Polynômes symétriques, résultant : correction (partielle)

Exercice 1.

1. Le fait que ii) implique i) ne pose pas de problème : il suffit de prendre la transposition $(i\,j)$ pour σ. Dans l'autre sens, il suffit d'écrire σ comme un produit de transpositions et de se rappeler que $\varepsilon(\sigma)$ 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.

   Il y a une autre solution : on peut voir Δ comme le déterminant d'une matrice de Vandermonde $M = (X_{n-i}^j)_{1\leq i,j\leq n}$, et le fait de permuter deux variables échange exactement deux colonnes de la matrice, qui change le signe du déterminant.
3. Soit P un polynôme antisymétrique dans $K[X_1,\dots,X_n]$. Il s'agit de démontrer que $X_i - X_j$ divise P, ces polynômes étant irréductibles et premiers entre eux, leur produit Δ divisera alors P. Montrons-le pour $X_1 - X_2$, la preuve étant la même pour $X_i - X_j$.

   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

   $$P = \sum_{k+l=d} P_{k,l} X_1^k X_2^l \qquad (P_{k,l} \in K[X_3,\dots,X_n]).$$

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

   $$P = \sum_{\substack{k+l=d \\ k\neq l}} P_{k,l} X_1^l X_2^k = \sum_{\substack{k+l=d \\ k>l}} X_1^k X_2^l (X_1^{k-l} - X_2^{k-l}),$$

   qui est donc divisible par $X_1 - X_2$. On peut donc écrire $P = D\overline{P}$, et l'on a bien que $\overline{P} \in K[X_1,\dots,X_n]$ est symétrique.

   Remarque. On a utilisé dans cette question l'hypothèse sur la caractéristique de K. Saurez-vous trouver où ?

Exercice 2.

1. Soit P un tel polynôme, et $Q = P^{(1,2)}$. Alors, si $\sigma \in \mathfrak{S}_n$, $\sigma = (1,2)\sigma'$, avec $\sigma' \in \mathfrak{A}_n$, et donc $P^{\sigma} = (P^{\sigma'})^{(1,2)} = P^{(1,2)} = Q$.
2. On vérifie que P+Q est symétrique et P−Q est antisymétrique. Par conséquent (souvenons-nous que K n'est pas de caractéristique 2), $P = \frac{1}{2}((P+Q)+(P-Q))$, et comme $P-Q$ est divisible par Δ (avec un quotient symétrique), on a bien l'écriture recherchée. Inversement, si $P = A + \Delta B$ avec A, B symétriques, on a $Q = A - \Delta B$ et donc $A = \frac{1}{2}(P+Q)$ et $B = \frac{1}{2}(P-Q)$.
3. Soit φ le morphisme de K-algèbres de $K[X_1,\dots,X_n,T]$ vers $K[X_1,\dots,X_n]$ 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

$$K[X_1,\dots,X_n,T]/\mathrm{Ker}\varphi.$$

Remarque. Que se passe-t-il si K est de caractéristique 2 ?

Exercice 3.
Pour $\alpha+\beta$, posons $R(X) = \mathrm{Rés}^t(P(t), Q(X-t)) \in K[X]$. Notons que les deux polynômes $P(t)$ et $Q(X-t)$ sont unitaires en t, donc par la question 1) de l'Exercice 4, pour $x \in \overline{K}$ $R(x) = 0$ si et seulement si $P(t)$ et $Q(X-t)$ ont une racine commune dans $\overline{K}$. Si $x = \alpha+\beta$, alors $t = \alpha$ est un zéro commun de $P(t)$ et $Q(\alpha+\beta-t)$, ce qui implique que $\alpha+\beta$ est bien une racine de R(X).
Pour $\alpha\beta$, on a un raisonnement similaire, avec $R(X) = \mathrm{Rés}^t(P(t), t^n Q(X/t)) \in K[X]$, où n est le degré de Q.
Le degré de R est le produit des degrés de P et Q dans les deux cas.

Exercice 4.

1. Notons év : $K[Y] \to K$ l'évaluation en y. Ce morphisme induit un morphisme $K[X,Y] \to K[X]$ (que nous continuerons à noter év) défini par $P(X,Y) \mapsto P(X,y)$. Notons p et q les degrés en X de P et Q, respectivement. On a donc $R = \mathrm{Rés}^X_{p,q}(P,Q)$. D'après le cours, $R(y) = \text{év}(\mathrm{Rés}^X_{p,q}(P,Q)) = \mathrm{Rés}_{p,q}(\text{év}(P), \text{év}(Q))$. Puisque P et Q sont unitaires, on a bien $\deg \text{év}(P) = \deg_X P$ et idem pour Q. Le résultant $\mathrm{Rés}_{p,q}(\text{év}(P), \text{év}(Q))$ est donc « de la bonne taille » et $\mathrm{Rés}_{p,q}(\text{év}(P), \text{év}(Q)) = 0$ si et seulement si év(P) et év(Q) ont une racine commune dans $\overline{K}$. On a donc bien montré que $R(y) = 0$ si et seulement si $P(X,y)$ et $Q(X,y)$ ont une racine commune dans $\overline{K}$.
2. Notons que le point important de la preuve précédente est que les polynômes conservent le même degré après évaluation en y : c'est effectivement vrai si le polynôme (vu comme polynôme en X) est unitaire, mais également si le coefficient dominant est un inversible de K. C'est le cas ici pour les deux exemples qui sont donnés, donc on peut appliquer la méthode de la question précédente.
   (a) On obtient comme résultant $3Y^4 - 3Y^2$, dont les racines sont −1, 0 et 1. Il reste alors à substituer à y ces trois valeurs pour chercher des racines communes aux deux polynômes : on trouve sans peine l'intersection $\{(1,0),(-1,0),(1,1),(0,-1)\}$.
   (b) On obtient comme résultant $Y^4 - 3Y^2$ dont les racines sont $-\sqrt{3}$, 0 et $-\sqrt{3}$. Après substitution et recherche des racines communes, on trouve pour intersection $\{(1-\sqrt{3},-\sqrt{3}),(0,0),(1-\sqrt{3},\sqrt{3})\}$.

3. Le calcul du résultant ne pose pas de problème, c'est Y.

   On observe ici une contradiction apparente avec la première question de l'exercice : $y = 0$ annule le résultant, sans pour autant qu'il existe de couple $(x, 0)$ qui soit zéro commun aux deux polynômes. Ceci est dû au fait que les polynômes $P(X, 0)$ et $Q(X, 0)$ sont de degrés en X strictement plus petits que P et Q, et donc que leur résultant (d'ordre $1, 1$) est forcément nul. (Et la contradiction n'est apparente, car la première question supposait les polynomes unitaires).

   De manière générale, la preuve de la première question montre que l'équivalence entre l'annulation du résultant en y et la présence d'un zéro commun d'ordonnée y reste vraie pour deux polynômes P et Q de degrés respectifs p et q, pourvu que l'on n'ait pas simultanément $\deg_X P(X, y) < p$ et $\deg_X Q(X, y) < q$.

   Si les deux degrés sont diminués, alors $R(y) = 0$ car on a une ligne complète de zéros sur la matrice de Sylvester, comme dans l'exemple précédent.

   Par contre, si un seul des degrés diminue, par exemple celui de P (et que $P(X, y)$ n'est pas constant, afin que $\text{Rés}_X(P(X, y), Q(X, y))$ ait un sens), alors le résultat reste vrai. En effet, en écrivant la matrice de Sylvester, on obtient un seul coefficient non nul sur la première ligne, et en développant par rapport à cette ligne, on voit que $\text{Rés}_{X,p,q}(P(X, y), Q(X, y))$ est proportionnel à $\text{Rés}_{X,p-1,q}(P(X, y), Q(X, y))$. Quitte à réitérer le processus si $\deg_X P(X, y) < p-1$, on voit que le résultant $p \times q$ est proportionnel au « bon » résultant $\text{Rés}_X(P(X, y), Q(X, y))$, qui est bien nul si et seulement si il existe x tel que $P(x, y) = Q(x, y) = 0$.

Exercice 5.

Expliquons ici la méthode générale à employer lorsqu'on considère des paramétrages rationnels (c'est-à-dire par des fractions rationnelles).

Si on a $x = A(t)/B(t)$ et $y = C(t)/D(t)$, alors $xB(t) - A(t) = 0$ et $D(t)y - C(t) = 0$. Si l'on considère $R(X, Y) = \text{Rés}_T(B(T)X - A(T), D(T)Y - C(T)) \in \mathbf{R}[X, Y]$, on a alors pour tout (x, y) de la courbe paramétrée l'existence d'un t tel que $xB(t) - A(t) = yD(t) - C(t) = 0$ et donc $R(x, y) = 0$.

Le polynôme R nous donne donc une équation vérifiée par tous les points de la courbe paramétrée considérée. Ici on obtenait comme équations :

1. $X^2Y^2 - 2X^2Y + X^2 + Y^2 + 4XY - 4X + 3 = 0$.
2. $X^4 + Y^4 + 2X^2Y^2 - X^2 + Y^2 = 0$.

Une étude plus soignée, notamment des cas d'abaissement du degré des polynômes comme dans l'exercice précédent, montrerait l'égalité entre la courbe paramétrée et la courbe implicite.

Exercice 6.

1. Dans le cas $n = d = 3$, les polynômes r_i sont :
   - $r_2 = X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2$;
   - $r_3 = X_1^3 + X_2^3 + X_3^3$.
2. On a $p_d = \sum_j X_j^d = r_d$.

3. On a pour $k \geq 2$:

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

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 $\mathrm{K}[\mathrm{X}_1,\dots,\mathrm{X}_n]^{\mathfrak{S}_n}$, 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 $(i \leq n)$..

Pour montrer que cette expression est unique, il suffit maintenant de montrer que si $f \in k[\mathrm{X}_1,\dots,\mathrm{X}_n]$ est un polynôme tel que $f(p_1,\dots,p_n)=0$, alors $f=0$. Pour $1 \leq k \leq n$, posons $\mathrm{I}_k = (\Sigma_1,\dots,\Sigma_{k-1})$: c'est un idéal de $k[\mathrm{X}_1,\dots,\mathrm{X}_n]^{\mathfrak{S}_n}$ et tout élément de $k[\mathrm{X}_1,\dots,\mathrm{X}_n]^{\mathfrak{S}_n}/\mathrm{I}_k$ s'écrit de façon unique comme un polynôme en $\overline{\Sigma}_k,\dots,\overline{\Sigma}_n$. D'après la forme précise des identités de Newton, $p_k \equiv \pm\Sigma_k \pmod{\mathrm{I}_k}$. En réduisant modulo I_n, on obtient $f(\overline{0},\dots,\overline{0},\pm\overline{\Sigma_n}) = \overline{0}$. 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

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

Exercice 7.
cf. X.Gourdon, *Les maths en tête : Algèbre*