Corrigé du DM n°25

Exercice 1

Tout d'abord, écrivons M sous forme plus explicite :

$$\Delta_n = \begin{vmatrix} 0 & 1 & 2 & 3 & \dots & n-1 \\ 1 & 0 & 1 & 2 & \dots & n-2 \\ 2 & 1 & 0 & 1 & \dots & n-3 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ n-2 & n-3 & \dots & 1 & 0 & 1 \\ n-1 & n-2 & \dots & 2 & 1 & 0 \end{vmatrix}$$

Effectuons l'opération $C_1 \leftarrow C_1 - C_2$:

$$\Delta_n = \begin{vmatrix} -1 & 1 & 2 & 3 & \dots & n-1 \\ 1 & 0 & 1 & 2 & \dots & n-2 \\ 1 & 1 & 0 & 1 & \dots & n-3 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 1 & n-3 & \dots & 1 & 0 & 1 \\ 1 & n-2 & \dots & 2 & 1 & 0 \end{vmatrix}$$

Si on fait à présent $C_2 \leftarrow C_2 - C_3$:

$$\Delta_n = \begin{vmatrix} -1 & -1 & -1 & \dots & n-1 \\ 1 & -1 & -1 & \dots & n-2 \\ 1 & 1 & -1 & \dots & n-3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 0 \end{vmatrix}$$

On fait cela pour toutes les colonnes sauf la dernière : chaque colonne moins la suivante, ce qui donne :

$$\Delta_n = \begin{vmatrix} -1 & -1 & -1 & \dots & -1 & n-1 \\ 1 & -1 & -1 & \dots & -1 & n-2 \\ 1 & 1 & -1 & \dots & -1 & n-3 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & 1 & -1 & 1 \\ 1 & 1 & \dots & 1 & 1 & 0 \end{vmatrix}$$

En d'autres termes, sauf sur la dernière colonne, on a des -1 au-dessus (au sens large) de la diagonale, et des 1 en-dessous (au sens strict) de la diagonale. Si on ajoute la dernière ligne à toutes les autres (i.e. $L_i \leftarrow L_i + L_n, \forall i \leqslant n-1$) :

$$\Delta_n = \begin{vmatrix} 0 & 0 & 0 & \dots & 0 & n-1 \\ 2 & 0 & 0 & \dots & 0 & n-2 \\ 2 & 2 & 0 & \dots & 0 & n-3 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 2 & 2 & \dots & 2 & 0 & 1 \\ 2 & 2 & \dots & 2 & 2 & 0 \end{vmatrix}$$

Si on développe à présent par rapport à la première ligne (ne pas oublier la puissance de -1) :

$$\Delta = (-1)^{n+1} \times (n-1) \times \begin{vmatrix} 2 & 0 & 0 & \dots & 0 \\ 2 & 2 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 2 & 2 & \dots & 2 & 0 \\ 2 & 2 & \dots & 2 & 2 \end{vmatrix}$$

On obtient une matrice triangulaire inférieure (de taille $n-1$). On trouve finalement que :

$$\boxed{\Delta = (-1)^{n+1} \times (n-1) \times 2^{n-1}}$$

Exercice 2

1 Soit $\sigma \in \mathrm{S}_n$. Précisons que les $\mathrm{X}_{i,j}$ sont d'espérance nulle et de variance égale à 1 (ce qu'on trouve par un calcul direct). Par indépendance des $\mathrm{X}_{i,j}$, on a :

$$\mathrm{E}(\mathrm{Y}_\sigma) = \prod_{i=1}^{n} \mathrm{E}(\mathrm{X}_{\sigma(1),1})$$

si bien que $\mathrm{E}(\mathrm{Y}_\sigma) = 0$. De plus, Y_σ étant un produit de variables aléatoires valant ± 1, son carré est constant égal à 1 donc son espérance vaut 1. Finalement,

$$\boxed{\mathrm{E}(\mathrm{Y}_\sigma) = 0 \qquad \text{et} \qquad \mathrm{E}({\mathrm{Y}_\sigma}^2) = 1}$$

2 Découle du fait que σ et σ' sont deux fonctions distinctes donc diffèrent en au moins un point. De plus, le produit de l'énoncé ne contient aucune variable aléatoire de la forme $\mathrm{X}_{\sigma(i),i}$ ou $\mathrm{X}_{\sigma'(i),i}$ et les différentes $\mathrm{X}_{i,j}$ sont indépendantes : on conclut par le lemme des coalitions.

$$\boxed{\text{D'après le lemme des coalitions, } \mathrm{X}_{\sigma(i),i}\mathrm{X}_{\sigma'(i)} \text{ est indépendante de } \prod_{j\neq i} \mathrm{X}_{\sigma(j),j}\mathrm{X}_{\sigma'(j),j}.}$$

3 Par définition du déterminant :

$$\det(\mathrm{M}) = \sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)\mathrm{Y}_\sigma$$

Le problème est que les Y_σ ne sont pas indépendantes (il y a plusieurs permutations σ vérifiant $\sigma(1) = 1$ par exemple, donc on trouve dans les expressions des Y_σ correspondantes la même v.a. $\mathrm{X}_{1,1}$ donc les Y_σ ne sont pas indépendantes). Il faut donc le faire à la main. D'après la formule de König-Huygens :

$$\mathrm{V}(\det(\mathrm{M})) = \mathrm{E}\left(\left(\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)\mathrm{Y}_\sigma\right)^2\right) - \mathrm{E}\left(\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)\mathrm{Y}_\sigma\right)^2$$

En développant le premier terme (on obtient une somme double car on multiplie deux sommes simples) et par linéarité de l'espérance pour le deuxième :

$$\mathrm{V}(\det(\mathrm{M})) = \mathrm{E}\left(\sum_{(\sigma,\sigma')\in{\mathrm{S}_n}^2} \varepsilon(\sigma)\mathrm{Y}_\sigma\varepsilon(\sigma')\mathrm{Y}_{\sigma'}\right) - \left(\sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)\mathrm{E}(\mathrm{Y}_\sigma)\right)^2$$

D'une part, la deuxième quantité est nulle d'après la question 1, car les Y_σ sont d'espérance nulle. D'autre part, par linéarité de l'espérance et en séparant les cas où $\sigma = \sigma'$ des cas où $\sigma \neq \sigma'$:

$$\mathrm{V}(\det(\mathrm{M})) = \sum_{\sigma\in\mathrm{S}_n} \varepsilon(\sigma)^2\mathrm{E}({\mathrm{Y}_\sigma}^2) + \sum_{(\sigma,\sigma')\in{\mathrm{S}_n}^2,\sigma\neq\sigma'} \varepsilon(\sigma)\varepsilon(\sigma')\mathrm{E}(\mathrm{Y}_\sigma)\mathrm{Y}_{\sigma'}$$

D'après la question 1, et puisqu'une signature vaut ± 1, les termes de la première somme valent tous 1, et d'après la question 2, les termes de la deuxième somme sont tous nuls. Puisque S_n est de cardinal $n!$, cela donne le résultat voulu.

$$\boxed{\mathrm{V}(\det(\mathrm{M})) = n!}$$

Exercice 3

1 Soient donc x, y, z trois réels. On a

$$\begin{aligned}\mathrm{C}_2(x,y) &= \begin{vmatrix}\cos(x) & \cos(y)\\ \sin(x) & \sin(y)\end{vmatrix}\\ &= \cos(x)\sin(y) - \sin(x)\cos(y)\\ &= \sin(y-x)\end{aligned}$$

$$\text{et}\quad \mathrm{C}_3(x,y,z)=\begin{vmatrix}\cos(x) & \cos(y) & \cos(z)\\ \sin(x) & \sin(y) & \sin(z)\\ \cos(x+\pi/4) & \cos(y+\pi/4) & \cos(z+\pi/4)\end{vmatrix}$$

$$=\begin{vmatrix}\cos(x) & \cos(y) & \cos(z)\\ \sin(x) & \sin(y) & \sin(z)\\ \cos(x)\cos(\pi/4)-\sin(x)\sin(\pi/4) & \cos(y)\cos(\pi/4)-\sin(y)\sin(\pi/4) & \cos(z)\cos(\pi/4)-\sin(z)\sin(\pi/4)\end{vmatrix}$$

La dernière ligne étant CL des deux premières, les lignes sont liées donc le déterminant est nul.

$$\boxed{\mathrm{C}_2(x,y)=\sin(y-x)\text{ et }\mathrm{C}_3(x,y,z)=0.}$$

2 Soit $(x_1,\dots,x_n)\in\mathbb{K}^n$. Par hypothèse, il existe $(\lambda_1,\dots,\lambda_n)$ non tous nuls tels que $\sum_{i=1}^{n}\lambda_i f_i=0$. Par conséquent, pour tout $j\in[\![1\,;n]\!]$, $\sum_{i=1}^{n}\lambda_i f_i(x_j)=0$. En d'autres termes, si on note $\mathrm{L}_1,\dots,\mathrm{L}_n$ les vecteurs lignes, $\sum_{i=1}^{n}\lambda_n\mathrm{L}_i=0$: les vecteurs lignes sont liés, donc le déterminant est nul.

$$\boxed{\text{Si }(f_1,\dots,f_n)\text{ est liée, alors }\mathrm{C}_n\text{ est la fonction nulle.}}$$

3 Suivons l'indication de l'énoncé et supposons $\mathrm{C}_{n-1}\neq 0$, c'est-à-dire que C_{n-1} n'est pas la fonction nulle, donc il existe $(u_1,\dots,u_{n-1})$ tel que $\mathrm{C}_{n-1}(u_1,\dots,u_{n-1})\neq 0$. Notons

$$g:x\mapsto \mathrm{C}_n(u_1,\dots,u_{n-1},x)=\begin{vmatrix}f_1(u_1) & \dots & f_1(u_{n-1}) & f_1(x)\\ \vdots & \ddots & \vdots & \vdots\\ f_{n-1}(u_1) & \dots & f_{n-1}(u_{n-1}) & f_{n-1}(x)\\ f_n(u_1) & \dots & f_n(u_{n-1}) & f_n(x)\end{vmatrix}=0$$

Soit $x\in\mathrm{X}$. Développons par rapport à la dernière colonne : il existe $\lambda_1,\dots,\lambda_n$ tels que

$$\sum_{i=1}^{n}\lambda_i f_i(x)=0$$

Or, le coefficient devant $f_n(x)$ vaut $\lambda_n=\mathrm{C}_{n-1}(u_1,\dots,u_{n-1})\neq 0$ (la puissance de -1 est égale à 1). On a donc une CL de coefficients non tous nuls qui annule $f_1,\dots,f_n$: la famille est liée. On peut donc prouver le résultat voulu (si $\mathrm{C}_n=0$ alors $(f_1,\dots,f_n)$ est liée) par récurrence :

- le résultat est immédiat si $n=1$: si $\mathrm{C}_1=0$ alors f_1 est la fonction nulle donc f_1 est une famille liée (à un élément).
- supposons le résultat vrai au rang $n-1$: si $\mathrm{C}_{n-1}=0$ alors, par HR, $f_1,\dots,f_{n-1}$ sont liées donc $f_1,\dots,f_n$ le sont aussi (une famille contenant une famille liée est liée) et, si $\mathrm{C}_{n-1}\neq 0$, on vient de prouver que la famille $(f_1,\dots,f_n)$ est tout de même liée. Dans les deux cas, l'hérédité est prouvée.

$$\boxed{\text{D'où la réciproque.}}$$

4.(a) Soit $i\in[\![1\,;n]\!]$ et soit $x\in\mathrm{X}$. Par définition, on remplace u_i par x en i-ième colonne si bien que :

$$\begin{vmatrix}f_1(u_1) & \dots & f_1(u_{i-1}) & f_1(x) & f_1(u_{i+1}) & \dots & f_1(x_n)\\ f_2(u_1) & \dots & f_2(u_{i-1}) & f_2(x) & f_2(u_{i+1}) & \dots & f_2(x_n)\\ \vdots & \vdots & \ddots & \vdots & & & \\ f_n(u_1)\dots & f_n(u_{i-1}) & f_n(x) & f_n(u_{i+1}) & \dots & f_n(x_n) & \end{vmatrix}$$

Il suffit de développer par rapport à la i-ième colonne pour conclure.

$$\boxed{\text{Il existe des }\alpha_{i,j}\in\mathbb{K}\text{ tels que : }\forall i\in[\![1\,;n]\!],\forall x\in\mathrm{X},\mathrm{F}_i(x)=\sum_{j=1}^{n}\alpha_{i,j}f_j(x)}$$

4.(b) D'après la question précédente, les $\alpha_{i,j}$ sont les cofacteurs du déterminant ci-dessus. Mais, une fois barrée la colonne i, ces cofacteurs sont les mêmes que ceux du déterminant $\mathrm{C}_n(u_1,\dots,u_n)\neq 0$. On en déduit que la matrice P est la comatrice de la matrice M associée au déterminant $\mathrm{C}_n(u_1,\dots,u_n)$. Ce déterminant étant non nul, M est inversible donc sa comatrice

également (car sa transposée est inversible, puisque la transposée de la comatrice de M est, à multiplication par un scalaire près, l'inverse de M). On en déduit donc que

$$\boxed{\text{P est inversible.}}$$

La question précédente donne l'inclusion $\text{Vect}\,(\text{F}_1,\dots,\text{F}_n) \subset \text{Vect}\,(f_1,\dots,f_n)$. De plus, si on note B le vecteur colonne contenant $\text{F}_1,\dots,\text{F}_n$ et A le vecteur colonne contenant $f_1,\dots,f_n$, la question précédente donne l'égalité : $\text{B} = \text{PA}$. Dès lors, $\text{A} = \text{P}^{-1}\text{B}$, c'est-à-dire que :

$$\boxed{\forall i \in [\![\,1\,;\,n\,]\!], \forall x \in \text{X}, f_i(x) = \sum_{j=1}^{n} \left(\text{P}^{-1}\right) i,j\text{F}_j(x)}$$

ce qui permet de prouver l'inclusion réciproque, d'où l'égalité.

$$\boxed{\text{Vect}\,(\text{F}_1,\dots,\text{F}_n) = \text{Vect}\,(f_1,\dots,f_n)}$$

Exercice 4

1 Si $i > j$ alors $\text{P}_{i,j} = 0$ car i ne divise par j si bien que P est triangulaire supérieure. De plus, les termes diagonaux sont tous égaux à 1 car i divise i pour tout i. Dès lors,

$$\boxed{\det(\text{P}) = 1}$$

2 Soit $(i,j) \in [\![\,1\,;\,n\,]\!]^2$. Par définition d'un produit matriciel :

$$\begin{aligned}\text{M}_{i,j} &= \sum_{k=1}^{n} \left(\text{P}^{\top}\right)_{i,k} (\Delta\text{P})_{k,j} \\ &= \sum_{k=1}^{n} \text{P}_{k,i} \sum_{\ell=1}^{n} \Delta_{k,\ell}\text{P}_{\ell,j}\end{aligned}$$

Or, par définition, Δ est diagonale donc $\Delta_{k,\ell} = 0$ si $k \neq \ell$ et vaut $f(k)$ si $k = \ell$ si bien que :

$$\text{M}_{i,j} = \sum_{k=1}^{n} \text{P}_{k,i} f(k) \text{P}_{k,j}$$

Par définition de P, il ne reste que les termes pour lesquels k divise i et j donc :

$$\boxed{\text{M}_{i,j} = \sum_{k \text{ divise } i \text{ et } j} f(k)}$$

3 Notons $\text{S} = \sum_{d|n} f(d)$, et on cherche donc à prouver que $\text{S} = g(n)$. Remplaçons, pour tout d divisant n, $f(d)$ par sa valeur, ce qui donne :

$$\text{S} = \sum_{d|n} \sum_{c|d} \mu\left(\frac{d}{c}\right) g\,(c)$$

Intervertissons ces deux sommes (faites le geste) : lorsque d parcourt les diviseurs de n et c les diviseurs de d, alors c parcourt les diviseurs de n (par transitivité) et d les multiples de c divisant n :

$$\text{S} = \sum_{c|n} \sum_{d \text{ multiple de } c \text{ divisant } n} \mu\left(\frac{d}{c}\right) g\,(c)$$

Dans la deuxième somme, posons $k = d/c$, $d = kc$ (ce qui est possible car d est un multiple de c). Or, on sait que d divise n donc il existe p tel que $dp = n$ donc $kcp = n$ et donc $kp = n/c$ donc k divise n/c et, réciproquement, si k divise n/c alors kc divise n. En d'autres termes, lorsque $d = kc$ parcourt les multiples de c divisant n, alors k parcourt les diviseurs de n/c si bien qu'on a finalement :

$$\begin{aligned}\text{S} &= \sum_{c|n} \sum_{k|n/c} \mu\,(k)\, g\,(c) \\ &= \sum_{c|n} g(c) \sum_{k|n/c} \mu(k)\end{aligned}$$

Si $c \neq n$, la deuxième somme est nulle car $n/c \neq 1$, d'après la propriété rappelée dans l'énoncé, et donc il ne reste que le terme pour $c = n$, et la deuxième somme vaut alors $\mu(1) = 1$, si bien que $\mathrm{S} = 1$.

$$\boxed{\text{On a bien } g(n) = \sum_{d|n}^{f}(d)}$$

4 Rappelons (cf. chapitre 6) qu'un entier divise i et j si et seulement s'il divise leur PGCD. Dès lors, pour tous i et j,

$$\mathrm{M}_{i,j} = \sum_{k|i\,\wedge\,j} f(k)$$

Prenons donc la fonction f définie par :

$$\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g\,(d)$$

On a donc, pour cette valeur de f,

$$\mathrm{M}_{i,j} = \sum_{k|i\,\wedge\,j} f(k) = g(i \wedge j)$$

d'après la question précédente, et donc on a bien $\mathrm{M} = \mathrm{A}_g$. Par conséquent, $\det(\mathrm{M}) = \det(\mathrm{A}_g)$. Or, le déterminant étant multiplicatif, $\det(\mathrm{M}) = \det(\mathrm{P}^\top) \times \det(\Delta) \times \det(\mathrm{P})$. De plus, P est de déterminant 1 donc sa transposée également, si bien que $\det(\mathrm{M}) = \det(\Delta)$. Enfin, Δ étant diagonale, son déterminant est égal au produit de ses coefficients diagonaux, si bien que

$$\boxed{\det(\mathrm{A}_g) = \prod_{k=1}^{n} f(k) \text{ où, pour tout } n,\ f(n) = \sum_{j|n} \mu\left(\frac{n}{d}\right) g(d)}$$

5.(a) Notons U l'union de droite. Par définition, U est contenue dans $[\![\,1\,;\,n\,]\!]$. De plus, elle est disjointe car un même k ne peut pas avoir deux PGCD différents avec n. Enfin, pour tout $k \in [\![\,1\,;\,n\,]\!]$, si on note $d = k \wedge n$, alors d divise n donc k est dans l'ensemble $\{k \in [\![\,1\,;\,n\,]\!] \,|\, k \wedge n = d\}$, si bien que $[\![\,1\,;\,n\,]\!]$ est aussi inclus dans U.

$$\boxed{[\![\,1\,;\,n\,]\!] = \textstyle\bigcup_{d|n}\{k \in [\![\,1\,;\,n\,]\!] \,|\, k \wedge n = d\} \text{ et cette union est disjointe.}}$$

5.(d) Le sens direct découle du chapitre 6 : si $k \wedge n = d$ alors d divise k et k/d et n/d sont premiers entre eux. Réciproquement, supposons que d divise k et k/d et n/d soient premiers entre eux. Soit $m = k \wedge n$. Alors d divise m (le PGCD est divisible par tous les diviseurs communs) donc il existe a tel que $m = ad$. Puisque k/m et n/m sont des entiers, il en découle que a divise n/d et k/d qui sont premiers entre eux donc $a = 1$ donc $m = d$.

$$\boxed{k \wedge n = d \text{ si et seulement si } d \text{ divise } k \text{ et } (k/d) \wedge (n/d) = 1.}$$

5.(c) D'après la question 5.(a), l'union étant disjointe, la somme des cardinaux est le cardinal de l'union :

$$n = \sum_{d|n} \mathrm{Card}\,\{k \in [\![\,1\,;\,n\,]\!] \,|\, k \wedge n = d\}$$

Or, d'après la question précédente, le cardinal de $\{k \in [\![\,1\,;\,n\,]\!] \,|\, k \wedge n = d\}$ est égal au nombre d'entiers k multiples de d tels que k/d soit premier avec n/d. En d'autres termes, ce cardinal est égal au nombre d'entiers de la forme $i \times d$ avec i premier avec n/d : il y a donc autant d'éléments dans cet ensemble que d'entiers premiers avec n/d. Finalement, le cardinal de cet ensemble est égal au nombre d'entiers premiers avec n/d, c'est-à-dire à $\varphi(n/d)$, c'est-à-dire que :

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$$

La conclusion découle de la formule d'inversion de Möbius (la réciproque de la question 3, vraie d'après l'exercice 25 du chapitre 17).

$$\boxed{\forall n \in \mathbb{N}^*, \sum_{d|n}^{\mu} \left(\frac{n}{d}\right) \times d = \varphi(n)}$$

5.(d) Il s'agit d'appliquer la question 4 avec $g : n \mapsto n$. La fonction f est alors définie par :

$$\forall n \in \mathbb{N}^*, f(n) = \sum_{j|n} \mu\left(\frac{n}{d}\right) \times d$$

donc f est l'indicatrice d'Euler d'après la question précédente. D'après la question 4 :

$$\boxed{\det((i \wedge j)_{i,j}) = \varphi(1) \times \cdots \times \varphi(n)}$$

Puisque l'indicatrice d'Euler ne s'annule pas, la matrice associée est inversible.

Problème

Partie A. La propriété fondamentale du résultant

1 S'ils ne sont pas premiers entre eux, alors il existe R un polynôme non constant qui divise à la fois P et Q, c'est-à-dire qu'il existe P_1 et Q_1 de degrés inférieurs ou égaux respectivement à $n-1$ et $m-1$ tels que $P = RP_1$ et $Q = RQ_1$. Il suffit alors de prendre $A = Q_1$ et $B = P_1$ si bien que $AP = BQ = RP_1Q_1$, d'où la première implication.

Réciproquement, supposons qu'il existe A et B comme dans l'énoncé et que P et Q soient premiers entre eux. P divise BQ donc, d'après le théorème de Gauß, P divise B ce qui est absurde car $\deg(P) > \deg(B)$ et B est non nul. Donc P et Q ne sont pas premiers entre eux.

On a bien l'équivalence voulue.

2 On sait que $\mathbb{K}_p[X]$ est de dimension $p+1$ et que la dimension de l'espace vectoriel produit $F \times G$ est égale à la somme des dimensions de F et G. On obtient ainsi que :

Ces deux espaces sont de dimension $n+m$.

3 Il faut faire attention qu'**un** élément de l'espace de départ est un couple de **deux** éléments. Montrons que f est linéaire. Pour tous (P_1, Q_1) et (P_2, Q_2) dans $\mathbb{K}_{m-1}[X] \times K_{n-1}[X]$ et tous $\lambda, \mu \in \mathbb{K}$ on a :

$$\begin{aligned} f\left((\lambda\,(P_1, Q_1) + \mu\,(P_2, Q_2)\right) &= f\left(\lambda P_1 + \mu P_2, \lambda Q_1 + \mu Q_2\right) \\ &= \left(\lambda P_1 + \mu P_2\right) P + \left(\lambda Q_1 + \mu Q_2\right) Q \\ &= \lambda P_1 P + \lambda Q_1 Q + \mu P_2 P + \mu Q_2 Q \\ &= \lambda f(P_1, Q_1) + \mu f(P_2, Q_2) \end{aligned}$$

et f est, en conclusion, bien linéaire. Une base de l'espace d'arrivée est la base canonique $(1, X, \ldots, X^{n+m-1})$. Montrons que la famille $(1,0), \ldots, (X^{m-1}, 0), (0,1), \ldots, (0, X^{n-1})$ est une base de l'espace de départ. Comme cette famille est de cardinal $n+m$, c'est-à-dire la dimension de l'espace, il suffit de montrer que c'est une famille génératrice (juste pour changer : on peut aussi montrer facilement qu'elle est libre). Soient

$$C = \sum_{i=0}^{m-1} c_i X^i \in \mathbb{K}_{m-1}[X] \qquad \text{et} \qquad D = \sum_{i=0}^{n-1} d_i X^i \in \mathbb{K}_{n-1}[X]$$

Dès lors

$$(C, D) = (C, 0) + (0, D) = \sum_{i=0}^{m-1} c_i (X^i, 0) + \sum_{i=0}^{n-1} d_i (0, X^i)$$

Cette famille est bien génératrice et donc c'est une base. Vérifions que la matrice de f dans ces deux bases et la transposée de la matrice résultante. $f(1,0) = P = a_0 + a_1 X + \cdots + a_n X^n$ et donc la première colonne de cette matrice est le vecteur

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

D

e même$f(\mathrm{X},0) = \mathrm{XP} = a_0\mathrm{X} + a_1\mathrm{X}^2 + \cdots + a_n\mathrm{X}^{n+1}$ et donc la deuxième colonne de cette matrice est le vecteur

$$\begin{pmatrix} 0 \\ a_0 \\ a_1 \\ \vdots \\ a_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

De même pour chaque élément $(\mathrm{X}^i, 0)$: la i-ème colonne de la matrice associée à f est le vecteur avec ses $i-1$ premières coordonnées nulles, les $n+1$ suivantes valant $a_0, \ldots, a_n$ et les suivantes aussi nulles. On a ainsi les n premières colonnes de cette matrice. Pour la $n+1$ et les suivantes, il faut regarder $f(0, \mathrm{X}^i)$ et cela marche exactement de la même façon et on trouve le résultat demandé.

C'est bon.

4 D'après la première question, P et Q sont premiers entre eux si et seulement si f est injective, donc si et seulement si le déterminant de la matrice associée à f est non nul. Or, le déterminant d'une matrice étant égal à celui de sa transposée, et le résultant étant égal au déterminant de la transposée de la matrice de f par la question précédente, on en déduit le résultat voulu.

P et Q sont premiers entre eux si et seulement si leur résultat est non nul.

5 Le résultant recherché est le déterminant de la matrice suivante

$$\begin{pmatrix} a_0\lambda^n & a_1\lambda^{n-1} & \cdots & a_{n-1}\lambda & a_n & 0 & \cdots & 0 \\ 0 & a_0\lambda^n & \ddots & & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0\lambda^n & a_1\lambda^{n-1} & a_2\lambda^{n-2} & \cdots & a_n \\ b_0\lambda^m & b_1\lambda^{m-1} & \cdots & b_{m-1}\lambda & b_m & 0 & \cdots & 0 \\ 0 & b_0\lambda^m & \ddots & & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & b_0\lambda^m & b_1\lambda^{m-1} & \cdots & b_{m-1}\lambda & b_m \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \} m \\ \\ \\ \\ \} n \end{matrix}$$

$$\underbrace{\qquad\qquad}_{n} \quad \underbrace{\qquad\qquad}_{m}$$

Multiplions la colonne C_j par λ^j pour j allant de 1 à $m+n$ (ce qui divise le déterminant par λ^j). On peut alors mettre λ^{n+i} en facteur sur la ligne L_i pour les m premières lignes ($i \in [\![1\,;\, m]\!]$) et λ^i pour les n suivantes ($i \in [\![m+1\,;\, m+n]\!]$). Par n-linéarité du déterminant, on obtient :

$$\mathrm{Res}_{\mathbb{K}}\left(\lambda^n \mathrm{P}\left(\frac{\mathrm{X}}{\lambda}\right), \lambda^m \mathrm{Q}\left(\frac{\mathrm{X}}{\lambda}\right)\right) = \lambda^{\alpha} \mathrm{Res}_{\mathbb{K}}(\mathrm{P}, \mathrm{Q})$$

où
$$\begin{aligned}\alpha &= \sum_{i=1}^{m}(n+i) + \sum_{i=m+1}^{n+m} i - \sum_{j=1}^{n+m} j \\ &= nm + \frac{m(m+1)}{2} - \sum_{j=1}^{m} i \\ &= nm + \frac{m(m+1)}{2} - \frac{m(m+1)}{2} \\ &= nm\end{aligned}$$

En conclusion
$$\boxed{\mathrm{Res}_{\mathbb{K}}\left(\lambda^n \mathrm{P}\left(\frac{\mathrm{X}}{\lambda}\right), \lambda^m \mathrm{Q}\left(\frac{\mathrm{X}}{\lambda}\right)\right) = \lambda^{nm}\mathrm{Res}_{\mathbb{K}}(\mathrm{P},\mathrm{Q})}$$

6.(a) Tout d'abord, le discriminant de P est nul si et seulement si le résultant de P et P′ est nul. D'après la question 1, le discriminant de P est nul si et seulement si P et P′ ne sont pas premiers entre eux, c'est-à-dire s'ils ont une racine complexe commune. Or, P et P′ ont une racine commune si et seulement si c'est une racine multiple. Le résultat en découle :

P a une racine multiple si et seulement si son discriminant est nul.

6.(b) $\mathrm{P} = a\mathrm{X}^2 + b\mathrm{X} + c$ et $\mathrm{P}' = 2a\mathrm{X} + b$ donc
$$\mathrm{Res}(\mathrm{P},\mathrm{P}') = \begin{vmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{vmatrix} = 4a^2c - ab^2$$
et en multipliant par $\dfrac{(-1)^{2\times 3/2}}{a} = -\dfrac{1}{a}$ on obtient le résultat voulu.

P a une racine multiple si et seulement si son discriminant est nul.

6.(c) $\mathrm{P} = \mathrm{X}^3 + p\mathrm{X} + q$ et $\mathrm{P}' = 3\mathrm{X}^2 + p$ ce qui donne
$$\mathrm{Res}(\mathrm{P},\mathrm{P}') = \begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix} = 27q^2 + 4p^3$$
en développant, par exemple, suivant la première colonne. Comme le polynôme est unitaire et $n = 3$, le discriminant est lui aussi égal à $27q^2 + 4p^3$.

Le discriminant de $\mathrm{X}^3 + p\mathrm{X} + q$ est égal à $27q^2 + 4p^3$.

> On en déduit que ce polynôme a une racine multiple si et seulement si $27q^2 + 4p^3 = 0$. On avait prouvé ce résultat d'une autre façon dans l'exercice 74 du chapitre 19.

Partie B. Nombres algébriques

1 En développant on obtient
$$\mathrm{P} = \mathrm{X}^3 - 3\mathrm{X}^2\mathrm{Y} + 3\mathrm{X}\mathrm{Y}^2 - \mathrm{Y}^3 + 2\mathrm{X}^2\mathrm{Y}^2 = (\mathrm{X}^3) + (-3\mathrm{X}^2)\mathrm{Y} + (3\mathrm{X} + 2\mathrm{X}^2)\mathrm{Y}^2 + (-1)\mathrm{Y}^3$$

2 De même que dans la question précédente on peut mettre les deux polynômes sous la forme $(\mathrm{X}^3+1) + (\mathrm{X}^2)\mathrm{Y} + (\mathrm{X})\mathrm{Y}^2$ et $1 + (\mathrm{X})\mathrm{Y}$. Le résultant de ces deux polynômes, en tant que polynômes en Y à coefficients dans K est alors
$$\boxed{\begin{vmatrix} 1+\mathrm{X}^3 & \mathrm{X}^2 & \mathrm{X} \\ 1 & \mathrm{X} & 0 \\ 0 & 1 & \mathrm{X} \end{vmatrix} = \mathrm{X}^2(1+\mathrm{X}^3) + \mathrm{X} - \mathrm{X}^3 = \mathrm{X} + \mathrm{X}^2 - \mathrm{X}^3 + \mathrm{X}^5}$$

3 Le résultant demandé est un déterminant d'une matrice à coefficients dans $\mathbb{Z}[X]$ et comme le déterminant est polynomial en les coefficients, son déterminant est aussi à valeurs dans $\mathbb{Z}[X]$. Montrons que c'est un polynôme annulateur de z_1+z_2. Il faut montrer que la fonction polynomiale associée (en x) est nulle en z_1+z_2. Or, en évaluant cette fonction en z_1+z_2, on obtient le résultant des deux polynômes $P(z_1+z_2-Y)$ et $P_2(Y)$ qui s'annulent tous les deux en z_2 : les deux polynômes ont une racine commune, ils ne sont pas premiers entre eux et d'après la partie précédente, leur résultant est nul.

Ce polynôme est un élément de $\mathbb{Z}[X]$ qui annule z_1+z_2.

4 $P_1=X^2-2$ et $P_2=X^2-7$ sont respectivement annulateurs de $\sqrt{2}$ et $\sqrt{7}$. D'après la question précédente, $\sqrt{2}+\sqrt{7}$ est annulateur du polynôme $Q=\mathrm{Res}_K(P_1(X-Y),P_2(Y))$. On a évidemment $P_2(Y)=Y^2-7$ et $P_1(X-Y)=X^2-2XY+Y^2-2=(X^2-2)+(-2$
Par conséquent

$$Q=\begin{vmatrix} -7 & 0 & 1 & 0\\ 0 & -7 & 0 & 1\\ X^2-2 & -2X & 1 & 0\\ 0 & X^2-2 & -2X & 1\end{vmatrix}$$

Calculons ce déterminant. Développons par rapport à la dernière colonne :

$$Q=+1\times\begin{vmatrix} -7 & 0 & 1\\ X^2-2 & -2X & 1\\ 0 & X^2-2 & -2X\end{vmatrix}+1\times\begin{vmatrix} -7 & 0 & 1\\ 0 & -7 & 0\\ X^2-2 & -2X & 1\end{vmatrix}$$

$$=-28X^2+(X^2-2)^2+7(X^2-2)+49+7(X^2-2)$$

En conclusion $\boxed{X^4-18X^2+25 \text{ est annulateur de } \sqrt{2}+\sqrt{7}.}$

5 Il faut montrer que c'est un sous-corps de $\mathbb{R}$.

- 0 et 1 sont évidemment algébriques car racines de X et $X-1$.
- L'ensemble des nombres algébriques est stable par somme d'après la question 3.
- Montrons qu'il est stable par produit. On reprend les notations de la question 2.(c) et on cherche un polynôme à coefficients entiers annulant z_1z_2. Bien sûr, si z_1 ou z_2 est nul, $z_1z_2=0$ est algébrique. On supposera donc z_1 et z_2 non nuls. Il faut penser à l'analogue du polynôme de la question 3, version multiplication : l'analogue de $X-Y$ est $\dfrac{X}{Y}$. On a envie de regarder le résultant des polynômes $P_1\left(\dfrac{X}{Y}\right)$ et $P_2(Y)$. L'ennui, c'est que le premier n'est pas un polynôme en Y. On règle cela en multipliant par Y^n où n est le degré de P_1 : $Y^nP_1\left(\dfrac{X}{Y}\right)$ est bien un polynôme en Y à coefficients dans $\mathbb{Z}[X]$, et si on évalue en $X=z_1z_2$, le polynôme $Y^nP_1\left(\dfrac{z_1z_2}{Y}\right)$ s'annule en z_2 et donc lui et $P_2(Y)$ ont z_2 en racine commune : leur résultant est nul, ce qu'on voulait démontrer.
- Une fois qu'on a fait la multiplication, le passage à l'inverse n'est pas très compliqué : si z_1 est un nombre algébrique non nul annulant P_1, on voit avec le même raisonnement que $\dfrac{1}{z_1}$ est racine du résultant des deux polynômes en Y $P_1(Y)$ et $P_1\left(XY^2\right)$, puisque si on évalue en $X=\dfrac{1}{z_1}$ alors les deux polynômes en Y admettent z_1 comme racine commune.

En conclusion L'ensemble des nombres algébriques est un corps.