Résultant et critères d'irréductibilité : correction

Exercice 1.

1. Notons év : $\mathrm{K}[\mathrm{Y}] \to \mathrm{K}$ l'évaluation en y. Ce morphisme induit un morphisme $\mathrm{K}[\mathrm{X},\mathrm{Y}] \to \mathrm{K}[\mathrm{X}]$ (que nous continuerons à noter év) défini par $\mathrm{P}(\mathrm{X},\mathrm{Y}) \mapsto \mathrm{P}(\mathrm{X},y)$. Notons p et q les degrés en X de P et Q, respectivement. On a donc $\mathrm{R} = \mathrm{Rés}^{\mathrm{X}}_{p,q}(\mathrm{P},\mathrm{Q})$. D'après le cours, $\mathrm{R}(y) = \text{év}(\mathrm{Rés}^{\mathrm{X}}_{p,q}(\mathrm{P},\mathrm{Q})) = \mathrm{Rés}_{p,q}(\text{év}(\mathrm{P}),\text{év}(\mathrm{Q}))$. Puisque P et Q sont unitaires, on a bien $\deg \text{év}(\mathrm{P}) = \deg_{\mathrm{X}} \mathrm{P}$ et idem pour Q. Le résultant $\mathrm{Rés}_{p,q}(\text{év}(\mathrm{P}),\text{év}(\mathrm{Q}))$ est donc « de la bonne taille » et $\mathrm{Rés}_{p,q}(\text{év}(\mathrm{P}),\text{év}(\mathrm{Q})) = 0$ si et seulement si év(P) et év(Q) ont une racine commune dans $\overline{\mathrm{K}}$. On a donc bien montré que $\mathrm{R}(y) = 0$ si et seulement si $\mathrm{P}(\mathrm{X},y)$ et $\mathrm{Q}(\mathrm{X},y)$ ont une racine commune dans $\overline{\mathrm{K}}$.
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 $3\mathrm{Y}^4 - 3\mathrm{Y}^2$, 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 $\mathrm{Y}^4 - 3\mathrm{Y}^2$ 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 $\mathrm{P}(\mathrm{X},0)$ et $\mathrm{Q}(\mathrm{X},0)$ 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 $\deg_{\mathrm{X}} \mathrm{P}(\mathrm{X},y) < p$ et $\deg_{\mathrm{X}} \mathrm{Q}(\mathrm{X},y) < q$.

   Si les deux degrés sont diminués, alors $\mathrm{R}(y) = 0$ 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 $\mathrm{P}(\mathrm{X},y)$ n'est pas constant, afin que $\mathrm{Rés}_{\mathrm{X}}(\mathrm{P}(\mathrm{X},y),\mathrm{Q}(\mathrm{X},y))$ 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 $\mathrm{Rés}_{\mathrm{X},p,q}(\mathrm{P}(\mathrm{X},y),\mathrm{Q}(\mathrm{X},y))$ est proportionnel à $\mathrm{Rés}_{\mathrm{X},p-1,q}(\mathrm{P}(\mathrm{X},y),\mathrm{Q}(\mathrm{X},y))$. Quitte à réitérer le processus si $\deg_{\mathrm{X}} \mathrm{P}(\mathrm{X},y) < p-1$, on voit que le résultant $p \times q$ est proportionnel au « bon » résultant $\mathrm{Rés}_{\mathrm{X}}(\mathrm{P}(\mathrm{X},y),\mathrm{Q}(\mathrm{X},y))$, qui est bien nul si et seulement si il existe x tel que $\mathrm{P}(x,y) = \mathrm{Q}(x,y) = 0$.

Exercice 2.
Expliquons ici la méthode générale à employer lorsqu'on considère des paramétrages rationnels (c'est-à-dire par des fractions rationnelles).
Si on a $x = \mathrm{A}(t)/\mathrm{B}(t)$ et $y = \mathrm{C}(t)/\mathrm{D}(t)$, alors $x\mathrm{B}(t) - \mathrm{A}(t) = 0$ et $\mathrm{D}(t)y - \mathrm{C}(t) = 0$. Si l'on considère $\mathrm{R}(\mathrm{X}, \mathrm{Y}) = \mathrm{Rés}_{\mathrm{T}}(\mathrm{B}(\mathrm{T})\mathrm{X} - \mathrm{A}(\mathrm{T}), \mathrm{D}(\mathrm{T})\mathrm{Y} - \mathrm{C}(\mathrm{T})) \in \mathbf{R}[\mathrm{X}, \mathrm{Y}]$, on a alors pour tout (x, y) de la courbe paramétrée l'existence d'un t tel que $x\mathrm{B}(t) - \mathrm{A}(t) = y\mathrm{D}(t) - \mathrm{C}(t) = 0$ et donc $\mathrm{R}(x, y) = 0$.
Le polynôme R nous donne donc une équation vérifiée par tous les points de la courbe paramétrée considérée. Ici on obtenait comme équations :

1. $\mathrm{X}^2\mathrm{Y}^2 - 2\mathrm{X}^2\mathrm{Y} + \mathrm{X}^2 + \mathrm{Y}^2 + 4\mathrm{XY} - 4\mathrm{X} + 3 = 0$.
2. $\mathrm{X}^4 + \mathrm{Y}^4 + 2\mathrm{X}^2\mathrm{Y}^2 - \mathrm{X}^2 + \mathrm{Y}^2 = 0$.

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 3.
Convenons de noter $\widetilde{p}$ la fonction polynomiale associée à un polynôme p. L'hypothèse de l'énoncé est que $\widetilde{f}_{|\mathrm{D}(h)} = \widetilde{g}_{|\mathrm{D}(h)}$. Cela implique $(\widetilde{f} - \widetilde{g})\widetilde{h} = 0$. Comme le corps est infini, cela implique $(f - g)h = 0$. Mais l'anneau des polynômes est intègre et h est non nul, donc on a bien $f = g$.

Exercice 4.

1. Les polynômes constants sont clairement invariants par similitude. La somme et le produit de deux polynômes invariants sont des polynômes invariants. $\mathrm{K}[\mathrm{M}_n(\mathrm{K})]^{\mathrm{GL}_n(\mathrm{K})}$ est donc une sous-algèbre de $\mathrm{K}[\mathrm{M}_n(\mathrm{K})]$.
2. Le polynôme caractéristique de $(\mathrm{X}_{i,j})_{\substack{1\leq i\leq n\\1\leq j\leq n}}$ est $\chi(\mathrm{T}) = \mathrm{dét}(\delta_{i,j} - \mathrm{X}_{i,j})_{\substack{1\leq i\leq n\\1\leq j\leq n}}$. C'est un polynôme unitaire et de degré n de $\mathrm{A}[\mathrm{T}]$, que l'on peut donc écrire
$$\chi(\mathrm{T}) = \mathrm{T}^n - \varphi_1\mathrm{T}^{n-1} + \varphi_2\mathrm{T}^{n-2} + \cdots + (-1)^n\varphi_n, \text{ où } \forall p \in [\![1, n]\!], \varphi_p \in \mathrm{A}.$$
La fonction « polynôme caractéristique »
$$\begin{array}{ccc} \mathrm{M}_n(\mathrm{K}) & \to & \mathrm{K}[\mathrm{T}] \\ \mathrm{M} & \mapsto & \chi_{\mathrm{M}}(\mathrm{T}) \end{array}$$
est une fonction (polynomiale) sur $\mathrm{M}_n(\mathrm{K})$ invariante par similitude. Il en est donc de même de chacun de ses coefficients, qui sont précisément les fonctions polynomiales $\mathrm{M}_{\mathrm{K}} \to \mathrm{K}$ associées aux polynômes φ_p. On a donc bien $\varphi_p \in \mathrm{B}$.
D'après les relations coefficients-racines, la fonction φ_p s'identifie au p-ième polynôme symétrique des valeurs propres (comptées avec multiplicités). On a donc
$$\varphi_1 = \mathrm{tr} = \sum_{i=1}^{n} \mathrm{X}_{i,i};$$
$$\varphi_n = \mathrm{dét} = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} \mathrm{X}_{i,\sigma(i)}.$$
3. La conjugaison d'une matrice diagonale $\mathrm{diag}(z_1, \ldots, z_n)$ par une matrice de permutation P_σ est la matrice diagonale $\mathrm{diag}(z_{\sigma(1)}, \ldots, z_{\sigma(n)})$. La fonction polynomiale associée à $f \in \mathrm{B}$ se restreint donc sur $\mathrm{D} = \{\mathrm{diag}(z_1, \ldots, z_n)\}$ en un polynôme symétrique des z_i. Sur D, f coïncide donc avec un polynôme des $\Sigma_p(z_1, \ldots, z_n)$. Mais, d'après les relations coefficients-racines, $\Sigma_p(z_1, \ldots, z_n) = \varphi_p(\mathrm{diag}(z_1, \ldots, z_n))$; f coïncide donc sur D avec un polynôme des φ_p.

4. Soit $f \in \mathrm{B}$. D'après la question précédente, il existe $\mathrm{P} \in \mathrm{K}[\mathrm{Y}_1, \ldots, \mathrm{Y}_n]$ tel que f et $\mathrm{P}(\varphi_1, \ldots, \varphi_p)$ coïncident sur D. Mais ces deux fonctions polynomiales sont invariantes par similitude. Elles coïncident donc sur l'ensemble des matrices diagonalisables sur K. Puisque K est algébriquement clos, une matrice est diagonalisable dès que son polynôme caractéristique est séparable, c'est-à-dire dès que le discriminant de celui-ci ne s'annule pas. Les fonctions polynomiales f et $\mathrm{P}(\varphi_1, \ldots, \varphi_n)$ coïncident donc en particulier sur $\mathrm{D}(\Delta(\chi)) \subset \mathrm{M}_n(\mathrm{K})$. D'après l'exercice précédent, on a bien $f = \mathrm{P}(\varphi_1, \ldots, \varphi_n)$.
5. La question précédente dit exactement que ce morphisme (bien défini grâce à la propriété universelle) est surjectif. Reste à voir qu'il est injectif. Soit donc P un polynôme tel que $\mathrm{P}(\varphi_1, \ldots, \varphi_n) = 0$. On a vu que $\varphi_p(\mathrm{diag}(z_1, \ldots, z_n)) = \Sigma_p(z_1, \ldots, z_n)$: la relation précédente entraîne donc en particulier $\mathrm{P}(\Sigma_1, \ldots, \Sigma_n) = 0$ et donc $\mathrm{P} = 0$.

Exercice 5.

1. Soient $\tilde{\mathrm{P}}$ et $\tilde{\mathrm{Q}}$ comme dans l'énoncé. Alors on a $\tilde{\mathrm{P}}(\alpha_1, \alpha_1+\alpha_2) = \mathrm{P}(\alpha_1) = 0$ et $\tilde{\mathrm{Q}}(\alpha_1, \alpha_1+\alpha_2) = \mathrm{Q}(\alpha_2) = 0$. Donc les polynômes $\tilde{\mathrm{P}}(\mathrm{X}, \alpha_1 + \alpha_2)$ et $\tilde{\mathrm{Q}}(\mathrm{X}, \alpha_1 + \alpha_2)$ ont un zéro commun, ce qui prouve que $\mathrm{R}(\alpha_1 + \alpha_2) = 0$.
2. Considérons cette fois les polynômes $\tilde{\mathrm{P}} = \mathrm{P}(\mathrm{X})$ et $\tilde{\mathrm{Q}} = \mathrm{X}^{\deg \mathrm{Q}}(\mathrm{Y}/\mathrm{X})$. Alors on a $\tilde{\mathrm{P}}(\alpha_1, \alpha_1\alpha_2) = \mathrm{Q}(\alpha_1, \alpha_1\alpha_2)$ et donc $\mathrm{Rés}_{\mathrm{X}}(\tilde{\mathrm{P}}, \tilde{\mathrm{Q}})(\alpha_1\alpha_2) = 0$.

Exercice 6.

1. Notons α_i les racines réelles de P rangées par ordre croissant et $\gamma_i, \bar{\gamma_i}$ ses racines complexes conjuguées. On peut supposer que les α_i sont racines simples (sinon $\Delta(\mathrm{P}) = \prod_{i=1}^n \mathrm{P}'(\alpha_i) = 0$). Alors, en appliquant les formules du cours donnant $\mathrm{Rés}(\mathrm{PQ}, \mathrm{R}) = \mathrm{Rés}(\mathrm{P}, \mathrm{R})\,\mathrm{Rés}(\mathrm{Q}, \mathrm{R})$ et $\mathrm{Rés}(\mathrm{X} - \alpha, \mathrm{P}) = \mathrm{P}(\alpha)$, on obtient

$$\mathrm{Disc}(\mathrm{P}) = (-1)^{\frac{d(d-1)}{2}} \prod_{i=1}^{n} \mathrm{P}'(\alpha_i) \prod_j \mathrm{P}'(\gamma_j)\mathrm{P}'(\bar{\gamma_j}) = (-1)^{\frac{d(d-1)}{2}} \prod_{i=1}^{n} \mathrm{P}'(\alpha_i) \prod_j |\mathrm{P}'(\gamma_j)|^2$$

et l'assertion sur le signe en découle.

2. Puisque les α_i sont racines simples, on sait par des arguments d'analyse que les signes des $\mathrm{P}'(\alpha_i)$ sont alternés. On distingue le cas où d est pair du cas où d est impair. Dans les deux cas on aura $\mathrm{P}'(\alpha_n) > 0$ (car le coefficient dominant de P est positif). Si d est pair, on aura $\mathrm{P}'(\alpha_1) < 0$ et donc $\mathrm{sgn}(\prod_{i=1}^n \mathrm{P}'(\alpha_i)) = \prod_{i=1}^n (-1)^i = (-1)^{\frac{n(n-1)}{2}}$. Au passage on a obtenu que n était pair car $(-1)^n = 1$. De même, si d est impair, on a $\mathrm{P}'(\alpha_1) > 0$ et donc $\mathrm{sgn}(\prod_{i=1}^n \mathrm{P}'(\alpha_i)) = \prod_{i=1}^n (-1)^{i-1} = (-1)^{\frac{(n-1)(n-2)}{2}}$, avec n impair.
   À présent, plaçons nous dans le cas où $\mathrm{Disc}(\mathrm{P}) > 0$, avec par exemple d pair. D'après la première question et ce que l'on vient de dire, $(-1)^{\frac{d(d-1)}{2} + \frac{n(n-1)}{2}} = 1$, donc $\frac{d(d-1)}{2} + \frac{n(n-1)}{2}$ est pair. De deux choses l'une : soit $d \equiv 0$ (toutes les congruences dans la suite sont modulo 4), et alors $\frac{d(d-1)}{2}$ est divisible par 2, donc il en va de même de $\frac{n(n-1)}{2}$, et donc de $\frac{n}{2}$ (car $n-1$ impair) ; soit $d \equiv 2$ et alors on a aussi $\frac{n}{2} \equiv 2$.
   Dans le cas où d est impair, on a $\frac{d(d-1)}{2} + \frac{(n-1)(n-2)}{2}$ qui est pair (avec n et d impairs. Le même raisonnement nous prouve que $d - 1 \equiv n - 1$ et donc $n \equiv d$.
   Enfin dans le cas où $\mathrm{Disc}(\mathrm{P}) < 0$. Traitons uniquement le cas où d est pair, le cas d impair s'en déduit facilement. On a donc $\frac{d(d-1)}{2} + \frac{n(n-1)}{2}$ qui est impair. Si $d \equiv 0$, alors $\frac{n(n-1)}{2}$ est impair, donc $n \equiv 2$. Et de même, si $d \equiv 2$ on a $n \equiv 0$.

Exercice 7.

1. Soit $\mathrm{R} \in \mathbf{C}(\mathrm{X})[\mathrm{Y}]$ irréductible qui divise P et Q. On peut écrire $\mathrm{R} = \frac{\mathrm{D}}{a}$ avec $a \in \mathbf{C}[\mathrm{X}]$ et $\mathrm{D} \in \mathbf{C}[\mathrm{X}][\mathrm{Y}]$ primitif (et donc irréductible), et on a alors D qui divise à la fois aP et aQ. Écrivons alors $a\mathrm{P} = \mathrm{DS}_1$ et $a\mathrm{Q} = \mathrm{DS}_2$. Si b est un facteur irréductible de a dans $\mathbf{C}[\mathrm{X}]$, alors soit b divise D, soit b divise à la fois S_1 et S_2. Comme D est primitif, b divise S_1 et S_2. Par récurrence (sur les facteurs irréductibles de a), on voit que D divise P et Q. Or, par hypothèse, ceci implique que $\mathrm{D} = 1$, et donc $\mathrm{R} = \frac{1}{a}$ est inversible dans $\mathbf{C}(\mathrm{X})[\mathrm{Y}]$, et donc P et Q sont premiers entre eux dans cet anneau.
2. Dans $\mathbf{C}(\mathrm{X})[\mathrm{Y}]$, on dispose du théorème de Bézout, et donc il existe $\mathrm{U}, \mathrm{V} \in \mathbf{C}(\mathrm{X})[\mathrm{Y}]$ tels que $\mathrm{PU} + \mathrm{QV} = 1$. Si $\mathrm{D} \in \mathbf{C}[\mathrm{X}]$ est un dénominateur commun aux coefficients de U et V, alors on a $\mathrm{AP} + \mathrm{BQ} = \mathrm{D}$.
3. Si (x, y) est dans V, alors on a $\mathrm{D}(x) = 0$ d'après la question précédente. Ce qui implique déjà qu'il n'y a qu'un nombre fini de valeurs de x possibles pour les couples $(x, y) \in \mathrm{V}$. De même, on peut appliquer le raisonnement de la question précédente dans $\mathbf{C}(\mathrm{Y})[\mathrm{X}]$ et trouver un $\mathrm{D}' \in \mathrm{K}[\mathrm{Y}]$ tel que si (x, y) est dans V, alors $\mathrm{D}'(y) = 0$. Il n'y a donc aussi qu'un nombre fini de valeurs possibles de y, et donc de couples (x, y).

Exercice 8.

1. Puisque P et Q sont unitaires en Y, ils restent de même degré lorsqu'on les évalue en x. Ainsi on a bien l'équivalence usuelle $\mathrm{R}(x) = 0$ si et seulement si il existe $y \in \mathbf{C}$ tel que $\mathrm{P}(x, y) = \mathrm{Q}(x, y) = 0$, cette dernière condition étant équivalente à $x \in \pi(\mathrm{V})$.
2. Soit M la matrice de Sylvester de P et Q (vus comme polynômes en Y). On a

$$\deg_{\mathrm{X}} \mathrm{M}_{i,j} = \begin{cases} i - j & \text{si } 1 \leq j \leq q \\ i - j + q & \text{si } q + 1 \leq j \leq p + q \end{cases}$$

En appliquant la formule de définition du déterminant :

$$\mathrm{R} = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{j=1}^{p+q} \mathrm{M}_{\sigma(j),j}.$$

En étudiant les degrés, cela donne donc

$$\begin{aligned} \deg_{\mathrm{X}} \mathrm{R} \leq \sum_{j=1}^{p+q} \deg_{\mathrm{X}}(\mathrm{M}_{\sigma_j,j}) &= \sum_{j=1}^{q} \deg_{\mathrm{X}}(\mathrm{M}_{\sigma(j),j}) + \sum_{j=q+1}^{p+q} \deg_{\mathrm{X}}(\mathrm{M}_{\sigma(j),j}) \\ &\leq \sum_{j=1}^{q} \sigma(j) - j + \sum_{j=q+1}^{p+q} (\sigma_(j) - j + q) = pq \end{aligned}$$

On conclut immédiatement grâce à la question précédente.

Exercice 9.

1. Il s'agit de voir que $\Phi_p(\mathrm{X} + 1)$ est irréductible. En effet, cela implique alors que $\Phi_p(\mathrm{X})$ l'est aussi car si $\Phi_p(\mathrm{X}) = \mathrm{P}(\mathrm{X})\mathrm{Q}(\mathrm{X})$, alors $\Phi_p(\mathrm{X} + 1) = \mathrm{P}(\mathrm{X} + 1)\mathrm{Q}(\mathrm{X} + 1)$. Mais $\Phi_p(\mathrm{X} + 1) = \frac{(\mathrm{X}+1)^p - 1}{\mathrm{X}+1-1} = \sum_{k=1}^{p} \binom{p}{k} \mathrm{X}^{k-1}$. Or, pour $1 \leq k \leq p - 1$, p divise $\binom{p}{k}$. De plus, $\binom{p}{1} = p$ n'est pas divisible par p^2. Donc $\Phi_p(\mathrm{X} + 1)$ est un polynôme d'Eisenstein pour p, et donc est irréductible dans $\mathbf{Z}[\mathrm{X}]$.

2. Utilisons l'isomorphisme canonique $K[X, Y, Z] \simeq K[X, Y][Z]$. Pour montrer que $X^2+Y^2+Z^2$ est irréductible, il s'agit donc de montrer qu'il existe un premier P dans $K[X, Y]$ tel que P divise X^2+Y^2, mais tel que P^2 ne le divise pas. Or, si on considère $X^2+Y^2 \in K[X][Y]$, c'est un polynôme de degré 2, donc il possède un facteur irréductible non constant. Il s'agit de s'assurer qu'un de ces facteurs au moins n'est pas facteur multiple. Mais dans $K(X)[Y]$, X^2+Y^2 est sans facteur carré. En effet, un tel facteur diviserait alors le PGCD de X^2+Y^2 et de son polynôme dérivé. Mais dans $K(X)[Y]$, on dispose de la relation de Bézout, et on peut écrire $(X^2+Y^2) - \frac{Y}{2}(2Y) = X^2$, prouvant que le PGCD de X^2+Y^2 et de sa dérivée est une constante de $K(X)$. X^2+Y^2 n'a donc pas de facteur carré dans $K(X)[Y]$, et a fortiori dans $K[X][Y]$. Si P est un facteur irréductible de X^2+Y^2, on peut alors appliquer le critère d'Eisenstein dans $K[X, Y][Z]$.