Devoir surveillé $n°1$
correction

Exercice

1. On vérifie facilement que E est un espace vectoriel en tant qu'un sous-espace vectoriel de $\mathbb{R}$, considéré comme $\mathbb{Q}$-espace vectoriel. De plus l'application

$$\varphi : \begin{cases} \mathbb{Q}^2 \mapsto E \\ (a,b) \mapsto a + b\sqrt{2} \end{cases}$$

est un morphisme surjective par construction et injective puisque $\sqrt{2} \notin \mathbb{Q}$. Donc E est un $\mathbb{Q}$-espace vectoriel de dimension 2.

2. (a) Montrons que N_1 et N_2 sont des normes, en effet, si $N_1(a+b\sqrt{2}) = |a|+|b| = 0$ alors $a = b = 0$ et $N_2(a+b\sqrt{2}) = |a+b\sqrt{2}| = 0$ alors $a + b\sqrt{2} = 0$, donc $a = b = 0$ car $\sqrt{2}$ est irrationnel. Les autres propriétés sont évidentes.

(b) La formule de binome motre qu'il existe deux suites d'entiers $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ telles que $\forall n \in \mathbb{N}$, $u_n = a_n - b_n\sqrt{2}$ et $v_n = a_n + b_n\sqrt{2}$.

(c) On a $\lim\limits_{n\to\infty} u_n = 0$ ($-1 < 1 - \sqrt{2} < 1$) et $\lim\limits_{n\to\infty} v_n = +\infty$ ($1 + \sqrt{2} > 1$).
Puisque $a_n = \dfrac{u_n + v_n}{2}$, alors $\lim\limits_{n\to\infty} a_n = +\infty$ et $\lim\limits_{n\to\infty} b_n = 0$ (car $u_n = a_n - b_n\sqrt{2}$). Or, on a $N_1(u_n) = |a_n| + |b_n|$, donc $\lim\limits_{n\to\infty} N_1(u_n) = +\infty$, et $N_2(u_n) = |1-\sqrt{2}|^n$, donc $\lim\limits_{n\to\infty} N_2(u_n) = 0$.
En conclusion, la suite $\left(\dfrac{N_1(u_n)}{N_2(u_n)}\right)_{n\in\mathbb{N}}$ n'est pas bornée, et par conséquent les deux normes N_1 et N_2 ne sont pas équivalentes dans E.

Problème I

1. (a) Montrons que $(\mathbb{Z}\times\mathbb{Z}, +)$ est un groupe.
- L'associativité est claire.
- $(0,0)$ est l'élément neutre, car $\forall (a,b) \in \mathbb{Z}\times\mathbb{Z}\quad (a,b)+(0,0) = (0,0)+(a,b) = (a,b)$.
- $(a,b)+(-a,-b) = (-a,-b)+(a,b) = (0,0)$, (a,b) à pour symétrique $(-a,-b)$.

Montrons que p_1 et p_2 sont des morphismes de groupes. On a : $\forall (a,b),(a',b') \in \mathbb{Z}\times\mathbb{Z}$

$$\begin{aligned} p_1[(a,b)+(a',b')] &= p_1(a+a', b+b') \\ &= a + a' \\ &= p_1(a,b) + p_1(a',b') \end{aligned}$$

et

$$\begin{aligned} p_2[(a,b)+(a',b')] &= p_2(a+a', b+b') \\ &= b + b' \\ &= p_2(a,b) + p_2(a',b') \end{aligned}$$

(b) Comme p_1 et p_2 sont des morphismes

$$\mathbb{Z}\times(1,0) = \{(m,0) \ / \ m \in \mathbb{Z}\} = p_1^{-1}(\mathbb{Z})$$

est un sous-groupe de $\mathbb{Z}\times\mathbb{Z}$ et

$$\mathbb{Z}\times(0,1) = \{(0,n) \ / \ n \in \mathbb{Z}\} = p_2^{-1}(\mathbb{Z})$$

est sous-groupe de $\mathbb{Z}\times\mathbb{Z}$.

2. (a) G est un sous-groupe de $\mathbb{Z}\times\mathbb{Z}$, donc puisque p_2 est un morphisme $p_2(G)$ est un sous-groupe de $\mathbb{Z}$, et par conséquent il existe un entier $b \geq 0$ et un seul appartenant à $p_2(G)$ tel que $p_2(G) = b\mathbb{Z}$.

(b) $\forall x, y \in \mathbb{Z}$,

$$f[(x,0)+(y,0)] = f(x+y,0) = x+y = f(x,0)+f(y,0)$$

$\forall y \in \mathbb{Z}$, il existe x unique égale à y tel que $f(x,0) = y$, donc f est isomorphisme.
Soit H un sous-groupe de $\mathbb{Z}\times(1,0)$ on a $f(H)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme

$$k\mathbb{Z}\,;\, k \in \mathbb{N}$$

d'où

$$\begin{aligned} H &= f^{-1}(k\mathbb{Z}) \\ &= \{(kl,0) \ / \ l \in \mathbb{Z}\} \\ &= \mathbb{Z}\times(k,0) \end{aligned}$$

Donc les sous-groupes de $\mathbb{Z}\times(1,0)$ sont de la forme $\mathbb{Z}\times(k,0)$ avec $k \in \mathbb{N}$.

Si $b = 0$, $p_2(G) = b\mathbb{Z} = \{0\}$, donc $G \subset \mathbb{Z}\times(1,0)$ et d'après ce qui précède $G = \mathbb{Z}\times(k,0)$ avec $k \in \mathbb{N}$.

3. (a) Soit (m,n) de G on a $p_2(m,n) \in b\mathbb{Z}$ or $p_2(m,n) = n$ d'où $n \in b\mathbb{Z}$, donc $n = br$ avec $r \in \mathbb{Z}$ unique.
D'où

$$\begin{aligned} (m,n) &= (m,rb) \\ &= (ra_0 + m - ra_0, rb) \\ &= r(a_0,b) + (s,0) \end{aligned}$$

ou $s = m - ra_0$. r et s sont uniques donc l'écriture est unique.

(b) Pour (m',n') on obtient $s' = m' - r'a_0$ avec $n' = r'b$ d'où

$$\varphi[(m,n)+(m',n')] = \varphi(m+m', n+n') = s"$$

avec $s" = m+m'-r"a_0$ et $n+n' = r"b$, d'où $r"b = rb+r'b = b(r+r')$ donc $r" = r+r'$ donc

$$\begin{aligned} s" &= m+m'-(r+r')a_0 \\ &= m - ra_0 + m - r'a_0 \\ &= s+s' \end{aligned}$$

d'où

$$\begin{aligned} \varphi[(m,n)+(m,n)] &= s" \\ &= s+s' \\ &= \varphi(m,n)+\varphi(m',n') \end{aligned}$$

et par conséquent φ est un morphisme de groupes de G dans $\mathbb{Z}$.
On en déduit que $\varphi(G)$ est un sous-groupe de $\mathbb{Z}$ donc il existe $l \in \mathbb{Z}$ tel que $\varphi(G) = l\mathbb{Z}$.

4. Soit G un sous-groupe de $\mathbb{Z}\times\mathbb{Z}$, on $\varphi(G) = l\mathbb{Z}$, avec $l \in \mathbb{Z}$.
• Si $l = 0$, alors $\varphi(G) = \{0\}$, donc $\forall (m,n) \in G$, $\varphi(m,n) = s = 0$ d'où

$$(m,n) = r(a_0,b)$$

et comme $n = rb$ et n décrit $\mathbb{Z}$ donc r décrit $\mathbb{Z}$. Par conséquent $G = \mathbb{Z} \times (a_0, b)$.
• Si $l \neq 0$

$$\begin{aligned}(m,n) &= r(a_0,b) + (s,0) \\ &= r(a_0,b) + (r'l,0) \quad \text{car} \quad \varphi(G) = l\mathbb{Z} \\ &= r(a_0,b) + r'(l,0) \quad r' \in \mathbb{Z}\end{aligned}$$

donc

$$G = \mathbb{Z} \times (a_0,b) + \mathbb{Z} \times (l,0) = \mathbb{Z} \times g_0 + \mathbb{Z} \times g_1$$

car r et r' décrivent tout $\mathbb{Z}$. ($g_0 = (a_0,b)$ et $g_1 = (l,0)$ sont linéairement indépendants puisque $b \neq 0$.)

Problème II

Première Partie [1]

1. (a) $\mathbb{K}[\alpha]$ est une $\mathbb{K}$-algèbre commutative et l'application

$$\varphi_\alpha : \begin{cases} \mathbb{K}[X] \mapsto \mathbb{K}[\alpha] \\ P \mapsto P(\alpha) \end{cases}$$

est un morphisme surjectif de $\mathbb{K}$- algèbres. Le noyau de ce morphisme est un idéal de $\mathbb{K}[X]$ et c'est précisément $I_{\mathbb{K}}(\alpha)$.
Si $I_{\mathbb{K}}(\alpha) \neq \{0\}$, $I_{\mathbb{K}}(\alpha)$ est engendré par un unique polynôme unitaire de degré $n \geq 1$ que nous notons , comme indiqué dans la suite , $P_{\mathbb{K}}(\alpha)$.
Soit alors $\beta = P(\alpha) \in \mathbb{K}[\alpha]$. Par division euclidienne de P par $P_{\mathbb{K}}(\alpha)$, on peut écrire
$P = P_{\mathbb{K}}(\alpha).Q + R$ avec $\deg R \leq n-1$. Il vient donc $\beta = R(\alpha)$ et $\mathbb{K}[\alpha]$ est engendré par $1, \alpha, \ldots, \alpha^{n-1}$.
Réciproquement si $\mathbb{K}[\alpha]$ est de dimension finie $n \geq 1$, $(1, \alpha, \ldots, \alpha^n)$ est une famille liée de $\mathbb{K}[\alpha]$ Il existe une $\mathbb{K}$- combinaison linéaire non triviale de $1, \alpha, \ldots, \alpha^n$ qui est nulle , ce qui montre l'existence d'un polynôme non nul annulé par α. Donc $I_{\mathbb{K}}(\alpha) \neq \{0\}$.

(b) L'existence et l'unicité d'un polynôme répondant à la question a déjà été obtenue ci-dessus . Il reste à montrer l'irréductibilité de $P_{\mathbb{K}}(\alpha)$. Dans le cas contraire , on aurait : $P_{\mathbb{K}}(\alpha) = Q.R$ avec

$$\begin{cases} Q\ ,\ R \in \mathbb{K}[X] \\ 0 < \deg Q < \deg P_{\mathbb{K}}(\alpha) \\ 0 < \deg R < \deg P_{\mathbb{K}}(\alpha) \end{cases}$$

Puis $Q(\alpha).R(\alpha) = 0$ implique $Q(\alpha) = 0$ ou $R(\alpha) = 0$, d'où Q ou R appartiendrait à $I_{\mathbb{K}}(\alpha)$ qui est engendré par $P_{\mathbb{K}}(\alpha)$: on aurait alors $\deg Q \geq \deg P_{\mathbb{K}}(\alpha)$ ou $\deg R \geq \deg P_{\mathbb{K}}(\alpha)$, d'où la contradiction.

(c) La question $1)a$ a montré que $\dim \mathbb{K}[\alpha] \leq \deg P_{\mathbb{K}}(\alpha)$. Par ailleurs la famille $(1, \alpha, \ldots, \alpha^{n-1})$ où $n = \deg P_{\mathbb{K}}(\alpha)$ est libre, en effet, si $\sum_{k=0}^{n-1} a_k.\alpha^k = 0$, $P = \sum_{k=0}^{n-1} a_k.X^k \in I_{\mathbb{K}}(\alpha)$ et $\deg P < \deg P_{\mathbb{K}}(\alpha)$ et donc $P = 0$. D'où $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg P_{\mathbb{K}}(\alpha)$.

1. Corrigé de G.Deruelle

(d) Il suffit de montrer que tout élément non nul de $\mathbb{K}[\alpha]$ admet un inverse dans $\mathbb{K}[\alpha]$.
Soit $\beta = \sum_{k=0}^{n-1} a_k \alpha^k \in \mathbb{K}[\alpha]\backslash\{0\}$ et $P = \sum_{k=0}^{n-1} a_k X^k$ le polynôme P, de degré strictement inférieur à celui de $P_{\mathbb{K}}(\alpha)$ qui est irréductible, est premier avec $P_{\mathbb{K}}(\alpha)$, donc Bezout donne l'existence de Q et R dans $\mathbb{K}[X]$ tels que $PQ + P_{\mathbb{K}}(\alpha)R = 1$, d'où $P(\alpha)Q(\alpha) = 1$ avec $Q(\alpha) \in \mathbb{K}[\alpha]$.

2. (a) $X^2 - 2$ est un polynôme unitaire de $\mathbb{Q}[X]$ annulé par 2 . Il est de plus irréductible dans $\mathbb{Q}[X]$ car $\sqrt{2} \notin \mathbb{Q}$, donc $P_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$.

(b) $X^4 - X^2 - 1 \in \mathbb{Q}[X]$ et est annulé par α . Il suffit comme précédemment de justifier l'irréductibilité dans $\mathbb{Q}[X]$ de ce polynôme . Sa décomposition en produit de facteurs irréductibles dans $\mathbb{R}[X]$ est $(X-\alpha)(X+\alpha)(X^2+\beta)$ où $\beta = \dfrac{\sqrt{5}-1}{2}$: aucun des facteurs n'est dans $\mathbb{Q}[X]$ et l'on ne peut obtenir une décomposition en produit de facteurs irréductibles dans $\mathbb{Q}[X]$ en multipliant deux de ces facteurs (le troisième restant n'appartenant pas à $\mathbb{Q}[X]$). Montrons par exemple que $\alpha \notin \mathbb{Q}$: sinon , pour $\alpha = \dfrac{p}{q}$, $\text{pgcd}(p,q) = 1$, on aurait $p^4 - p^2q^2 - q^4 = 0$, soit $p^4 = q^2(p^2+q^2)$, d'où nécessairement $q = 1$ et $X^4 - X^2 - 1$ admettrait un zéro entier ce qui apparaît impossible par une simple étude de variations.

Deuxième Partie

1. Soit α un zéro de P dans $\mathbb{C}$. Il est clair que $P \in I_{\mathbb{K}}(\alpha)$ qui n'est pas réduit à $\{0\}$. Comme P est irréductible, $P = P_{\mathbb{K}}(\alpha)$. Si α est de multiplicité supérieure ou égale à 2, $P'(\alpha) = 0$. Or $P' \in \mathbb{K}[X]$ donc $P' \in I_{\mathbb{K}}(\alpha)$ et $P_{\mathbb{K}}(\alpha) = P$ diviserait P' ce qui est absurde.

2. (a) Un morphisme σ de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$ est entièrement déterminé par les images qu'il prend sur les éléments de la $\mathbb{K}$-base $(1, \alpha, \ldots, \alpha^{n-1})$ de $\mathbb{K}[\alpha]$ et donc , puisque $\sigma(\alpha^k) = \sigma(\alpha)^k$, par la donnée de $\sigma(\alpha)$.
Montrons par ailleurs que le morphisme σ de $\mathbb{K}$-espaces vectoriels de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$ défini par

$$\forall k = 0, 1, \ldots, n-1, \;\; \sigma(\alpha^k) = \lambda_i^k,$$

réalise un morphisme de $\mathbb{K}$-algèbres.
Il est immédiat de vérifier que si $u = P(\alpha) \in \mathbb{K}[\alpha]$ avec $\deg P \leq n-1$, $\sigma(u) = \sigma(P(\alpha)) = P(\lambda_i)$. Alors si P est un polynôme quelconque de $\mathbb{C}[X]$, $\sigma(P(\alpha)) = P(\lambda_i)$: P s'écrit $P = P_{\mathbb{K}}(\alpha)Q + R$ avec $\deg R \leq n-1$ et $\sigma(P(\alpha)) = \sigma(R(\alpha)) = R(\lambda_i) = P(\lambda_i)$ puisque λ_i est une racine de $P_{\mathbb{K}}(\alpha)$. Soient alors $u = P(\alpha)$ et $v = Q(\alpha)$ deux éléments quelconques de $\mathbb{K}[\alpha]$: on peut écrire $PQ = P_{\mathbb{K}}(\alpha)R + S$ avec $\deg S \leq n-1$; d'où $\sigma(uv) = \sigma(S(\alpha)) = S(\lambda_i) = P_{\mathbb{K}}(\alpha)(\lambda_i)R(\lambda_i) + S(\lambda_i) = P(\lambda_i)Q(\lambda_i) = \sigma(P(\alpha))\sigma(Q(\alpha))$.

(b) Soit σ un morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$ et $\lambda = \sigma(\alpha)$. Soit $P_{\mathbb{K}}(\alpha) = X^n - \sum_{k=0}^{n-1} a_k . X^k$.
On a : $\sigma(\alpha^n) = \sigma(\alpha)^n = \lambda^n = \sigma\left(\sum_{k=0}^{n-1} a_k \alpha^k\right) = \sum_{k=0}^{n-1} a_k \sigma(\alpha)^k = \sum_{k=0}^{n-1} a_k \lambda^k$, donc λ est un zéro de $P_{\mathbb{K}}(\alpha)$. On obtient bien tous les morphismes de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$ sous la forme du $2.a)$ de cette partie. On pourra remarquer que : $\forall P \in \mathbb{K}[X], \sigma(P(\alpha)) = P(\lambda)$.

3. Soit $\beta = P(\alpha) = \sum_{k=0}^{n-1} b_k \alpha^k \in \mathbb{K}[\alpha]$. On a immédiatement : $\mathbb{K}[\beta] \subset \mathbb{K}[\alpha]$. Notons, pour tout i, σ_i' la restriction de σ_i à $\mathbb{K}[\beta]$. Les applications σ_i' sont des morphismes de $\mathbb{K}$-algèbres de $\mathbb{K}[\beta]$ dans $\mathbb{C}$ vérifiant $\sigma_i'(\beta) = \sigma_i(\beta) = \sigma_i(P(\alpha)) = P(\lambda_i)$. D'après le $2.b)$ de cette partie, les complexes $P(\lambda_i)$ sont des racines de $P_{\mathbb{K}}(\beta)$. Or, par hypothèse, ils sont tous distincts, ce qui entraîne $\deg P_{\mathbb{K}}(\beta) \geq n$ c'est à dire $\dim \mathbb{K}[\beta] \geq n = \dim \mathbb{K}[\alpha]$.
Finalement on a : $\mathbb{K}[\beta] = \mathbb{K}[\alpha]$

4. Soit $\beta = P(\alpha) = \sum_{k=0}^{n-1} b_k \alpha^k \in \mathbb{K}[\alpha]$. Avec les notations du problème, on a :

$$\lambda \in E_{ij} \Longleftrightarrow \lambda.[P(\lambda_i) - P(\lambda_j)] = \lambda_j - \lambda_i$$

qui montre que pour $i \neq j$, E_{ij} contient au plus un élément.
De la même manière manière on montre que $F_{ij} = \{\lambda \in \mathbb{K} \,/\, \sigma_i(-\alpha + \lambda.\beta) = \sigma_j(-\alpha + \lambda.\beta)\}$ contient au plus un élément. Les ensembles $E = \bigcup_{i \neq j} E_{ij}$ et $F = \bigcup_{i \neq j} F_{ij}$ sont donc finis. Il suffit alors de choisir $\lambda_1 \notin E$ tel que $\lambda_2 = 1 - \lambda_1 \notin F$: on prend $\beta_1 = \alpha + \lambda_1.\beta$ et $\beta_2 = -\alpha + \lambda_2.\beta$.
Par construction β_1 et $\beta_2 \in \mathbb{K}[\alpha]$, $\beta_1 + \beta_2 = \beta$ et les complexes $\sigma_i(\beta_1)$ sont deux à deux distincts de même que les $\sigma_i(\beta_2)$.
En vertu de la question précédente, on a : $\mathbb{K}[\beta_1] = \mathbb{K}[\beta_2] = \mathbb{K}[\alpha]$.

•••••••••