Racines des polynômes : correction

Exercice 1.

1. Non : de tels entiers seraient les racines du polynôme
$$\mathrm{X}^3 - (m+n+l)\mathrm{X}^2 + (mn+nl+lm)\mathrm{X} - mnl = \mathrm{X}^3 - 288\mathrm{X}^2 + 540\mathrm{X} - 960,$$
mais celui-ci n'a pas toutes ses racines dans $\mathbf{Z}$: le critère d'Eisenstein (pour $p = 3$) montre par exemple qu'il est irréductible sur $\mathbf{Z}$; on pourrait également étudier la fonction polynomiale associée pour voir qu'il n'a qu'une racine, simple, dans $\mathbf{R}$.
2. Le corps $\mathrm{K}(\mathrm{T})$ est une extension de K. L'élément $\mathrm{T} \in \mathrm{K}(\mathrm{T})$ est transcendant sur K. (Le corps qu'il engendre, $\mathrm{K}(\mathrm{T})$ tout entier, est bien de dimension infinie sur K.)
3. La somme à calculer est la valeur du polynôme symétrique
$$\mathrm{X}_1^2 + \cdots + \mathrm{X}_n^2 = (\mathrm{X}_1 + \cdots + \mathrm{X}_n)^2 - 2 \sum_{1 \leq i < j \leq n} \mathrm{X}_i \mathrm{X}_j$$
évalué en $x_i = \zeta_n^{i-1}$. Les éléments $1, \zeta_n, \ldots, \zeta_n^{n-1}$ sont les racines de $\mathrm{X}^n - 1$ donc $\sum x_i$ en est le coefficient en X^{n-1} (0, dès que $n > 1$) et $\sum_{i<j} x_i x_j$ le coefficient en X^{n-2} (0, dès que $n > 3$). Ainsi la somme vaut 0 dès que $n > 2$, et un calcul direct donne qu'elle vaut 1 quand $n = 1$ et 2 quand $n = 2$.
En notant $\mu_n \subset \mathbf{C}$ le groupe des racines n-ièmes de l'unité, on pouvait également calculer la somme demandée, qui n'est autre que $\sum_{\zeta \in \mu_n} \zeta^2$, en remarquant que le morphisme $\zeta \mapsto \zeta^2$ est un automorphisme de μ_n quand n est impair et qu'il prend chaque valeur de $\mu_{n/2}$ exactement deux fois quand n est pair. La somme valait donc $\sum_{\zeta \in \mu_n} \zeta$ dans le premier cas est $2 \sum_{\zeta \in \mu_{n/2}} \zeta$ dans le second. Puisque, dès que $m > 1$, la somme des racines m-ièmes de l'unité est nulle, on retrouve le résultat.
4. Soit $\mathrm{P}(\mathrm{X}) = a_n \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_1 \mathrm{X} + a_0 \in \mathbf{Z}[\mathrm{X}]$ avec $a_n \neq 0$ et soit $a/b \in \mathbf{Q}$ (a et b premiers entre eux) une racine de P. Puisque $\mathrm{P}(a/b) = 0$, on obtient l'égalité (dans $\mathbf{Z}$) :
$$-a_0 b^n = a_n a^n + a_{n-1} b a^{n-1} + \cdots + a_1 b^{n-1} a.$$
Comme a divise le terme de droite, il divise le terme de gauche et doit donc diviser a_0 car $\mathrm{pgcd}(a, b) = 1$. De même, comme b divise $a_n a^n$ et que $\mathrm{pgcd}(a, b) = 1$, on a $b | a_n$. En particulier, quand P est unitaire, on doit avoir $b = \pm 1$ et $a/b \in \mathbf{Z}$.

Exercice 2.

1. L'anneau $\mathrm{K}[\mathrm{X}]$ est principal, et $\mathrm{pgcd}(\mathrm{P}_1, \mathrm{P}_2) = 1$ signifie que $(\mathrm{P}_1, \mathrm{P}_2) = (1)$; il existe donc deux polynômes $\mathrm{U}, \mathrm{V} \in \mathrm{K}[\mathrm{X}]$ tels que $\mathrm{P}_1\mathrm{U} + \mathrm{P}_2\mathrm{V} = 1$. En multipliant par C, on obtient $\mathrm{P}_1(\mathrm{UC}) + \mathrm{P}_2(\mathrm{VC}) = \mathrm{C}$.
Effectuons la division euclidienne de UC par P_2 : il existe deux polynômes $\mathrm{Q}_2, \mathrm{R}_2 \in \mathrm{K}[\mathrm{X}]$ tels que $\mathrm{UC} = \mathrm{Q}_2\mathrm{P}_2 + \mathrm{R}_2$ et $\deg \mathrm{R}_2 < \deg \mathrm{P}_2$. De même, il existe $\mathrm{Q}_1, \mathrm{R}_1$ tels que $\mathrm{VC} = \mathrm{Q}_1\mathrm{P}_1 + \mathrm{R}_1$ et $\deg \mathrm{R}_1 < \deg \mathrm{P}_1$.
On obtient donc
$$\mathrm{C} = \mathrm{P}_1(\mathrm{Q}_2\mathrm{P}_2 + \mathrm{R}_2) + \mathrm{P}_2(\mathrm{Q}_1\mathrm{P}_1 + \mathrm{R}_1) = (\mathrm{P}_1\mathrm{R}_2 + \mathrm{P}_2\mathrm{R}_1) + \mathrm{P}_1\mathrm{P}_2(\mathrm{Q}_1 + \mathrm{Q}_2).$$
Comme $\deg(\mathrm{P}_1\mathrm{R}_2 + \mathrm{P}_2\mathrm{R}_1) < \deg(\mathrm{PQ})$ et que $\deg(\mathrm{P}_1\mathrm{P}_2(\mathrm{Q}_1 + \mathrm{Q}_2)) \geq \deg(\mathrm{P}_1\mathrm{P}_2)$ si $\mathrm{Q}_1 + \mathrm{Q}_2 \neq 0$, on a nécessairement $\mathrm{Q}_1 + \mathrm{Q}_2 = 0$, d'où le résultat cherché.

2. Supposons que P_1 et P_2 soient irréductibles dans K[X]. La décomposition en éléments simples de C/P_1P_2 s'écrit alors

$$\frac{C}{P_1P_2} = \frac{R_1}{P_1} + \frac{R_2}{P_2},$$

avec $\deg R_k < \deg P_k$ et on a bien $C = R_1P_2 + R_2P_1$. Réciproquement, si les R_k sont ceux donnés par la question précédente, la décomposition en éléments simples s'écrit de cette façon.

Dans le cas général, décomposons les polynômes P_i en irréductibles :

$$P_1 = \prod_{i=1}^{r_1} Q_{1,i}^{n_{1,i}}, \quad P_2 = \prod_{i=1}^{r_2} Q_{2,i}^{n_{2,i}}.$$

Puisque P_1 et P_2 sont premiers entre eux, les $(Q_{1,i})$ et $(Q_{2,i})$ sont disjoints. La décomposition en éléments simples de C/P_1P_2 s'écrit alors

$$\frac{C}{P_1P_2} = \sum_{i=1}^{r_1}\sum_{j=1}^{n_{1,i}} \frac{R_{1,i,j}}{Q_{1,i}^j} + \sum_{i=1}^{r_2}\sum_{j=1}^{n_{2,i}} \frac{R_{2,i,j}}{Q_{2,i}^j}$$

où pour tous $k \in \{1,2\}$, $i \leq r_k$ et $j \leq n_{k,i}$, $\deg R_{k,i,j} < \deg Q_{k,i}$. En réduisant chacun des termes au même dénominateur, on obtient bien une décomposition

$$\frac{C}{P_1P_2} = \frac{R_1}{P_1} + \frac{R_2}{P_2}$$

avec les mêmes propriétés que plus haut.

En résumé, si P_1 et P_2 sont premiers entre eux, le polynôme R_1 (resp. R_2) s'obtient en réduisant au même dénominateur la partie de la décomposition en éléments simples de C/P_1P_2 faisant intervenir au dénominateur les facteurs irréductibles de P_1 (resp. P_2).

Exercice 3.

1. Soit α une racine de P d'ordre supérieur ou égal à m. Alors, par définition, $(X-\alpha)^m$ divise P. Écrivons $P = (X-\alpha)^m Q$, et appliquons alors la formule de Leibniz à P, à l'ordre $k \leq m-1$.

$$P^{(k)} = \sum_{i=0}^{k} \binom{k}{i} ((X-\alpha)^m)^{(i)} Q^{(k-i)}$$

Notons que pour $k < m$, on a $((X-\alpha)^m)^{(i)} = m(m-1)\dots(m-i+1)(X-\alpha)^{m-i}$. Donc en évaluant $P^{(i)}$ en α, on obtient $P^{(i)}(\alpha) = 0$, ce qui est le résultat recherché.

2. La réciproque se prouve par récurrence sur m. On sait déjà que le résultat est vrai pour $m = 2$ (résultat du cours). On suppose donc que la propriété est vraie en rang $m-1$ et que α annule toutes les dérivées de P jusqu'à l'ordre m. Alors par hypothèse de récurrence, α est racine d'ordre inférieur ou égal à $m-1$ de P mais aussi de P'. Donc il existe Q tel que $P = (X-\alpha)^{m-1}Q$ et $(X-\alpha)^{m-1}$ divise également P'. En dérivant P, on trouve que $0 = P^{(m-1)}(\alpha) = (m-1)!Q(\alpha)$. Puisque $(m-1)! \neq 0$ (c'est l'hypothèse que l'on a faite sur la caractéristique), $(X-\alpha)$ divise Q. Et donc $(X-\alpha)^m$ divise P.

Un contre-exemple est donné par $P = (X+1)^2X = X^3 + X \in \mathbf{F}_2[X]$. Assurément, 1 est racine d'ordre 2 de P, et pourtant $P' = X^2 + 1$ et $P'' = 0$, donc 1 annule toutes les dérivées de P.

3. Si P et P′ ne sont pas premiers entre eux, ils ont un facteur irréductible (non constant) commun. Si $\alpha \in \overline{\mathrm{K}}$ est une racine de ce facteur irréductible, alors α est racine de P et de P′, ce qui signifie donc que c'est une racine de P de multiplicité supérieure ou égale à 2, et donc P n'est pas séparable.
   Inversement, si P n'est pas séparable, il possède dans $\overline{\mathrm{K}}$ une racine multiple α, qui est donc racine de P et de P′. Alors P et P′ ne sont pas premiers entre eux dans $\overline{\mathrm{K}}[\mathrm{X}]$ et donc ne le sont pas non plus dans K[X].
4. Dans le premier cas, le polynôme dérivé est $n\mathrm{X}^{n-1}$, qui n'est pas nul grâce à l'hypothèse sur la caractéristique de K. Comme 0 est sa seule racine, d'ordre $n-1$, il est premier avec $\mathrm{X}^n - 1$ donc ce dernier est séparable.
   Dans le deuxième cas, la dérivée est $-1 = p-1$, qui est bien un polynôme (constant !) premier avec $\mathrm{X}^p - \mathrm{X} - a$.

Exercice 4.

1. Si $\mathrm{P} = \sum_{i=0}^{n} a_i \mathrm{X}^i$, alors $\mathrm{P}' = \sum_{i=0}^{n-1} (i+1) a_{i+1} \mathrm{X}^i$. Donc si $\mathrm{P}' = 0$, $(i+1)a_i = 0$ quel que soit $i \geq 0$ et donc $a_i = 0$ pour tout $i \geq 1$, autrement dit, P est constant. La réciproque est évidente.
2. Supposons que $\mathrm{P}' = 0$. Comme dans la question précédente, on a $ia_i = 0$ pour tout $i \geq 1$. Si i n'est pas divisible par p, i est inversible dans K, et donc $a_i = 0$. Donc $\mathrm{P} = \sum_{i=0}^{n} a_{pi} \mathrm{X}^{pi} = \sum_{i=0}^{n} a_{pi} (\mathrm{X}^p)^i$.
3. Soit $\mathbf{F}_{p^n}$ un corps fini. Il s'agit de prouver que $x \mapsto x^p$ est surjectif. Mais si $x \in \mathbf{F}_{p^n}^{\times}$, on sait que $x^{p^n} = x$, et donc $(x^{p^{n-1}})^p = x$. Donc les corps finis sont parfaits.
   On peut également remarquer que $x \mapsto x^p$ étant en caractéristique p un morphisme de corps (*le morphisme de Frobenius*), il est toujours injectif. C'est donc en particulier un automorphisme si le corps est fini.
4. Soit P un polynôme irréductible non constant de K[X], où K est un corps parfait.
   Si K est de caractéristique nulle, alors P et P′ sont nécessairement premiers entre eux, car les seuls diviseurs de P sont les constantes et les multiples scalaires de P, et que P′ est de degré strictement inférieur à celui de P. Donc P est séparable.
   Dans le cas où K est de caractéristique p, on sait que le morphisme de Frobenius est surjectif sur K. Puisque le degré de P′ est strictement inférieur à celui de P et que P est irréductible, P et P′ ne peuvent avoir un facteur commun que si $\mathrm{P}' = 0$. Mais cela impose alors l'existence de $\mathrm{Q} \in \mathrm{K}[\mathrm{X}]$ tel que $\mathrm{P} = \mathrm{Q}(\mathrm{X}^p)$. Écrivons $\mathrm{Q} = \sum_{i=0}^{n} a_i \mathrm{X}^i$. Puisque le morphisme de Frobenius est surjectif, il existe $b_i \in \mathrm{K}$ tel que $b_i^p = a_i$. On a alors $\mathrm{P} = \left(\sum_{i=0}^{n} b_i \mathrm{X}^i\right)^p$. Mais P est un polynôme irréductible non constant, donc une telle décomposition est absurde : P′ est non nul et P est séparable.
5. $\mathrm{X}^p - \mathrm{T}$ est irréductible d'après le critère d'Eisenstein appliqué à $\mathrm{A} = \mathbf{F}_p[\mathrm{T}]$ et $\mathrm{I} = (\mathrm{T})$. D'un autre côté, si $\mathrm{L}/\mathbf{F}_p(\mathrm{T})$ est une extension dans laquelle ce polynôme admet une racine α, on a $\mathrm{X}^p - \mathrm{T} = \mathrm{X}^p - \alpha^p = (\mathrm{X} - \alpha)^p \in \mathrm{L}[\mathrm{X}]$ puisque L est un corps de caractéristique p.

Exercice 5. Soit $\alpha_1, \ldots, \alpha_r$ les racines réelles distinctes de P et $\beta_1, \overline{\beta_1}, \ldots, \beta_s, \overline{\beta_s}$ ses racines complexes. On peut écrire

$$\mathrm{P} = a \prod_{i=1}^{r} (\mathrm{X} - \alpha_i)^{m_i} \prod_{j=1}^{s} (\mathrm{X} - \beta_j)^{n_j} (\mathrm{X} - \overline{\beta_j})^{n_j}.$$

Alors, puisque P est toujours positif, on en déduit que $a > 0$, et que les m_i sont tous pairs. On peut donc écrire

$$\mathrm{P} = \left(\sqrt{a}\prod_{i=1}^{r}(\mathrm{X}-\alpha_i)^{\frac{m_i}{2}}\prod_{j=1}^{s}(\mathrm{X}-\beta_j)^{n_i}\right)\left(\sqrt{a}\prod_{i=1}^{r}(\mathrm{X}-\alpha_i)^{\frac{m_i}{2}}\prod_{j=1}^{s}(\mathrm{X}-\overline{\beta_j})^{n_i}\right).$$

Autrement dit, $\mathrm{P} = (\mathrm{A} + i\mathrm{B})(\mathrm{A} - i\mathrm{B})$, avec A, B deux polynômes réels. On en déduit que $\mathrm{P} = \mathrm{A}^2 + \mathrm{B}^2$.
Remarque : Le nom de cet exercice est une allusion au dix-septième problème de David Hilbert, qui demandait si tout polynôme $\mathrm{P} \in \mathbf{R}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ définissant une fonction positive pouvait s'écrire comme somme de carrés de fractions rationnelles. Il a été résolu positivement par Emil Artin en 1927. On savait déjà (Hilbert, 1888) en revanche qu'un tel polynôme ne s'écrit pas forcément comme somme de carrés de polynômes.

Exercice 6. Si P est un polynôme homogène, il est facile de vérifier que la fonction polynomiale vérifie bien la propriété annoncée. Il est par contre plus dur de montrer la réciproque. Supposons donc que pour tout $\lambda \in \mathrm{K}$ et tout $(x_1, \ldots, x_n) \in \mathrm{K}^n$ on aie

$$\mathrm{P}(\lambda x_1, \ldots, \lambda x_n) = \lambda^d \mathrm{P}(x_1, \ldots, x_n).$$

Écrivons $\mathrm{P} = \sum_i \mathrm{P}_i$ la décomposition de P en polynômes homogènes. Soit $\lambda \in \mathrm{K}$, et considérons le polynôme $\mathrm{P}(\lambda \mathrm{X}_1, \ldots, \lambda \mathrm{X}_n) - \lambda^d \mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$. Par hypothèse, la fonction polynomiale associée est nulle, et donc (K étant infini), ce polynôme est nul également (et ce quel que soit λ). On a donc

$$\sum_i \lambda^i \mathrm{P}_i(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \lambda^d \sum_i \mathrm{P}_i(\mathrm{X}_1, \ldots, \mathrm{X}_n)$$

ce qui peut également s'écrire

$$\sum_i \lambda^{i-d} \mathrm{P}_i(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \sum_i \mathrm{P}_i(\mathrm{X}_1, \ldots, \mathrm{X}_n).$$

Or, pour $i \neq d$, soit λ tel que $\lambda^{i-d} \neq 1$ (un tel élément existe toujours, car il n'y a qu'un nombre fini de racines $(i-d)$-ièmes de l'unité dans K, qui est infini). L'unicité de la décomposition en composantes homogènes indique que pour un tel λ, $\lambda^{i-d}\mathrm{P}_i = \mathrm{P}_i$, et donc $\mathrm{P}_i = 0$. Ceci prouve que $\mathrm{P} = \mathrm{P}_d$ et donc que P est homogène de degré d.

Exercice 7. $\mathrm{D}(\mathrm{P}) = \mathrm{P}^{-1}(\mathbf{R} \setminus \{0\})$ est ouvert car P est continu. Nous allons montrer que son complémentaire est d'intérieur vide. Ce complémentaire est l'ensemble des points d'annulation de P. S'il contenait un ouvert, il contiendrait en particulier un produit de parties infinies de $\mathbf{R}$ (prendre une boule pour la norme du max sur $\mathbf{R}^n$). Or, un lemme du cours dit que si un polynôme s'annule sur un tel ensemble, alors il est nul. Donc le complémentaire est bien d'intérieur vide. La même preuve donne le même résultat sur $\mathbf{C}^n$.