DS 6 de mathématiques

1 Entiers algébriques

1.1 Généralités

1. Les polynômes X^3-2 et X^6-1 annulent respectivement $\sqrt[3]{2}$ et $e^{i\pi/3}$ dont ces nombres sont des entiers algébriques.
Le polynôme X^3-2 est irréductible dans $\mathbb{Q}[X]$. En effet, comme il est de degré 3, il aurait sinon une racine rationnelle, nécessairement $\sqrt[3]{2}$. Or, ce nombre n'est pas rationnel. Si $\sqrt[3]{2}$ s'écrivait $\frac{a}{b}$ avec $a, b \in \mathbb{N}^*$, on aurait $2b^3 = a^3$ et donc $1 + 3\nu_2(b) = 3\nu_2(a)$ (où ν_2 désigne la valuation dyadique), ce qui est absurde. Ainsi, X^3-2 est unitaire irréductible et divisible par le polynôme minimal de $\sqrt[3]{2}$: il est donc égal à ce polynôme minimal.
On peut encore écrire $e^{i\pi/3} = -j^2$ et on sait que $1 + j + j^2 = 0$. Donc, $e^{i\pi/3}$ est aussi racine de $X^2 - X + 1$. Ce polynôme est irréductible sur $\mathbb{Q}[X]$ car il n'a pas de racine réelle ; c'est le polynôme minimal de $e^{i\pi/3}$.

2. Notons $\alpha = \sqrt{2} + i$. On a $(\alpha - \sqrt{2})^2 + 1 = 0$, donc $\alpha^2 - 2\sqrt{2}\alpha + 3 = 0$. Ainsi, $\alpha^2 + 3 = 2\sqrt{2}\alpha$, donc en prenant le carré :

$$\alpha^4 - 2\alpha^2 + 9 = 0.$$

Ainsi $\sqrt{2}+i$ est un entier algébrique et son polynôme minimal divise X^4-2X^2+9. On factorise ce polynôme dans $\mathbb{R}[X]$. Comme $\sqrt{2}-i$ est aussi racine de X^4-2X^2+9, on peut le factoriser par $(X-\sqrt{2}-i)(X-\sqrt{2}+i) = X^2-2\sqrt{2}X+|\sqrt{2}+i|^2 = X^2-2\sqrt{2}X+3$. On peut deviner qu'on a la factorisation :

$$X^4 - 2X^2 + 9 = (X^2 - 2\sqrt{2}X + 3)(X^2 + 2\sqrt{2}X + 3),$$

ce qu'on vérifie en développant. Les deux facteurs de droite sont de discriminant strictement négatif, donc sont irréductibles dans $\mathbb{R}[X]$. Ainsi, ce sont les seuls diviseurs de degré $d \in [\![1, 3]\!]$ de $X^4 - 2X^2 + 9$ dans $\mathbb{R}[X]$. Comme aucun n'est dans $\mathbb{Q}[X]$ ($\sqrt{2}$ étant irrationnel), $X^4 - 2X^2 + 9$ est irréductible dans $\mathbb{Q}[X]$. Donc, c'est le polynôme minimal de α, par le même raisonnement que pour $\sqrt[3]{2}$.

3. Si $P_\alpha \in \mathbb{Z}[X]$, alors α est annulé par un polynôme unitaire dans $\mathbb{Z}[X]$, et donc α est un entier algébrique.
Pour l'autre sens, notons Q un polynôme unitaire de $\mathbb{Z}[X]$ annulant α. On sait que P_α et Q sont dans $\mathbb{Q}[X]$ et que $P_\alpha \mid Q$. On écrit $Q = RP_\alpha$, avec $R \in \mathbb{Q}[X]$. On peut multiplier P_α et R par des entiers N_P et N_R pour obtenir des polynômes à coefficients entiers, de contenu égal à 1 (quitte à diviser par le pgcd des coefficients des nouveaux polynômes). On a alors : $N_P N_R Q = (N_P P_\alpha)(N_R R)$.
En prenant le contenu dans cette égalité, on a $c(N_P N_R Q) = 1$; mais comme $Q \in \mathbb{Z}[X]$, tous les coefficients de $N_P N_R Q$ sont divisibles par $N_P N_R$; nécessairement $N_P = 1$ et $N_R = 1$. Et donc $P_\alpha \in \mathbb{Z}[X]$.

4. On a $|\omega| = \dfrac{\sqrt{3^2+4^2}}{5} = 1$, donc $\omega \in \mathbb{U}$. Si ω était une racine de l'unité, ω serait annulé par un polynôme de la forme $X^n - 1$, donc serait un entier algébrique, dont son polynôme minimal serait à coefficients entiers, par la question précédente.
Or, $(5\omega - 3)^2 + 16 = 0$, donc ω annule $25X^2 - 30X + 25$, donc aussi $X^2 - \dfrac{6}{5}X + 1$. Ce polynôme est le polynôme minimal de ω : il est unitaire, de degré 2, à coefficients rationnels et $\omega \notin \mathbb{Q}$. Comme il n'est pas à coefficients entiers, ω n'est pas un entier algébrique, et donc pas une racine de l'unité.

5. Pour tout $k \in [\![0, d-1]\!]$, on a
$$a_k = (-1)^{d-k} \sum_{1 \leq i_1 < \cdots < i_{d-k} \leq d} \alpha_{i_1} \dots \alpha_{i_{d-k}}.$$

6. Par la formule du binôme de Newton,
$$0 = (1 + (-1))^d = \sum_{\substack{0 \leq k \leq d \\ k \equiv 0\ [2]}} \binom{d}{k} - \sum_{\substack{0 \leq k \leq d \\ k \equiv 1\ [2]}} \binom{d}{k},$$
de sorte que $\displaystyle\sum_{\substack{0 \leq k \leq d \\ k \equiv 0\ [2]}} \binom{d}{k} = \sum_{\substack{0 \leq k \leq d \\ k \equiv 1\ [2]}} \binom{d}{k} = 2^{d-1}$ (car la somme des deux vaut 2^d). Si $i \in [\![0, d]\!]$, le coefficient $\binom{d}{i}$ apparait dans une des deux sommes (de termes positifs). Donc, on a en particulier $\binom{d}{i} \leq 2^{d-1}$.

7. Soit $k \in [\![0, d-1]\!]$. D'après la formule de la question 6 et l'inégalité triangulaire, on a
$$|a_k| \leq \sum_{1 \leq i_1 < \cdots < i_{d-k} \leq d} |\alpha_{i_1}| \dots |\alpha_{i_{d-k}}|.$$
Chaque terme $|\alpha_{i_1}| \dots |\alpha_{i_{d-k}}|$ peut être majoré par $\displaystyle\prod_{i=1}^{d} \max(1, |a_i|) = \mathcal{M}(P)$. Comme il y a $\binom{d}{d-k} = \binom{d}{k}$ termes dans la somme, on en déduit $|a_k| \leq \binom{d}{k} \mathcal{M}(P) \leq 2^{d-1} \mathcal{M}(P)$, par la question précédente.
Cette inégalité est vraie pour tout $k \in [\![0, d-1]\!]$ et aussi pour $k = d$ car $a_d = 1$ et que $\mathcal{M}(P) \geq 1$; on en déduit que $h(P) \leq 2^{d-1} \mathcal{M}(P)$, ce qui conclut.

8. Soit $P \in \mathcal{P}_{n,A}$. Notons d son degré. Si $d = 0$, alors $P = 1$ (un seul polynôme). Si $d \geq 1$, alors $h(P) \leq 2^{d-1} \mathcal{M}(P) \leq 2^{n-1} A$. Donc, tous les coefficients de P sont en valeur absolue majorés par $2^{n-1} A$. Comme ces coefficients sont entiers, il n'y a qu'un nombre fini de possibilités.
Donc, $\mathcal{P}_{n,A}$ est fini.

1.2 Théorème de Kronecker

9. Montrons déjà l'unicité. Si (F,G) et (F',G') conviennent, on a $(F-F')(X^2) = X(G'-G)(X^2)$. Le membre de gauche ne fait intervenir que des puissances paires de X, celui de droite que des puissances impaires. Donc, les deux sont nuls. Ainsi, pour tout $x \in \mathbb{Z}$, $(F-F')(x^2) = x(G'-G)(x^2) = 0$. En particulier, $F-F'$ et $G-G'$ s'annule en une infinité de valeurs ; donc ils sont nuls : $F = F'$ et $G = G'$.
Pour l'existence, on écrit $P = \sum_{k=0}^{d} a_k X^k = \sum_{i=0}^{\lfloor d/2 \rfloor} a_{2i} X^{2i} + X \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} a_{2i+1} X^{2i}$. Ainsi, $F = \sum_{i=0}^{\lfloor d/2 \rfloor} a_{2i} X^i$ et $G = \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} a_{2i+1} X^i$ conviennent.

10. Soit $x \in \mathbb{Z}$. On a
$$F^2(x^2) - x^2 G^2(x^2) = (F(x^2) - xG(x^2))(F(x^2) + xG(x^2)) = P(x)P(-x).$$
Or $P = \prod_{i=1}^{d}(X - \alpha_i)$. Donc, pour tout $x \in \mathbb{Z}$,
$$F^2(x^2) - x^2 G^2(x^2) = \prod_{i=1}^{d}(x-\alpha_i)(-x-\alpha_i) = (-1)^d \prod_{i=1}^{d}(x^2 - \alpha_i^2).$$
Ainsi, les polynômes $F^2 - XG(X^2)$ et $(-1)^d \prod_{i=1}^{d}(X - \alpha_i^2)$ coïncident sur tous les carrés parfaits, donc sur une infinité de valeurs. Ils sont donc égaux.

11. (a) Notons $d \leq n$ le degré de α, P_α le polynôme minimal de α, $\alpha_1, \ldots, \alpha_d$ ses racines (avec p. ex. $\alpha_1 = \alpha$). Par la question 3, $P_\alpha \in \mathbb{Z}[X]$. Par la question précédente, le polynôme $\prod_{i=1}^{d}(X - \alpha_i^2)$ est à coefficients entiers (puisque F et G le sont). Comme ce polynôme est unitaire, dans $\mathbb{Z}[X]$ et annule α^2, α^2 est un entier algébrique. Comme ce polynôme est de degré d et qu'il est divisible par le polynôme minimal de α^2, le degré de α^2 est inférieur à d.

    (b) On garde les notations de la réponse précédente. Comme le polynôme minimal de α^2 divise $\prod_{i=1}^{d}(X - \alpha_i^2)$, l'ensemble de ses racines est contenu dans l'ensemble $\{\alpha_1^2, \ldots, \alpha_d^2\}$. Si on suppose que tous les α_i vérifient $|\alpha_i| \leq 1$, on a aussi $|\alpha_i^2| = |\alpha_i|^2 \leq 1$ pour tout i. Et donc, les conjugués de α^2 sont tous de module ≤ 1.

12. Par récurrence immédiate, en utilisant les deux questions précédentes, on sait que pour tout $k \in \mathbb{N}^*$, α^{2^k} est un entier algébrique de degré inférieur à d (le degré de α) et dont tous les conjugués sont de module ≤ 1. Ainsi, $\mathcal{M}(P_{\alpha_{2^k}}) = 1$ pour tout k et donc tous les $P_{\alpha_{2^k}}$ sont dans $\mathcal{P}_{d,1}$. D'après la question 9, cet ensemble est fini, donc l'ensemble des racines des polynômes de cet ensemble aussi.
Ainsi, on peut trouver $k \neq \ell \geq 1$ tels que $\alpha^{2^k} = \alpha^{2^\ell}$. On en déduit que $\alpha^{2^\ell - 2^k} = 1$, donc que α est une racine de l'unité.

1.3 Nombres de Pisot-Vijayaraghavan

13. On note f la fonction définie sur $\mathbb{R}$ par $f(x) = x^3 - x - 1$. Elle est dérivable de dérivée $f'(x) = 3x^2 - 1$. Donc, f est strictement croissante sur $]-\infty, -1/\sqrt{3}]$, strictement décroissante sur $[-1/\sqrt{3}, 1/\sqrt{3}]$ et strictement croissante sur $[1/\sqrt{3}, +\infty[$ (*Faire un tableau de variations*).
On a $f(-1/\sqrt{3}) = \dfrac{2}{3\sqrt{3}} - 1 < 0$. Donc, f ne s'annule pas sur $]-\infty, 1/\sqrt{3}]$. Et f s'annule une unique fois sur $[1/\sqrt{3}, +\infty[$: elle s'annule car $f(1/\sqrt{3}) < 0$ et $\lim\limits_{+\infty} f = +\infty$; une seule fois par stricte croissance.
De plus, comme $f(1) = -1$, la stricte croissance permet de préciser que le point d'annulation est strictement supérieur à 1.

14. Par définition, ψ est racine de $X^3 - X - 1$ donc ψ est un entier algébrique. Ce polynôme est irréductible dans $\mathbb{Q}[X]$. En effet, comme il est de degré 3, il aurait sinon une racine rationnelle $\dfrac{a}{b}$, avec $a \wedge b = 1$. On aurait $a^3 - b^2 a - b^3 = 0$. Donc, $a \mid b^3$ et $b \mid a^3$. Comme a et b sont premiers entre eux, ceci implique que $a = \pm 1$ et $b = \pm 1$. Donc, $\dfrac{a}{b} = \pm 1$; mais ni 1, ni -1 ne sont racines de $X^3 - X - 1$.
Les conjugués de ψ, autres que ψ, ne sont pas réels par la question précédente. Ce sont donc deux nombres complexes conjugués (car $X^3 - X - 1$ est à coefficients réels) z et $\overline{z}$. Par formule de Viète, on a $\psi z\overline{z} = 1$. Comme $\psi > 1$, $|z|^2 < 1$. Ainsi, $|z| = |\overline{z}| < 1$.
Donc, ψ est un nombre PV de degré 3.

15. Par les formules de Viète, on sait que

$$P = X^d - \sigma_1 X^{d-1} + \cdots + (-1)^{d-1}\sigma_{d-1} X + (-1)^d \sigma_d.$$

Pour $i \in [\![1, d]\!]$, on évalue en x_i pour obtenir la formule annoncée (puisque $P(x_i) = 0$).

16. Soit $p \geq d$. On multiplie la relation de la question précédente par x_i^{p-d} pour obtenir :

$$x_i^p - \sigma x_i^{p-1} + \cdots + (-1)^{d-1}\sigma_{d-1} x_i^{p-d+1} + (-1)^d x_i^{p-d},$$

pour tout $i \in [\![1, d]\!]$. On fait la somme de ces relations pour $i \in [\![1, d]\!]$ et on obtient :

$$S_p - \sigma_1 S_{p-1} + \cdots + (-1)^{d-1}\sigma_{d-1} S_{p-d+1} + (-1)^d \sigma_d S_{p-d} = 0.$$

17. On procède par récurrence forte sur $p \in \mathbb{N}$.

- Initialisation. On remarque simplement que $S_0 = d$.
- Hérédité. Soit $p \in \mathbb{N}^*$ tel que $S_k \in \mathbb{Z}$, pour tout $k \in [\![0, p-1]\!]$.
  Si $p \leq d - 1$, la relation admise donne :

$$S_p = \sigma_1 S_{p-1} + \cdots + (-1)^p \sigma_{p-1} S_1 + (-1)^{p+1} p\sigma_p.$$

  Les S_k apparaissant à droite sont des entiers par hypothèse de récurrence ; les σ_j sont aussi des entiers car ce sont au signe près les coefficients de P. Donc, $S_p \in \mathbb{Z}$.
  Si $p \geq d$, on utilise la relation de la question 17. On a

$$S_p = \sigma_1 S_{p-1} + \cdots + (-1)^d \sigma_{d-1} S_{p-d+1} + (-1)^{d+1} \sigma_d S_{p-d}.$$

L'argument est alors le même : les S_k à droite sont entiers par hypothèse de récurrence ; les σ_j sont aussi entiers. Donc, $S_p \in \mathbb{Z}$.
Ceci conclut la récurrence.

18. Soit α un nombre PV. On note $\alpha_1, \ldots, \alpha_d$ les racines de son polynôme minimal, avec $\alpha_1 = \alpha$. Par hypothèse, on a donc $|\alpha_k| < 1$, pour tout $k \in [\![2, d]\!]$.
Notons $S_n = \sum_{k=1}^{n} \alpha_k^n = \alpha^n + \sum_{k=2}^{d} \alpha_k^n$. Par la question précédente, $S_n \in \mathbb{Z}$. De plus, la somme $\sum_{k=2}^{d} \alpha_k^n$ tend vers 0 quand $n \to +\infty$ car tous les α_k sont de module strictement inférieur à 1.
Pour tout $n \in \mathbb{N}$, comme $S_n \in \mathbb{Z}$, on a

$$0 \leq d(\alpha^n, \mathbb{Z}) \leq |\alpha^n - S_n|,$$

donc par encadrement $d(\alpha^n, \mathbb{Z}) \to 0$, quand $n \to +\infty$.

2 Automorphismes d'algèbre de $\mathcal{L}(E)$

1. Par définition, $\mathcal{A}$ est l'intersection de $\mathrm{GL}\left(\mathcal{L}(E)\right)$ et de l'ensemble des automorphismes d'anneaux de $\mathcal{L}(E)$. Ce sont deux sous-groupes du groupe des permutations de $\mathcal{L}(E)$. Donc, $\mathcal{A}$ est un groupe, comme intersection de ces deux sous-groupes.
On n'a pas vraiment montré en cours que si A est un anneau, l'ensemble des automorphismes de cet anneau est un groupe pour la composition. Le refaire rapidement pour être sûr.

2. On vérifie successivement que :

   - $\phi_u(\mathrm{id}_E) = u^{-1} \circ \mathrm{id}_E \circ u = \mathrm{id}_E$;
   - Si $f, g \in \mathcal{L}(E)$,
   $$\phi_u(g)\phi_u(f) = (u^{-1}gu)(u^{-1}fu) = u^{-1}(gf)u = \phi_u(gf);$$
   - Si $f, g \in \mathcal{L}(E)$ et si $\alpha, \beta \in \mathbb{K}$,
   $$\phi_u(\alpha f + \beta_g) = u^{-1}(\alpha f + \beta g)u = \alpha u^{-1}fu + \beta u^{-1}gu = \alpha\phi_u(f) + \beta\phi_u(g),$$
   par distributivité dans l'anneau $\mathcal{L}(E)$.

   De plus, ϕ_u est bijective, d'inverse $\phi_{u^{-1}}$. Donc, $\phi_u \in \mathcal{A}$.

3. Comme p_k est un projecteur, on a $p_k^2 = p_k$. Comme ϕ est un morphisme d'anneaux, on a $\phi(p_k)^2 = \phi(p_k^2) = \phi(p_k)$. Par caractérisation des projecteurs, $\phi(p_k)$ est un projecteur. Comme ϕ est injective et que p_k est non nul, $\phi(p_k)$ est non nul aussi.

4. Soient $u_1, \dots, u_n$ respectivement dans $F_1, \dots, F_k$. On suppose que $u_1 + \cdots + u_n = 0$. Comme chaque u_k est dans F_k, on a l'égalité $u_k = \phi(p_k)(u_k)$, donc
   $$\sum_{k=1}^{n} \phi(p_k)(u_k) = 0.$$
   Soit $i \in [\![1, n]\!]$. En prenant l'image de la relation précédente par $\phi(p_i)$ et en utilisant la linéarité et le fait que ϕ est un morphisme d'anneaux, on a :
   $$0 = \sum_{k=1}^{n} \phi(p_i) \circ \phi(p_k)(u_k) = \sum_{k=1}^{n} \phi(p_k \circ p_i)(u_k).$$
   Or, $p_k \circ p_i = p_i$ si $k = i$ et 0 sinon. On a donc, pour tout i, $u_i = \phi(p_i^2)(u_i) = 0$. Donc, les F_k sont en somme directe.
   On en déduit que $\sum_{k=1}^{n} \dim F_k = \dim(F_1 + \cdots + F_n) \leq \dim E = n$. Comme les F_k sont non nuls, chaque $\dim F_k$ vaut au moins 1 ; donc nécessairement $\dim F_k = 1$, pour tout k.
   On a montré que les F_k étaient en somme directe et que $\sum_{k=1}^{n} \dim F_k = \dim E$. Donc, $E = \bigoplus_{k=1}^{n} F_k$.

5. Comme $(e_1, \dots, e_n)$ est une base de E, il existe une unique application linéaire $u \in \mathcal{L}(E)$ telle que $u(e_k) = f_k$ pour tout k. D'après la question précédente, $(f_1, \dots, f_n)$ est une famille libre car chaque f_k est un vecteur non nul de F_k et que les F_k sont en somme directe.
   Comme u envoie une base sur une famille libre, u est injective. Comme c'est un endomorphisme de E de dimension finie, $u \in \mathrm{GL}(E)$.

6. Soit $k \in [\![1, n]\!]$. On a $\psi(p_k) = u^{-1} \circ \phi(p_k) \circ u$. Soit $i \in [\![1, n]\!]$. Si $i = k$,
$$\psi(p_k)(e_i) = u^{-1} \circ \phi(p_k)(f_i) = u^{-1}(f_i) = e_i.$$
   Et si $i \neq k$,
$$\psi(p_k)(e_i) = u^{-1} \circ \phi(p_k)(f_i) = u^{-1}(0) = 0.$$
   Ainsi, $\psi(p_k)$ coïncide avec p_k sur la base $(e_1, \dots, e_n)$. Ils sont donc égaux.

7. Soient, pour $i, j \in [\![1, n]\!]$, des scalaires $\alpha_{i,j}$ tels que $\sum_{i,j} \alpha_{i,j} f_{i,j} = 0$.
   Soit $k \in [\![1, n]\!]$. En évaluant en e_k, on a $\sum_{i,j} \alpha_{i,j} f_{i,j}(e_k) = 0$, donc $\sum_j \alpha_{k,j} e_j = 0$. Comme $(e_1, \dots, e_n)$ est une base de E, tous les $\alpha_{k,j}$ sont nuls. Comme c'est vrai pour tout k, la famille $(f_{i,j})$ est libre.
   Comme elle est constituée de n^2 éléments et que $\dim \mathcal{L}(E) = n^2$, c'est une base de $\mathcal{L}(E)$.

8. Soient i, j distincts dans $[\![1, n]\!]$. On a $p_j \circ f_{i,j}(e_i) = p_j(e_j) = e_j$ et $p_j \circ f_{i,j}(e_k) = p_j(0) = 0$ si $k \neq i$. Donc, $p_j \circ f_{i,j}$ coïncide avec $f_{i,j}$ sur la base $(e_1, \dots, e_n)$. Comme $p_j \circ f_{i,j} = f_{i,j}$.
   De même, $f_{i,j} \circ p_i(e_i) = f_{i,j}(e_i) = e_j$ et $f_{i,j} \circ p_i(e_k) = 0$ si $k \neq i$. Donc, $f_{i,j} \circ p_i = f_{i,j}$.

9. Soient $i \neq j \in [\![1, n]\!]$. Comme $p_j \circ f_{i,j} = f_{i,j}$ et que ψ est un automorphisme d'anneaux, on a aussi $\psi(p_j) \circ \psi(f_{i,j}) = \psi(f_{i,j})$, donc $p_j \circ \psi(f_{i,j}) = \psi(f_{i,j})$.
   De même, on a $\psi(f_{i,j}) \circ p_i = \psi(f_{i,j})$. Pa la première égalité, l'image de $\psi(f_{i,j})$ est incluse dans l'image de p_j, c'est-à-dire dans D_j. Par la deuxième égalité, le noyau de $f_{i,j}$ est inclus dans celui de p_i, c'est-à-dire dans $\bigoplus_{k \neq i} D_k$. Il existe donc $\alpha_{i,j} \in \mathbb{K}$ tel que $\psi(f_{i,j})(e_i) = \alpha_{i,j} e_j$; et pour tous $k \neq i$, $\psi(f_{i,j})(e_k) = 0$. Donc, comme $(e_1, \dots, e_n)$ est une base de E, on a $\psi(f_{i,j}) = \alpha_{i,j}(f_{i,j})$. Comme $f_{i,j}$ est non nulle et que ψ est injective, on a aussi $\alpha_{i,j} \neq 0$.

   On constate que $f_{j,k} \circ f_{i,j} = f_{i,k}$ si $i, j, k \in [\![1, n]\!]$ (calculs similaires à la question 8). En prenant l'image par ψ, on a aussi $\alpha_{j,k}\alpha_{i,j} f_{j,k} \circ f_{i,j} = \alpha_{i,k} f_{i,k}$. Comme $f_{i,k}$ est non nul, on en déduit que $\alpha_{i,j}\alpha_{j,k} = \alpha_{i,k}$.

10. En notant $\mathbf{d}^{-1} = (d_1^{-1}, \dots, d_n^{-1})$, on a $v_{\mathbf{d}} \circ v_{\mathbf{d}^{-1}}$ sur la base $(e_1, \dots, e_n)$, donc sur E. Ainsi, $v_{\mathbf{d}} \in \mathrm{GL}(E)$.
    Calculons maintenant l'image des p_i et des $f_{i,j}$ par un $\phi_{v_{\mathbf{d}}}$. Soit $i \in [\![1, n]\!]$. On a
$$\phi_{v_{\mathbf{d}}}(p_i) = v_{\mathbf{d}^{-1}} \circ p_i \circ v_{\mathbf{d}}.$$
    En évaluant en e_k, on trouve que $\phi_{\mathbf{v}_d}(p_i)(e_k) = e_k$ si $i = k$ et 0 sinon, donc $\phi_{\mathbf{v}_d}(p_i) = p_i$.
    Soient $i \neq j \in [\![1, n]\!]$. On a
$$\phi_{v_{\mathbf{d}}}(f_{i,j}) = v_{\mathbf{d}^{-1}} \circ f_{i,j} \circ v_{\mathbf{d}}.$$

En évaluant en e_k, on trouve que $\phi_{v_{\mathbf{d}}}(f_{i,j})(e_k) = 0$ si $k \neq i$ et $\phi_{v_{\mathbf{d}}}(f_{i,j})(e_i) = \dfrac{d_i}{d_j} e_j$. Ainsi, $\phi_{v_{\mathbf{d}}}(f_{i,j}) = \dfrac{d_i}{d_j} f_{i,j}$. On aura donc $\psi = \phi_{v_{\mathbf{d}}}$ ssi $\alpha_{i,j} = \dfrac{d_i}{d_j}$, pour tous $i \neq j$.
On pose $d_i = \alpha_{i,1}$ pour tout $i \in [\![1, n]\!]$. Alors, pour tous $i, j \in [\![1, n]\!]$, $\alpha_{i,j} = \alpha_{i,1}\alpha_{1,j} = \alpha_{i,1}\alpha_{j,1}^{-1} = \dfrac{d_i}{d_j}$. On a utilisé que $\alpha_{j,1}\alpha_{1,j} = \alpha_{j,j} = 1$, la dernière égalité venant de ce que $f_{j,j} = p_j$ et que $\psi(p_j) = p_j$. Ainsi, $\mathbf{d}$ convient.

11. On en déduit que $\phi = (\phi_u)^{-1} \circ \phi_{v_{\mathbf{d}}} = \phi_{u^{-1} \circ v_{\mathbf{d}}}$, par un calcul immédiat.
Ainsi, tout $\phi \in \mathcal{A}$ s'écrit ϕ_w, pour un $w \in \mathrm{GL}(E)$. La réciproque a été montrée à la question 2 ; donc $\mathcal{A} = \big\{\phi_w, w \in \mathrm{GL}(E)\big\}$.

3 Corps engendré par un nombre transcendant

1. Comme α est transcendant, $Q(\alpha) \neq 0$ si $Q \in \mathbb{Q}[X] \setminus \{0\}$. Donc $\mathbb{Q}(\alpha)$ est bien défini (pas de division par 0). Par définition, un élément β de $\mathbb{Q}(\alpha)$ peut s'écrire $\dfrac{P(\alpha)}{Q(\alpha)}$, avec $P, Q \in \mathbb{Q}[X]$, Q non nul. On peut écrire $P = P_1(P \wedge Q)$ et $Q = Q_1(P \wedge Q)$, et alors P_1 et Q_1 sont premiers entre eux. De plus, $\beta = \dfrac{P_1(\alpha)(P \wedge Q)(\alpha)}{Q_1(\alpha)(P \wedge Q)(\alpha)} = \dfrac{P_1(\alpha)}{Q_1(\alpha)}$. Donc, β peut bien s'écrire sous la forme annoncée.

2. Soient $z, w \in \mathbb{Q}(\alpha)$, soient $\lambda, \mu \in \mathbb{Q}$. On peut écrire $z = \dfrac{P(\alpha)}{Q(\alpha)}$ et $w = \dfrac{R(\alpha)}{S(\alpha)}$, avec $P, Q, R, S \in \mathbb{Q}[X]$, $R, S \neq 0$. Alors,

   - $\lambda z + \mu w = \dfrac{\lambda P(\alpha)S(\alpha) + \mu R(\alpha)Q(\alpha)}{Q(\alpha)S(\alpha)} = \dfrac{(\lambda PS + \mu RQ)(\alpha)}{(QS)(\alpha)} \in \mathbb{Q}(\alpha)$;
   - $zw = \dfrac{(PR)(\alpha)}{(QS)(\alpha)} \in \mathbb{Q}(\alpha)$;
   - si $z \neq 0$, $P \neq 0$ (car α transcendant) et $\dfrac{1}{z} = \dfrac{Q(\alpha)}{P(\alpha)}$
   - $1 \in \mathbb{Q}(\alpha)$ car $1 = \dfrac{P(\alpha)}{Q(\alpha)}$, en prenant pour P et Q les polynômes constants à 1.

   Ceci montre que $\mathbb{Q}(\alpha)$ est un sous-espace vectoriel de $\mathbb{C}$ (vu comme $\mathbb{Q}$-ev) et un sous-corps de $\mathbb{C}$ (la stabilité par somme est un cas particulier de la linéarité).

3. Soient $q_1, \ldots, q_r \in \mathbb{Q}$ deux à deux distincts, $\lambda_1, \ldots, \lambda_r \in \mathbb{Q}$, $n \in \mathbb{N}$ et $\mu_0, \ldots, \mu_n \in \mathbb{Q}$ tels que
$$\sum_{k=1}^{r} \lambda_k \beta_{q_k} + \sum_{i=0}^{n} \mu_i \alpha^i = 0.$$
On doit montrer que les λ_k et mes μ_i sont tous nuls.
On multiplie la relation par le produit des $(\alpha - q_k)$. On obtient :
$$\sum_{k=1}^{r} \lambda_k \prod_{\ell \neq k} (\alpha - q_\ell) + \prod_{k=1}^{r} (\alpha - q_k) \sum_{i=0}^{n} \mu_i \alpha^i = 0.$$
Le membre de gauche est l'évaluation en α du polynôme $P = \displaystyle\sum_{k=1}^{r} \lambda_k \prod_{\ell \neq k} (X - q_\ell) + \prod_{k=1}^{r} (X - q_k) \sum_{i=0}^{n} \mu_i X^i \in \mathbb{Q}[X]$. Comme α est transcendant, on a $P = 0$, donc
$$\sum_{k=1}^{r} \lambda_k \prod_{\ell \neq k} (X - q_\ell) + \prod_{k=1}^{r} (X - q_k) \sum_{i=0}^{n} \mu_i X^i = 0.$$
On fixe $j \in [\![1, r]\!]$ et on évalue cette relation en q_j. On obtient : $\lambda_j \displaystyle\prod_{\ell \neq j} (q_j - q_\ell) = 0$,

donc $\lambda_j = 0$, pour tout j. En reportant dans la première égalité, on a donc $\sum_{i=0}^{n} \mu_i \alpha^i = 0$; donc les μ_i sont tous nuls, par transcendance de α.

4. Comme ϕ est un morphisme de corps, c'est en particulier un morphisme du groupe additif $(\mathbb{Q}(\alpha), +)$. En particulier, il préserve les itérés additifs de 1 et donc $\forall n \in \mathbb{Z}, \phi(n) = n$. Si $q \in \mathbb{Q}$, on peut l'écrire $q = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. On a $\phi(q) = \frac{\phi(a)}{\phi(b)} = \frac{a}{b} = q$.
Finalement, si $z, w \in \mathbb{Q}(\alpha)$ et si $\lambda, \mu \in \mathbb{Q}$, on a

$$\phi(\lambda z + \mu w) = \phi(\lambda)\phi(z) + \phi(\mu)\phi(w) = \lambda\phi(z) + \mu\phi(w).$$

La première égalité vient de ce que ϕ est un morphisme de corps et qu'on peut avoir λ et μ comme des éléments de $\mathbb{Q}(\alpha)$; la deuxième, de ce qu'on a dit ci-dessus. Donc, ϕ est un automorphisme linéaire de $\mathbb{Q}(\alpha)$.

5. Soit $P \in \mathbb{Q}[X]$, écrit $P = \sum_{k=0}^{d} p_k X^k$. On a $P(\alpha) = \sum_{k=0}^{d} p_k \alpha^k$. En prenant l'image par ϕ et en utilisant les propriétés de morphisme (de corps et linéaire) :

$$\phi(P(\alpha)) = \sum_{k=0}^{d} p_k \phi(\alpha)^k = \sum_{k=0}^{d} p_k \beta^k = P(\beta).$$

En particulier, si P est non nul, alors $P(\alpha)$ aussi (transcendance de α), donc $\phi(P(\alpha)) = P(\beta)$ aussi (car ϕ est injective), donc β est transcendant.
Si on considère aussi $Q \in \mathbb{Q}[X] \setminus \{0\}$, on a de même $\phi(Q(\alpha)) = Q(\beta)$. Donc, par propriété de morphisme de corps :

$$\phi\left(\frac{P(\alpha)}{Q(\alpha)}\right) = \frac{\phi(P(\alpha))}{\phi(Q(\alpha))} = \frac{P(\beta)}{Q(\beta)}.$$

6. Par hypothèse, ϕ est bijective. On note $\gamma = \frac{P(\alpha)}{Q(\alpha)}$ l'antécédent de α par ϕ. Alors, par la question précédente, $\alpha = \frac{P(\beta)}{Q(\beta)}$. Par la question 1., on peut de plus supposer P et Q premiers entre eux.

7. On a $P(\beta) = \alpha Q(\beta)$. Donc,

$$\sum_{j=0}^{d} p_j \beta^j = \alpha \sum_{k=0}^{d} q_k \beta^k.$$

On remplace par l'expression de $\beta = \frac{A(\alpha)}{B(\alpha)}$ et on multiplie par $B(\alpha)^d$. On obtient :

$$\sum_{j=0}^{d} p_j A(\alpha)^j B(\alpha)^{d-j} = \alpha \sum_{k=0}^{d} q_k A(\alpha)^k B(\alpha)^{d-k}.$$

Ainsi, le polynôme $\sum_{j=0}^{d} p_j A^j B^{d-j} - X \sum_{k=0}^{d} q_k A^k B^{d-k}$ s'annule en α. Comme α est transcendant, ce polynôme est nul ; on obtient l'égalité annoncée.

8. Dans l'égalité précédente, A divise tous les termes sauf ceux pour $j = 0$ à gauche et $k = 0$ à droite. En isolant ces deux termes, A doit diviser leur différence qui vaut $p_0B^d - q_0XB^d = (p_0 - q_0X)B^d$.
Comme A est premier avec B, il est aussi premier avec B^d. Par le lemme de Gauss, A divise donc $p_0 - q_0X$. Ce polynôme est de degré 0 ou 1 : en effet, comme P et Q sont premiers entre eux, ils ne s'annulent pas tous les deux en 0 et donc l'un au moins des rationnels p_0, q_0 est non nul. Donc, A est aussi de degré 0 ou 1.

9. De même, B divise tous les termes dans la relation de la question 7, sauf peut-être les derniers de chaque somme. En faisant la différence, on en déduit que B divise $p_dA^d - Xq_dA^d = (p_d - q_dX)A^d$. Comme B est premier avec A, il divise $p_d - q_dX$. Par définition de d, l'un au moins des coefficients p_d, q_d est non nul. Donc, B est de degré 0 ou 1.

10. On peut donc écrire $A = aX + b$ et $B = cX + d$ avec $a, b, c, d \in \mathbb{Q}$ et $(c, d) \neq (0, 0)$. De plus, comme A et B sont premiers entre eux, $ad - bc \neq 0$.
Finalement, $\beta = \dfrac{A(\alpha)}{B(\alpha)} = \dfrac{a\alpha + b}{c\alpha + d}$.

11. Soient $a, b, c, d \in \mathbb{Q}$ tels que $ad - bc \neq 0$. On note $\beta = \dfrac{a\alpha + b}{c\alpha + d}$. On définit ϕ_β de $\mathbb{Q}(\alpha)$ dans $\mathbb{Q}(\alpha)$ par $\phi_\beta\left(\dfrac{P(\alpha)}{Q(\alpha)}\right) = \dfrac{P(\beta)}{Q(\beta)}$.
Notons déjà que ϕ_β est bien définie. Si on a une égalité $\dfrac{P(\alpha)}{Q(\alpha)} = \dfrac{P_1(\alpha)}{Q_1(\alpha)}$, alors, $P(\alpha)Q_1(\alpha) = P_1(\alpha)Q(\alpha)$, donc le polynôme $PQ_1 - P_1Q$ s'annule en α. Comme α est transcendant, ce polynôme est nul, donc s'annule en β ; on a donc $P(\beta)Q_1(\beta) = P_1(\beta)Q(\beta)$ et donc $\dfrac{P(\beta)}{Q(\beta)} = \dfrac{P_1(\beta)}{Q_1(\beta)}$ (les dénominateurs ne s'annulent pas car β est transcendant aussi ; en effet, si on avait un polynôme non nul s'annulant en β, on obtiendrait un polynôme non nul s'annulant en α).
Par des calculs analogues à ceux de la question 5, on montre que ϕ est un morphisme de corps de $\mathbb{Q}(\alpha)$. Si on note $\gamma = \dfrac{1}{ad - bc} \times \dfrac{d\alpha - b}{-c\alpha + a}$, on vérifie par un calcul direct que $\phi_\beta(\gamma) = \dfrac{1}{ad - bc} \times \dfrac{d\beta - b}{-c\beta + a} = \alpha$. On peut définir de même le morphisme de corps de $\mathbb{Q}(\alpha)$, $\phi_\gamma : \left(\dfrac{P(\alpha)}{Q(\alpha)}\right) = \dfrac{P(\gamma)}{Q(\gamma)}$. On a donc $\phi_\beta \circ \phi_\gamma(\alpha) = \phi_\beta(\gamma) = \alpha$. Ainsi, $\phi_\beta \circ \phi_\gamma$ est un morphisme de corps envoyant α sur α. Toujours par le même calcul, il envoie tout $P(\alpha)$ sur lui-même ; et donc tout élément de $\mathbb{Q}(\alpha)$ sur lui-même.
Finalement, ceci montre que ϕ_β est un automorphisme de corps de $\mathbb{Q}(\alpha)$ (il est surjectif par l'argument qui précède et injectif car c'est un morphisme de corps).
Réciproquement, la question 10 montre que l'image de α par un automorphisme de corps doit être de la forme $\dfrac{a\alpha + b}{c\alpha + d}$, avec $ad - bc \neq 0$. Et par la question 5, ϕ vaut alors ϕ_β.
Ainsi, les automorphismes de corps de $\mathbb{Q}(\alpha)$ sont exactement les ϕ_β, pour $\beta = \dfrac{a\alpha + b}{c\alpha + d}$, où $a, b, c, d \in \mathbb{Q}$ sont tels que $ad - bc \neq 0$.