Deuxième composition
Mines Ponts 1975

Les deux parties du problème sont indépendantes l'une de l'autre.

PARTIE I

On considère l'équation du second degré

$$z^2 - bz + c = 0 \tag{1}$$

dont les coefficients b et c sont dans $\mathbf{Z}$ et vérifient $b^2 - 4c < 0$; α étant l'une des racines de cette équation, on désigne par $\mathbf{Z}_\alpha$ l'ensemble des nombres complexes $z = p + q\alpha$ où p et q appartiennent à $\mathbf{Z}$. On désigne également par $\mathbf{Q}_\alpha$ l'ensemble des nombres complexes $w = u + v\alpha$ où u et v appartiennent à $\mathbf{Q}$.

I.1) Montrer que $\mathbf{Z}_\alpha$ est un sous-anneau de $\mathbf{C}$. Que peut-on dire de la seconde racine de l'équation (1) ?

I.2) Soit f l'application de $\mathbf{Z}_\alpha$ dans $\mathbf{Z}$ définie par

$$f(p + q\alpha) = p^2 + bpq + cq^2 \ .$$

Montrer

$$f(x) = 0 \Longleftrightarrow x = 0$$
$$f(xy) = f(x)f(y) \ .$$

I.3) Soit G_α l'ensemble des éléments de $\mathbf{Z}_\alpha$ qui sont inversibles dans $\mathbf{Z}_\alpha$. Montrer que G_α est un groupe pour la multiplication. Quelle est l'image de G_α par f ? En déduire que si $x = p + q\alpha$ est un élément de G_α, on a l'inégalité :

$$q^2(4c - b^2) \leq 4 \ .$$

En discutant suivant les valeurs attribuées à b et à c, déterminer tous les éléments de G_α.

I.4) a) Montrer que $\mathbf{Q}_\alpha$ est un sous-corps de $\mathbf{C}$.

b) Montrer que l'ensemble des matrices à coefficients dans $\mathbf{Q}$ définies par

$$M_{u,v} = \begin{pmatrix} u & v \\ -vc & u + bv \end{pmatrix}$$

(où u et v sont des rationnels quelconques) est un corps pour l'addition et la multiplication matricielles. Démontrer que ce corps est isomorphe au corps $\mathbf{Q}_\alpha$.

I.5) a) Montrer que $\mathbf{Q}_\alpha$ est un sous-espace vectoriel de $\mathbf{C}$ considéré comme espace vectoriel sur $\mathbf{Q}$. Quelle est la dimension de ce sous-espace vectoriel ?

b) Montrer que la fonction définie sur $\mathbf{Q}_\alpha$ à valeurs dans $\mathbf{R}$

$$x \mapsto \sqrt{f(x)} = \sqrt{f(u + v\alpha)} = \sqrt{u^2 + buv + cv^2}$$

est une norme euclidienne sur l'espace vectoriel $\mathbf{Q}_\alpha$. Déterminer le produit scalaire dont dérive cette norme. Que peut-on dire de la restriction à $\mathbf{Q}_\alpha$ de la fonction module sur $\mathbf{C}$?

I.6) a) Étant donné un élément Y de $\mathbf{Q}_\alpha$, $Y \neq 0$, montrer que $\{Y, \alpha Y\}$ constitue une base de $\mathbf{Q}_\alpha$.

b) On considère deux éléments X et Y dans $\mathbf{Z}_\alpha$ avec $Y \neq 0$. Montrer qu'il existe un élément Q dans $\mathbf{Z}_\alpha$ et deux rationnels λ et μ appartenant à l'intervalle $[0; 1[$ tels que

$$X = YQ + R \text{ où } R = Y(\lambda + \mu\alpha) .$$

I.7) On suppose dans cette septième question qu'on a $c = 1$ et $b = -1$;

a) Montrer que, pour tout X dans $\mathbf{Z}_\alpha$ et pour tout Y dans $\mathbf{Z}_\alpha$, $Y \neq 0$, il existe un couple (Q, R) d'éléments de $\mathbf{Z}_\alpha$ tel que

$$X = YQ + R \text{ et } f(R) < f(Y) .$$

b) On donne $X = 5+7\alpha$ et $Y = 3+\alpha$. Déterminer une solution (Q, R) du problème précédent et montrer que cette solution n'est pas unique.

c) Soit I un idéal arbitraire de l'anneau $\mathbf{Z}_\alpha$. Montrer que cet idéal est principal.
Si le même idéal non nul est engendré par deux éléments distincts Z et Z' de $\mathbf{Z}_\alpha$, quelle est la relation qui existe entre Z et Z' ?

d) Montrer que l'ensemble des éléments $X = (5+7\alpha)A+(3+\alpha)B$ où A et B sont des éléments quelconques de $\mathbf{Z}_\alpha$ est un idéal. Déterminer tous les générateurs de cet idéal.

I.8) Soit A_α l'ensemble des automorphismes φ de l'espace vectoriel $\mathbf{Q}_\alpha$ tels que

$$\varphi(xy) = \varphi(x)\varphi(y)$$

pour tous éléments x et y dans $\mathbf{Q}_\alpha$. Déterminer tous les éléments de A_α.

PARTIE II

On considère l'équation du troisième degré

$$x^3 - x^2 - 2x + 1 = 0 . \tag{2}$$

II.1) Montrer que toutes les racines de (2) sont réelles et appartiennent à l'intervalle $]-2; 2[$. Soit θ l'une de ces racines, montrer que θ n'est pas rationnel et que $2 - \theta^2$ est une autre racine de l'équation (2).

Dans la suite, on désigne par $\mathbf{Q}_\theta$ l'ensemble des réels $x = u + v\theta + w\theta^2$ où u, v, w sont trois rationnels arbitraires.

Montrer que $\mathbf{Q}_\theta$ est un sous-espace vectoriel de $\mathbf{R}$ considéré comme espace vectoriel sur le corps $\mathbf{Q}$ des rationnels. Quelle est la dimension de cet espace vectoriel ? Que peut-on dire de l'ensemble des trois racines de l'équation (2) ?

On admet que $\mathbf{Q}_\theta$ est un sous-corps du corps des réels.

II.2) On désigne par A_θ l'ensemble des automorphismes φ du corps $\mathbf{Q}_\theta$. Montrer que A_θ est un sous-groupe du groupe des automorphismes de l'espace vectoriel $\mathbf{Q}_\theta$.

Montrer que A_θ est un ensemble de trois éléments que l'on désignera par φ_0, φ_1, φ_2 et que l'on définira explicitement. Trouver les espaces propres de φ_1, φ_2.

(On pourra supposer que φ_0 désigne l'automorphisme identité de $\mathbf{Q}_\theta$ autrement dit l'élément unité de A_θ) .

II.3) On considère les trois applications de $\mathbf{Q}_\theta$ dans lui-même T_1, T_2, T_3 définies par

$$\begin{aligned} T_1(x) &= \varphi_0(x) + \varphi_1(x) + \varphi_2(x) \\ T_2(x) &= \varphi_0(x)\varphi_1(x) + \varphi_0(x)\varphi_2(x) + \varphi_1(x)\varphi_2(x) \\ T_3(x) &= \varphi_0(x)\varphi_1(x)\varphi_2(x)\ . \end{aligned}$$

a) Montrer que les images de ces trois applications T_1, T_2, T_3 sont incluses dans $\mathbf{Q}$.

De façon plus générale, soit un polynôme P, élément de $\mathbf{Q}[X_1, X_2, X_3]$, symétrique et homogène [a].

Montrer que l'application de $\mathbf{Q}_\theta$ dans $\mathbf{Q}_\theta$ définie par :

$$x \mapsto P\left(\varphi_0(x), \varphi_1(x), \varphi_2(x)\right)$$

est à valeurs dans $\mathbf{Q}$.

b) Montrer que l'application B définie par :

$$\forall (x, y) \in \mathbf{Q}_\theta \times \mathbf{Q}_\theta\ ,\ B(x, y) = T_1(xy)$$

est un produit scalaire.

Montrer que l'application T_2 est une forme quadratique sur l'espace $\mathbf{Q}_\theta$.

Cette forme quadratique est-elle non dégénérée positive ?

Question subsidiaire : démontrer que Q_θ est effectivement un corps.

a. i.e. $P(X_1, X_2, X_3) = P(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)})$ pour tout σ dans $\mathscr{S}_3$ et $\exists k \in \mathbf{N}$, $\forall \lambda \in \mathbf{Q}$, $P(\lambda X_1, \lambda X_2, \lambda X_3) = \lambda^k P(X_1, X_2, X_3)$.

Deuxième composition – Mines-Ponts 1975

PARTIE I

I.1) On a $1 = 1+0\alpha$ et donc $1 \in \mathbf{Z}_\alpha$. Soit p, q, r et s dans $\mathbf{Z}$, on a $p+q\alpha-(r+s\alpha) = (p-r)+(q-s)\alpha$ et $(p+q\alpha)(r+s\alpha) = pr - cqs + (qr+ps+bqs)\alpha$ et donc

$\boxed{\mathbf{Z}_\alpha \text{ est un sous-anneau de } \mathbf{C}.}$

Puisque la somme des racines de l'équation (1) est b, l'autre racine est $b-\alpha$. Par ailleurs comme les coefficients de (1) sont réels et comme le discriminant de X^2-bX+c est strictement négatif, c'est aussi le complexe conjugué de α :

$\boxed{\text{La deuxième racine de l'équation (1) est } \overline{\alpha}, \text{ ou encore } b-\alpha, \text{ et appartient à } \mathbf{Z}_\alpha.}$

I.2) Puisque $\overline{\alpha}$ est la seconde racine de l'équation (1), on a $|\alpha|^2 = \alpha\overline{\alpha} = c$ et $2\,\mathrm{Re}(\alpha) = \alpha+\overline{\alpha} = b$. D'où, pour p et q dans $\mathbf{Z}$,

$$|p+q\alpha|^2 = p^2 + q^2\,|\alpha|^2 + 2\,\mathrm{Re}(\overline{p}q\alpha) = p^2 + cq^2 + pqb = f(p+q\alpha)\ .$$

Il en résulte, pour x et y dans $\mathbf{Z}_\alpha$,

$\boxed{f(x) = 0 \Longleftrightarrow |x|^2 = 0 \Longleftrightarrow x = 0 \text{ et } f(xy) = |xy|^2 = |x|^2\,|y|^2 = f(x)f(y).}$

I.3) L'ensemble des éléments inversibles d'un anneau est un groupe multiplicatif.

$\boxed{G_\alpha \text{ est un sous-groupe multiplicatif de } \mathbf{C}^\times.}$

Puisque f préserve la multiplication, c'est donc un morphisme du groupe G_α dans le groupe des inversibles de $\mathbf{Z}$, et donc f est à valeurs dans $\{\pm 1\}$. Par ailleurs f est à valeurs positives, donc

$\boxed{f \text{ est constante égale à 1 sur } G_\alpha.}$

Remarquons que, réciproquement, si p et q sont entiers et vérifient $f(p+q\alpha) = 1$, alors $p+q\overline{\alpha}$ est l'inverse de $p+q\alpha$ dans $\mathbf{C}$ et cet inverse est en fait dans $\mathbf{Z}_\alpha$. Autrement dit, pour x dans $\mathbf{Z}_\alpha$, $x \in G_\alpha \Longleftrightarrow f(x) = 1$.

Soit donc p et q dans $\mathbf{Z}$ tels que $p+q\alpha \in G_\alpha$. On a alors $f(p+q\alpha) = 1$, i.e. $p^2+cq^2+pqb = 1$. Le trinôme du second degré $X^2 + qbX + cq^2 - 1$ admet alors p comme racine réelle et admet donc un discriminant positif, i.e. $q^2b^2 - 4(cq^2-1) \geq 0$ et donc $\boxed{q^2(4c-b^2) \leq 4.}$

Si $q = 0$, l'équation $f(p+q\alpha) = 1$ s'écrit $p^2 = 1$ et donc -1 et 1 sont exactement les éléments réels de G_α.

On suppose maintenant $q \neq 0$ et donc, puisque $4c-b^2$ est un entier strictement positif, la quantité $q^2(4c-b^2)$ est un entier compris entre 1 et 4. Par ailleurs, modulo 4, les carrés sont égaux à 0 ou 1, de sorte que $4c-b^2$ est congru à 0 ou 3 modulo 4. On obtient donc $3 \leq 4c-b^2 \leq 4$, et aussi $q^2 = 1$.

Si $b^2 = 4(c-1)$, alors b est pair et $\alpha = (b/2) \pm i$, de sorte que $\mathbf{Z}_\alpha = \mathbf{Z}_i$. Comme un élément de $\mathbf{Z}_\alpha$ s'écrit aussi $x+iy$ avec x et y entier, on a $f(x+iy) = x^2+y^2$ et donc les inversibles de $\mathbf{Z}_\alpha$ sont exactement les racines quatrièmes de l'unité.

Si $b^2 = 4c-3$, alors b est impair et $\alpha = (b-1)/2 + 1/2 \pm i\sqrt{3}/2$, de sorte que $\mathbf{Z}_\alpha = \mathbf{Z}_j$, où j est une racine cubique de l'unité. On peut reprendre l'étude précédente avec $b = -1$ et $c = 1$. Comme $|q| = 1$ et comme, pour chaque valeur de q, on a au plus deux valeurs de p, il y a en tout au plus quatre éléments inversibles non réels. Comme on sait que $\pm j$ et $\pm j^2$ sont de module 1 et donc inversibles, ce sont les seuls.

Si $b^2 = 4(c-1)$, alors $G_\alpha = \mathbf{U}_4 = \{\pm 1, \pm i\}$ et si $b^2 = 4c-3$, alors $G_\alpha = \mathbf{U}_6 = \{\pm 1, \pm j, \pm j^2\}$. Sinon $G_\alpha = \{\pm 1\}$.

I.4) a) On a $1 \in \mathbf{Q}_\alpha$. De plus, pour p, q, r et s dans $\mathbf{Q}$, on a $p+q\alpha-(r+s\alpha) = (p-r)+(q-s)\alpha$ et $(p+q\alpha)(r+s\alpha) = pr-cqs+(qr+ps+bqs)\alpha$ et donc $\mathbf{Q}_\alpha$ est un sous-anneau de $\mathbf{C}$. Si x est dans $\mathbf{Q}_\alpha \setminus \{0\}$, avec $x = p+q\alpha$ pour p et q entiers, alors $|x|^2 = p^2+q^2c+pqb$ et donc $|x|^2 \in \mathbf{Q}$. Comme $x \neq 0$, on a $|x|^2 \in \mathbf{Q}_+^*$. Il en résulte $\overline{x}/|x|^2 = (p+qb)/|x|^2 - q\alpha/|x|^2 \in \mathbf{Q}_\alpha$, i.e. $x^{-1} \in \mathbf{Q}_\alpha$. Et donc $\boxed{\mathbf{Q}_\alpha \text{ est un sous-corps de } \mathbf{C}.}$

b) On note $\mathbf{K}$ l'ensemble des matrices à coefficients dans $\mathbf{Q}$ de la forme $M_{u,v}$ avec u et v dans $\mathbf{Q}$. C'est l'espace vectoriel, sur $\mathbf{Q}$, engendré par les matrices I_2 et A avec $A = \begin{pmatrix} 0 & 1 \\ -c & b \end{pmatrix}$.

Pour vérifier que c'est un sous-anneau de $\mathscr{M}_2(\mathbf{C})$, il suffit de vérifier que A^2 appartient à $\mathbf{K}$ et cela résulte de $A^2 = bA - cI_2$.

Remarquons que $\mathbf{Q}_\alpha$ est le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{C}$ engendré par $(1, \alpha)$ et c'est donc un espace vectoriel. Comme α n'est pas rationnel, puisqu'il n'est pas réel, la famille $(1, \alpha)$ est libre et est donc une base de $\mathbf{Q}_\alpha$.

Or l'application φ qui à x dans $\mathbf{Q}_\alpha$, avec $x = u+v\alpha$ pour $(u,v) \in \mathbf{Q}^2$, associe $M_{u,v}$ est une application linéaire puisque c'est l'application linéaire entre $\mathbf{Q}$-espaces vectoriels définie par l'image de la base $(1, \alpha)$ de $\mathbf{Q}_\alpha$, à savoir $\varphi(1) = I_2$ et $\varphi(\alpha) = A$. Pour obtenir que c'est un morphisme d'anneaux, il suffit de le vérifier sur la base, et en tenant compte du fait que 1 et I_2 sont des éléments neutres, il suffit de montrer $\varphi(\alpha^2) = \varphi(\alpha)^2 = A^2$. Or $\alpha^2 = b\alpha - c$ de sorte qu'on a $\varphi(\alpha^2) = b\varphi(\alpha) - c\varphi(1) = bA - cI_2 = A^2$.

Donc φ est un morphisme d'anneaux. Puisque $\mathbf{Q}_\alpha$ est un corps, $\varphi(\mathbf{Q}_\alpha)$ est un corps et φ est injectif. En d'autres termes $\mathbf{K}$ est un corps isomorphe à $\mathbf{Q}_\alpha$.

L'ensemble des matrices $M_{u,v} = \begin{pmatrix} u & v \\ -vc & u+bv \end{pmatrix}$ (où u et v sont des rationnels quelconques) est un corps pour l'addition et la multiplication matricielles et est isomorphe au corps $\mathbf{Q}_\alpha$.

I.5) a) On a déjà répondu à cette question précédemment :

$\mathbf{Q}_\alpha$ est un sous-espace vectoriel de $\mathbf{C}$ considéré comme espace vectoriel sur $\mathbf{Q}$ et il est de dimension 2.

b) On définit sur $(\mathbf{Q}_\alpha)^2$ l'application

$$(u+v\alpha, w+t\alpha) \mapsto \langle u+v\alpha \,|\, w+t\alpha\rangle = uw + \frac{b}{2}(ut+vw) + cvt\,.$$

En tant que somme de produits, c'est une forme bilinéaire symétrique et on a $f(u+v\alpha) = |u+v\alpha|^2 = \langle u+v\alpha \,|\, u+v\alpha\rangle$. La forme est donc définie positive puisque cette dernière expression est positive et n'est nulle que si $u = v = 0$.

Autrement dit

$x \mapsto \sqrt{f(x)}$ est une norme euclidienne sur l'espace vectoriel $\mathbf{Q}_\alpha$ et elle dérive du produit scalaire donné par $\langle u+v\alpha \,|\, w+t\alpha\rangle = uw + \frac{b}{2}(ut+vw) + cvt$.

Comme cette dernière fonction est la fonction module, on en déduit que
la restriction à $\mathbf{Q}_\alpha$ de la fonction module sur $\mathbf{C}$ est une norme euclidienne.

I.6) a) Soit Y non nul dans $\mathbf{Q}_\alpha$ et $aY + b\alpha Y = 0$ une relation de dépendance linéaire sur $\mathbf{Q}$ entre Y et αY. En mettant Y en facteur, on obtient une relation de dépendance linéaire entre 1 et α et donc $a = b = 0$. Donc $(Y, \alpha Y)$ est libre. Par cardinalité,
$\{Y, \alpha Y\}$ constitue une base de $\mathbf{Q}_\alpha$.

b) Puisque X appartient à $\mathbf{Z}_\alpha$, on peut écrire $X = uY + v\alpha Y$ avec u et v dans $\mathbf{Q}$, d'après ce qui précède. On pose $Q = [u] + [v]\,\alpha$ (en notant $[x]$ la partie entière de x), de sorte que Q appartient à $\mathbf{Z}_\alpha$. Enfin on définit λ et μ par $\lambda = \{u\} = u - [u]$ et $\mu = \{v\} = v - [v]$. De la sorte λ et μ sont des rationnels dans $[0;1[$. On a de plus $X = YQ + (\lambda + \mu\alpha)Y$, i.e.
$X = YQ + R$ où $R = Y\,(\lambda + \mu\alpha)$.

I.7) a) Soit X et Y dans $\mathbf{Z}_\alpha$, avec Y non nul. La relation obtenue précédemment permet de choisir Q et R dans $\mathbf{Z}_\alpha$ tels que $X = YQ + R$ avec $f(R) = f(Y)(\lambda^2 - \lambda\mu + \mu^2)$ pour un certain couple de rationnels (λ, μ) dans $[0;1[$. Or, par convexité de $\lambda \mapsto \lambda^2 - \lambda\mu + \mu^2$ cette fonction est majorée par ses valeurs en 0 et 1 sur $[0;1[$, i.e. par $\max(\mu^2, \mu^2 + 1 - \mu)$. Pour μ dans $[0;1[$, ce maximum est donc $\mu^2 + 1 - \mu$. Toujours par convexité, cette quantité est majorée sur $[0;1[$ par ses valeurs en 0 et 1, i.e. par 1.

Comme par ailleurs $\lambda^2 - \lambda\mu + \mu^2$ est un module au carré, il est positif et, finalement, c'est un rationnel compris entre 0 et 1. Par stricte convexité, il ne pourrait valoir 1 qu'aux bornes, i.e. $\lambda = \mu = 0$ puisque les intervalles sont ouverts en 1, mais en ce cas $\lambda^2 - \lambda\mu + \mu^2 = 0$. D'où $f(R) < f(Y)$ puisque $f(Y) \neq 0$:

pour tout $X \in \mathbf{Z}_\alpha$ et pour tout $Y \in \mathbf{Z}_\alpha$, $Y \neq 0$, il existe un couple (Q, R) d'éléments de $\mathbf{Z}_\alpha$ tel que $X = YQ + R$ et $f(R) < f(Y)$.

b) Dans notre cas $\alpha^2 + \alpha + 1 = 0$ et donc $\overline{\alpha} = -1 - \alpha = \alpha^2$. On a par ailleurs

$$\frac{X}{Y} = \frac{(5 + 7\alpha)(3 + \overline{\alpha})}{9 - 3 + 1} = \frac{15 + 7 + 21\alpha + 5\overline{\alpha}}{7} = \frac{17 + 16\alpha}{7}$$

et on obtient $Q = 2 + 2\alpha$, d'où $R = X - YQ = 1 + \alpha$.
Par ailleurs on a $X = Y(3 + 2\alpha) - 2$ et $f(-2) = 4 < 7 = f(3 + \alpha)$. Donc
la solution du problème précédent n'est pas unique.

c) Soit I est nul et alors il est principal. Sinon soit $\{n \in \mathbf{N} \mid \exists x \in I \setminus \{0\}\ ,\ n = f(x)\}$. C'est une partie non vide de $\mathbf{N}^*$ et on peut donc en choisir un élément minimal. Soit alors Y dans I tel que $f(Y)$ soit ce minimum.

Comme c'est un minimum d'une partie de $\mathbf{N}^*$, $f(Y)$ est non nul, donc Y non plus. Soit alors X dans I, on l'écrit $X = QY + R$ avec (Q, R) dans $\mathbf{Z}_\alpha$ et $f(R) < f(Y)$. Comme I est un idéal et qu'on a $Y \in I$, on a aussi $QY \in I$ et donc $X - QY \in I$, soit $R \in I$. Par minimalité, il vient $f(R) = 0$ et donc $R = 0$, i.e. $X = QY$ et $X \in (Y)$. Il en résulte $I = (Y)$ et donc I est un idéal principal.

Deux générateurs d'un même idéal sont multiples l'un de l'autre. S'ils sont non nuls, cela impose qu'ils soient multiples par un élément inversible et donc ils sont associés :

Si le même idéal non nul est engendré par deux éléments distincts Z et Z' de $\mathbf{Z}_\alpha$, alors $Z/Z' \in \mathbf{U}_6$, i.e. Z' est parmi $\pm Z$, $\pm jZ$, $\pm j^2 Z$.

d) Comme X est l'idéal engendré par $5+7\alpha$ et $3+\alpha$, c'est un idéal de $\mathbf{Z}_\alpha$. Comme $\alpha^2 = 1+\alpha = 5+7\alpha-(3+\alpha)(2+2\alpha)$, on a $\alpha^2 \in X$. Or α^2 est une unité de $\mathbf{Z}_\alpha$, donc l'idéal engendré par α^2 est $\mathbf{Z}_\alpha$ et donc $\boxed{X = \mathbf{Z}_\alpha.}$

L'ensemble de ses générateurs est constitué des éléments inversibles, i.e. $\boxed{\pm 1,\ \pm j \text{ et } \pm j^2.}$

I.8) On cherche donc les automorphismes de corps de $\mathbf{Q}_\alpha$. Soit φ un tel automorphisme. On le détermine via l'image de la base $(1,\alpha)$ de $\mathbf{Q}_\alpha$. On a nécessairement $\varphi(1)=1$. Soit maintenant $\beta = \varphi(\alpha)$, il vient, puisque φ est $\mathbf{Q}$-linéaire et multiplicative, $\beta^2 = \varphi(\alpha)^2 = \varphi(\alpha^2) = \varphi(\alpha)+\varphi(1) = \beta+1$. Par conséquent $\beta = \alpha$ ou $\beta = \overline{\alpha}$ et φ est soit l'identité, soit la conjugaison complexe. Comme ces deux applications sont effectivement des automorphismes de corps, $\boxed{A_\alpha \text{ est constitué de l'identité et de la conjugaison complexe.}}$

PARTIE II

II.1) Soit P le polynôme donné par $P = X^3 - X^2 - 2X + 1$. On a $P(-2) = -7$, $P(-1) = 1$, $P(1) = -1$ et $P(2) = 1$. Donc d'après le théorème de Rolle (sur le polynômes, ou sur les fonctions continues, au choix), P admet des racines dans $]-2;-1[$, $]-1;1[$ et $]1;2[$, et donc trois racines réelles dans l'intervalle $]-2;2[$. Comme P est de degré 3, il admet au plus trois racines et donc exactement trois, i.e.

$\boxed{\text{toutes les racines de (2) sont réelles et appartiennent à l'intervalle }]-2;2[.}$

Supposons que θ soit rationnel et soit p/q une écriture irréductible de θ. On a alors $p^3 - p^2q - 2pq^2 + q^3 = 0$. Comme q divise $-p^2q - 2pq^2 + q^3$, il divise donc p^3 et donc $q = 1$ puisqu'il est premier à p. Mézalor de même p divise $p^3 - p^2q - 2pq^2$ et donc il divise 1, de sorte que θ est égal à ± 1. Comme P ne s'annule pas en ± 1, d'après le calcul précédent, il s'ensuit que $\boxed{\theta \text{ n'est pas rationnel.}}$

On utilise la formule de Taylor et il vient

$$P(2-\theta^2) = P(2) - P'(2)\theta^2 + \frac{P''(2)}{2}\theta^2 - \frac{P'''(2)}{6}\theta^6 = 1 - 6\theta^2 + 5\theta^4 - \theta^6 .$$

Par ailleurs

$$\theta^4 = \theta^3\theta = (\theta^2+2\theta-1)\theta = (\theta^2+2\theta-1) + 2\theta^2 - \theta = 3\theta^2 + \theta - 1$$

et

$$\theta^6 = \theta^4\theta^2 = 3\theta^4 + \theta^3 - \theta^2 = \theta^3 + 8\theta^2 + 3\theta - 3$$

et il vient

$$P(2-\theta^2) = 1 - 6\theta^2 + 5(3\theta^2+\theta-1) - (\theta^3+8\theta^2+3\theta-3) = -1 + 2\theta + \theta^2 - \theta^3 = -P(\theta) = 0 .$$

Par définition $\mathbf{Q}_\theta$ est le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{R}$ engendré par 1, θ et θ^2 et donc $\boxed{\mathbf{Q}_\theta \text{ est un espace vectoriel.}}$

Comme θ n'est pas rationnel, la famille $(1,\theta)$ est libre. Si la famille $(1,\theta,\theta^2)$ ne l'était pas, on pourrait trouver une relation de dépendance linéaire non triviale, i.e. un polynôme de degré au plus deux, non nul, disons Q, dans $\mathbf{Q}[X]$ tel que $Q(\theta)=0$. Soit alors $P=BQ+R$ la division euclidienne de P par Q, on a alors $R(\theta)=0$. Si R est non nul, θ est alors racine d'un polynôme de degré au plus un et est donc rationnel, ce qui n'est pas. Donc R est nul et donc Q divise P. Mézalor soit Q, soit B est de degré 1 et donc P admet une racine rationnelle, à savoir celle du polynôme de degré 1 parmi B et Q, et ceci est une nouvelle contradiction.
Par conséquent $(1,\theta,\theta^2)$ est libre et $\boxed{\mathbf{Q}_\theta \text{ est de dimension trois.}}$ De plus $2-\theta^2\neq\theta$ et comme on a vu $P(2-\theta^2)=0$, il en résulte que $\boxed{2-\theta^2 \text{ est une autre racine de l'équation (2).}}$
Notons θ, θ' et θ'' les trois racines de P et E le sous-espace vectoriel de $\mathbf{Q}_\theta$ qu'elles engendrent. Comme leur somme vaut 1, d'après les relations de Viète, $1\in E$. Comme $2-\theta^2$ est une racine de P, $\theta^2=2.1+(-1)(2-\theta^2)$ aussi appartient à E et donc E contient $(1,\theta,\theta^2)$, i.e. $E=\mathbf{Q}_\theta$. Il en résulte que

$\boxed{\text{l'ensemble des trois racines de l'équation (2) forme une famille libre et aussi une base de } \mathbf{Q}_\theta.}$

II.2) L'ensemble A_θ est donc l'ensemble des automorphismes de corps de $\mathbf{Q}_\theta$ et c'est donc $\boxed{\text{un sous-groupe de Aut}(\mathbf{Q}_\theta).}$
Soit φ un tel automorphisme. On note $\alpha=\varphi(\theta)$. Comme en I.8, il vient

$$P(\alpha)=P(\varphi(\theta))=\varphi(P(\theta))=\varphi(0)=0$$

et donc α est une racine de P. Par ailleurs φ est entièrement déterminé par α puisqu'alors l'image de la base $(1,\theta,\theta^2)$ de $\mathbf{Q}_\theta$ est $(1,\alpha,\alpha^2)$. Par conséquent A_θ est un ensemble d'au plus trois éléments.
Réciproquement soit α une racine de P et φ l'endomorphisme de $\mathbf{Q}_\theta$ qui envoie $(1,\theta,\theta^2)$ sur $(1,\alpha,\alpha^2)$. Pour vérifier que c'est un morphisme d'anneau (donc de corps), il suffit de le faire sur la base et donc de vérifier

$$\varphi(\theta^k\theta^\ell)=\varphi(\theta^k)\varphi(\theta^\ell)=\alpha^{k+\ell}$$

pour k et ℓ dans $\{1,2\}$. Soit $X^{k+\ell}=PQ+R$ la division euclidienne de $X^{k+\ell}$ par P. On a alors $\theta^{k+\ell}=R(\theta)$ et $\alpha^{k+\ell}=R(\alpha)$ puisque α et θ sont racines de P. Il vient

$$\varphi(\theta^k\theta^\ell)=\varphi(R(\theta))=R(\varphi(\theta))=R(\alpha)=\alpha^{k+\ell}$$

et donc φ est un automorphisme de corps.
Donc $\boxed{A_\theta \text{ est un ensemble de trois éléments.}}$
Si $\alpha=\theta$, alors $\boxed{\varphi_0 \text{ est l'identité.}}$
Si $\alpha=2-\theta^2$, alors $\alpha^2=4-4\theta^2+\theta^4=3+\theta-\theta^2$ et donc la matrice de φ_1 dans la base $(1,\theta,\theta^2)$ est $\boxed{\mathrm{Mat}_{(1,\theta,\theta^2)}(\varphi_1)=\begin{pmatrix}1&2&3\\0&0&1\\0&-1&-1\end{pmatrix}}$.

Enfin si α est la troisième racine, alors puisque la somme de ces racines est 1, on a $\alpha = 1-\theta-(2-\theta^2) = \theta^2-\theta-1$. Et alors

$$\alpha^2 = (\theta^2-\theta-1)^2 = \theta^4-2\theta^3-\theta^2+2\theta+1 = 3\theta^2+\theta-1-2\theta^2-4\theta+2-\theta^2+2\theta+1 = 2-\theta$$

et donc a matrice de ϕ_2 dans la base $(1,\theta,\theta^2)$ est $\boxed{\mathrm{Mat}_{(1,\theta,\theta^2)}(\varphi_2) = \begin{pmatrix} 1 & -1 & 2 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{pmatrix}.}$

On calcule le polynôme caractéristique de φ_1 et φ_2, i.e. le déterminant de $A - X.I_3$ où A est leur matrice dans la base $(1,\theta,\theta^2)$. En développant par rapport à la première colonne, on trouve pour les deux endomorphismes $(1-X)(X^2+X+1)$. Comme le trinôme n'a pas de racine dans $\mathbf{Q}$, seul 1 est valeur propre de φ_0, φ_1 et φ_2. Et les espaces propres sont de dimensions respectives 3, 1 et 1.

Le seul espace propre de φ_1 et φ_2 est $\mathbf{Q}$, pour la valeur propre 1.

II.3) a) comme A_θ est un groupe, l'application de A_θ dans lui-même donnée par $v \mapsto \varphi_1 \circ v$ est injective, donc bijective (par cardinalité). Comme l'image de φ_0 est φ_1, celle de φ_2 est soit φ_0, soit φ_2, mais ce dernier cas est impossible car $\varphi_1 \neq \mathrm{Id}_{A_\theta}$ et il vient enfin $\varphi_1^2 = \varphi_2$.

Considérons alors x dans $\mathbf{Q}_\theta$. On a

$$\varphi_1\left(T_1(x)\right) = \varphi_1\left(\sum_{v\in A_\theta} v(x)\right) = \sum_{v\in A_\theta} \varphi_1 \circ v(x) = \sum_{w\in A_\theta} w(x) = T_1(x)\ .$$

Or $\mathrm{Ker}(\varphi_1 - \mathrm{Id}) = \mathbf{Q}$ et donc $T_1(x) \in \mathbf{Q}$. Cet argument est également valide pour T_2 et T_3 et même pour tout polynôme symétrique homogène en les éléments de A_θ. En effet

$$\varphi_1\left(P(\varphi_0(x),\varphi_1(x),\varphi_2(x))\right) = P(\varphi_1\circ\varphi_0(x),\varphi_1\circ\varphi_1(x),\varphi_1\circ\varphi_2(x)) = P(\varphi_1(x),\varphi_2(x),\varphi_0(x))\ .$$

D'où, par symétrie $\varphi_1\left(P(\varphi_0(x),\varphi_1(x),\varphi_2(x))\right) = P(\varphi_0(x),\varphi_1(x),\varphi_2(x))$ et cette quantité est donc rationnelle.

Les images des trois applications T_1, T_2, T_3 sont incluses dans $\mathbf{Q}$, toute comme celle de l'application de $\mathbf{Q}_\theta$ dans $\mathbf{Q}_\theta$ définie par : $x \mapsto P\left(\varphi_0(x),\varphi_1(x),\varphi_2(x)\right)$.

b) L'application B est bilinéaire en tant que composée d'une application linéaire avec une application bilinéaire. Comme T_1 est à valeurs dans $\mathbf{Q}$, c'est une forme bilinéaire. De plus elle est symétrique par commutativité du produit dans $\mathbf{C}$. Sa forme quadratique associée est définie par $q(x) = T_1(xx)$.

Par ailleurs, pour x dans $\mathbf{Q}_\theta$, on a $T_1(x^2) = \sum_{i=0}^{2} \varphi_i(x)^2$ puisqu'on a affaire à des morphismes de corps. Comme $\mathbf{Q}_\theta \subset \mathbf{R}$, $T_1(x^2)$ est une somme de réels positifs et est donc positif. Il n'est nul que si tous les termes de la somme le sont et donc en particulier $\varphi_0(x)$, i.e. x. Donc

B est une forme bilinéaire symétrique de forme quadratique associée définie positive.

On considère l'application C définie sur $\mathbf{Q}_\theta \times \mathbf{Q}_\theta$ par

$$C(x,y) = \frac{1}{2}\sum_{i\neq j} \varphi_i(x)\varphi_j(y)\ .$$

C'est une somme de produits d'applications linéaires (à valeurs dans $\mathbf{Q}_\theta$) et c'est donc une application bilinéaire. Mais si u est dans A_θ, l'ensemble des couples (v,w) d'éléments distincts de A_θ est permuté par u (par composition à gauche) et donc $u \circ C = C$, ce qui prouve, en choisissant $u = \varphi_1$ qu'en fait C est à valeurs dans $\mathbf{Q}$. Elle est symétrique par définition et $T_2(x) = C(x,x)$, donc $\boxed{T_2 \text{ est une forme quadratique sur l'espace } \mathbf{Q}_\theta.}$

Comme $T_2(\theta) = -2$, $\boxed{\text{cette forme quadratique n'est pas non dégénérée positive.}}$

Question subsidiaire. Comme $X^3 - X^2 - 2X + 1$ n'a pas de racine dans $\mathbf{Q}$ et est de degré 3, il est irréductible sur $\mathbf{Q}$. Soit alors x dans $\mathbf{Q}_\theta$ et R un polynôme de degré au plus 2 dans $\mathbf{Q}[X]$ tel que $x = R(\theta)$. On a déjà vu que R ne saurait annuler θ que si R est nul. Supposons donc R non nul, alors il est premier à $X^3 - X^2 - 2X + 1$ puisque ce dernier est irréductible. Soit donc une relation de Bézout $AR + (X^3 - X^2 - 2X + 1)B = 1$ dans $\mathbf{Q}[X]$. On obtient, en spécialisant en θ, $x.A(\theta) = 1$ et donc x est inversible dans $\mathbf{Q}_\theta$, i.e. $\boxed{\mathbf{Q}_\theta \text{ est un corps.}}$

Démonstration du théorème de Newton

Ce théorème peut être utilisé pour répondre à la question II.3(a) et est de toute façon un bon élément de culture générale. En voici l'énoncé : soit P dans $\mathbf{Q}[X_1, X_2, X_3]$ un polynôme en trois variables. Si P est symétrique, on peut construire un polynôme Q dans $\mathbf{Q}[Y_1, Y_2, Y_3]$ tel que $P(X_1, X_2, X_3) = Q(\Sigma_1, \Sigma_2, \Sigma_3)$ où $\Sigma_1 = X_1 + X_2 + X_3$, $\Sigma_2 = X_1X_2 + X_2X_3 + X_3X_1$ et $\Sigma_3 = X_1X_2X_3$ sont des polynômes de $\mathbf{Q}[X_1, X_2, X_3]$, appelés polynômes symétriques élémentaires, et où $Q(\Sigma_1, \Sigma_2, \Sigma_3)$ désigne la composition des polynômes (ou encore la substitution).

Si $X_1^{i_1}X_2^{i_2}X_3^{i_3}$ est un monôme, on dit que $i_1 + i_2 + i_3$ est son degré. Le degré (total) de P est le maximum des degrés des monômes qui apparaissent dans P, i.e. des triplets (i_1, i_2, i_3) dans le support (fini) de P. On va démontrer le théorème par récurrence sur le nombre de variables et sur le degré de P.

Si P est un polynôme en une variable, $Q = P$ convient.

Plaçons-nous dans le cas de deux variables. Si $p \leq 0$, on pose $P = Q$. On va raisonner par récurrence sur p en se ramenant au cas d'une seule variable. Considérons donc $P(X_1, 0)$, c'est un polynôme en X_1. On le note Q_1 et on considère $P_1 = P - Q_1(X_1 + X_2)$. On a par construction $P_1(X_1, 0) = P(X_1, 0) - Q_1(X_1) = 0$ et donc X_1 divise P_1. Comme P_1 est symétrique, X_1X_2 divise P_1. De plus le degré de P_1 est inférieur à celui de P et donc si $P_1 = X_1X_2P_2$, alors P_2 est symétrique et de degré strictement inférieur à celui de P. Par hypothèse de récurrence, on a $P_2 = Q_2(X_1 + X_2, X_1X_2)$ et alors le polynôme $Q_1(Y_1) + Y_2Q_2(Y_1, Y_2)$ répond au problème.

La même méthode fonctionne en degré supérieur. On se limite ici au degré 3. Si $p \leq 0$, on pose $P = Q$. Sinon on raisonne par récurrence. On substitue 0 à X_3 pour obtenir un polynôme symétrique en X_1 et X_2. On écrit alors $P(X_1, X_2, 0) = Q_1(X_1 + X_2, X_1X_2)$ avec Q_1 dans $\mathbf{Q}[Y_1, Y_2]$. On pose alors $P_1 = P - Q_1(\Sigma_1, \Sigma_2)$. C'est un polynôme symétrique et son degré est au plus p. Mais quand on substitue 0 à X_3, on obtient $P_1(X_1, X_2, 0) = P(X_1, X_2, 0) - Q_1(X_1 + X_2, X_1X_2) = 0$ et donc X_3 divise P_1. Comme P_1 est symétrique, en fait $X_1X_2X_3 = \Sigma_3 | P_1$. On écrit donc $P_1 = \Sigma_3 P_2$ avec P_2 symétrique, de degré inférieur à $p - 3$. Par récurrence sur p, on en déduit que P_2 s'écrit $Q_2(\Sigma_1, \Sigma_2, \Sigma_3)$ et donc $Q_3 + Y_3Q_2$ répond à la question.
Bien entendu ce théorème est valide en un nombre quelconque de variables !