X}_{j_1} \cdots \mathrm{X}_{j_{d-k}}\right) \\
&= \sum_{\substack{j_1 < \ldots < j_{d-k} \\ j_0 \notin \{j_1, \ldots, j_{d-k}\}}} \mathrm{X}_{j_0}^k \cdot \mathrm{X}_{j_1} \cdots \mathrm{X}_{j_{d-k}} + \sum_{\substack{j_1 < \ldots < j_{d-k} \\ j_0 \in \{j_1, \ldots, j_{d-k}\}}} \mathrm{X}_{j_0}^k \cdot \mathrm{X}_{j_1} \cdots \mathrm{X}_{j_{d-k}} \\
&= \sum_{\substack{j_1 < \ldots < j_{d-k} \\ j_0 \notin \{j_1, \ldots, j_{d-k}\}}} \mathrm{X}_{j_0}^k \cdot \mathrm{X}_{j_1} \cdots \mathrm{X}_{j_{d-k}} + \sum_{\substack{j_1 < \ldots < j_{d-k-1} \\ j_0 \notin \{j_1, \ldots, j_{d-k-1}\}}} \mathrm{X}_{j_0}^{k+1} \cdot \mathrm{X}_{j_1} \cdots \mathrm{X}_{j_{d-k-1}} \\
&= r_k + r_{k+1}.
\end{aligned}$$

4. On a :

$$\begin{aligned}
p_1\Sigma_{d-1} &= \left(\sum_{j_0} X_{j_0}\right)\cdot\left(\sum_{j_1<\cdots<j_{d-1}} X_{j_1}\cdots X_{j_{d-1}}\right)\\
&= \sum_{\substack{j_1<\ldots<j_{d-1}\\ j_0\notin\{j_1,\ldots,j_{d-1}\}}} X_{j_0}\cdot X_{j_1}\cdots X_{j_{d-1}} + \sum_{\substack{j_1<\ldots<j_{d-1}\\ j_0\in\{j_1,\ldots,j_{d-1}\}}} X_{j_0}\cdot X_{j_1}\cdots X_{j_{d-k}}\\
&= d\sum_{j_1<\ldots<j_d} X_{j_1}\cdots X_{j_d} + \sum_{\substack{j_1<\ldots<j_{d-2}\\ j_0\notin\{j_1,\ldots,j_{d-2}\}}} X_{j_0}^2\cdot X_{j_1}\cdots X_{j_{d-k-1}}\\
&= d\Sigma_d + r_2.
\end{aligned}$$

L'avant-dernière égalité est justifiée car un monôme produit de d indéterminées toutes différentes se décompose d'exactement d façons comme produit d'une indéterminée et d'un autre monôme.

Remarque. Les calculs précédents sont bien plus agréables avec de meilleures notations. On pourra par exemple comparer avec Mead, *Newton's Identities*, American Mathematical Monthly **99** n°8 (1992), pp. 749-751.

5. Grâce aux deux questions précédentes,

$$\begin{aligned}
p_d + \sum_{i=1}^{d-1}(-1)^i\Sigma_i p_{d-i} + (-1)^d d\Sigma_d\\
&= p_d + \sum_{i=1}^{d-2}(-1)^i\Sigma_i p_{d-i} + (-1)^{d-1}p_1\Sigma_{d-1} + (-1)^d d\Sigma_d\\
&= r_d + \sum_{i=1}^{d-2}(-1)^i(r_{d-i}+r_{d-i+1}) + (-1)^{d-1}(d\Sigma_d + r_2) + (-1)^d d\Sigma_d\\
&= r_d + \sum_{i=1}^{d-2}(-1)^i(r_{d-i}+r_{d-i+1}) + (-1)^{d-1}r_2\\
&= 0.
\end{aligned}$$

6. La première formule de Newton montre que $\Sigma_1 = p_1$, la seconde que $\Sigma_2 = 1/2(\Sigma_1 p_1 - p_2) = 1/2(p_1^2 - p_2)$, et ainsi de suite. On montre par récurrence (et en divisant à chaque étape par d, d'où l'hypothèse sur la caractéristique de K !) que les polynômes élémentaires Σ_i peuvent s'écrire comme polynômes en p_i. Précisément, on a une relation de la forme

$$d\Sigma_d = \pm p_d + \text{polynôme}(\Sigma_1,\ldots,\Sigma_{d-1}).$$

Autrement dit, les Σ_i appartiennent à l'algèbre engendrée par les p_i. Puisqu'à leur tour les polynômes Σ_i engendrent la K-algèbre $K[X_1,\ldots,X_n]^{\mathfrak{S}_n}$, on obtient bien que cette dernière est engendrée par les p_i, c'est-à-dire que tout polynôme symétrique s'écrit comme un polynôme en p_i ($i \le n$)..

Pour montrer que cette expression est unique, il suffit maintenant de montrer que si $f \in k[X_1,\ldots,X_n]$ est un polynôme tel que $f(p_1,\ldots,p_n) = 0$, alors $f = 0$. Pour $1 \le k \le n$, posons $I_k = (\Sigma_1,\ldots,\Sigma_{k-1})$: c'est un idéal de $k[X_1,\ldots,X_n]^{\mathfrak{S}_n}$ et tout élément de $k[X_1,\ldots,X_n]^{\mathfrak{S}_n}/I_k$ s'écrit de façon unique comme un polynôme en $\overline{\Sigma}_k,\ldots,\overline{\Sigma}_n$. D'après la forme précise des identités de Newton, $p_k \equiv \pm\Sigma_k \pmod{I_k}$. En réduisant modulo I_n, on obtient $f(\overline{0},\ldots,\overline{0},\pm\overline{\Sigma_n}) = \overline{0}$. On en déduit donc (par unicité) que le polynôme

$f(0,\dots,0,\mathrm{T})$ est nul. On peut donc voir f comme un polynôme en $n-1$ variables tel que $f(p_1,\dots,p_{n-1}) = 0$. En réitérant l'argument, on montre qu'en fait $f = 0$.

7. Écrivons explicitement les quatre premières formules de Newton :

$$\begin{cases} p_1 - \Sigma_1 = 0 \\ p_2 - \Sigma_1 p_1 + 2\Sigma_2 = 0 \\ p_3 - \Sigma_1 p_2 + \Sigma_2 p_1 - 3\Sigma_3 = 0 \\ p_4 - \Sigma_1 p_3 + \Sigma_2 p_2 - \Sigma_3 p_1 + 4\Sigma_4 = 0 \end{cases} \Rightarrow \begin{cases} p_1 = \Sigma_1 \\ p_2 = \Sigma_1^2 - 2\Sigma_2 \\ p_3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3 \\ p_4 = \Sigma_1^4 - 4\Sigma_1^2\Sigma_2 + 4\Sigma_1\Sigma_3 + 2\Sigma_2^2 - 4\Sigma_4 \end{cases}$$

Si z_1, z_2, z_3 et z_4 sont les quatre racines de

$$(\mathrm{X}-1)(\mathrm{X}-2)(\mathrm{X}-3)(\mathrm{X}-4) = \mathrm{X}^4 - 10\mathrm{X}^3 + 35\mathrm{X}^2 - 50\mathrm{X} + 24,$$

les relations coefficients-racines entraînent, en notant $\Sigma_i = \Sigma_i(z_1, z_2, z_3, z_4)$:

$$\Sigma_1 = 10 \quad \Sigma_2 = 35 \quad \Sigma_3 = 50 \quad \Sigma_4 = 24.$$

On obtient donc

$$p_4(z_1, z_2, z_3, z_4) = 354.$$