

Feuille d'exercices n°15

Exercice 1 (***)

On pose

$$\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$$

1. Soient u, v dans $\mathbb{Z}[i]$ avec $v \neq 0$. Montrer qu'il existe un couple $(q, r) \in \mathbb{Z}[i]^2$ tel que $u = qv + r$ et $|r| < |v|$.
2. Montrer que les idéaux de $(\mathbb{Z}[i], +, \times)$ sont exactement les $v\mathbb{Z}[i]$ avec $v \in \mathbb{Z}[i]$.

Corrigé : 1. Notons $\frac{u}{v} = x + iy$ avec x et y réels et posons a et b les plus proches entiers relatifs respectivement de x et y . On a

$$|a - x| \leq \frac{1}{2} \quad \text{et} \quad |b - y| \leq \frac{1}{2}$$

Notant $q = a + ib$, il vient $\left| \frac{u}{v} - q \right| = \sqrt{(x - a)^2 + (y - b)^2} \leq \frac{1}{2}$

Posant $v = u - qv$, on a q, r dans $\mathbb{Z}[i]$ et $|r| \leq \frac{1}{2}|v| < |v|$. On conclut

Il existe un couple $(q, r) \in \mathbb{Z}[i]^2$ tel que $u = qv + r$ et $|r| < |v|$.

2. Pour $v \in \mathbb{Z}[i]$, on sait que $v\mathbb{Z}[i]$ est un idéal de $\mathbb{Z}[i]$. Montrons que ce sont les seuls idéaux possibles. Soit I idéal de $\mathbb{Z}[i]$ non nul. On note v un élément de I de module minimal. Par absorption, on a $v\mathbb{Z}[i] \subset I$. Réciproquement, soit $u \in I$. D'après le résultat de la question précédente, il existe $(q, r) \in \mathbb{Z}[i]^2$ tel que $u - qv = r$ et $|r| < |v|$. Or, on a $u - qv \in I$ d'où $r = 0$ par minimalité de $|v|$. Ainsi, on a $u \in v\mathbb{Z}[i]$ et on conclut

Les idéaux de $\mathbb{Z}[i]$ sont exactement les $v\mathbb{Z}[i]$ avec $v \in \mathbb{Z}[i]$.

Exercice 2 (****)

Un anneau intègre $(A, +, \times)$ est dit *principal* si tout idéal de cet anneau est engendré par un élément. On note $A = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}, (a, b) \in \mathbb{Z}^2\}$ muni des opérations $(+, \times)$.

1. Vérifier que $(A, +, \times)$ est un anneau commutatif.
2. Pour $z \in A$, on note $N(z) = z\bar{z}$. Vérifier que

$$\forall (z, z') \in A^2 \quad N(zz') = N(z)N(z')$$

En déduire $U(A)$.

3. Après avoir vérifié que $(1 + i\sqrt{5}) \times (1 - i\sqrt{5}) = 2 \times 3$, conclure que l'anneau n'est pas principal.

Corrigé : 1. On a $1 = 1 + 0 \times i\sqrt{5} \in A$. Soient (a, b) et (c, d) dans $\mathbb{Z}^2$. On trouve

$$a + ib\sqrt{5} - (c + id\sqrt{5}) = a - c + i(b - d)\sqrt{5} \in A$$

et

$$(a + ib\sqrt{5})(c + id\sqrt{5}) = (ac - 5bd) + i(ad + bc)\sqrt{5} \in A$$

ce qui prouve que A est un sous-anneau de $(\mathbb{C}, +, \times)$ et par conséquent

$$\boxed{\text{L'ensemble } (A, +, \times) \text{ est un anneau commutatif.}}$$

2. Soit $(z, z') \in A^2$. Par propriétés sur les complexes, il vient

$$N(z z') = (z z') (\overline{z z'}) = z z' \bar{z} \bar{z}' = z \bar{z} z' \bar{z}'$$

D'où

$$\boxed{\forall (z, z') \in A^2 \quad N(z z') = N(z) N(z')}$$

$$\text{On a} \quad \forall (a, b) \in \mathbb{Z}^2 \quad N(a + ib\sqrt{5}) = (a + ib\sqrt{5})(a - ib\sqrt{5}) = a^2 + 5b^2 \in \mathbb{N}$$

Soit $(a, b) \in \mathbb{Z}^2$ tel que $a + ib\sqrt{5} \in U(\mathbb{Z}[i\sqrt{5}])$. Il existe $(c, d) \in \mathbb{Z}^2$ tel que $(a + ib\sqrt{5})(c + id\sqrt{5}) = 1$ et

$$N((a + ib\sqrt{5})(c + id\sqrt{5})) = N(a + ib\sqrt{5})N(c + id\sqrt{5}) = N(1) = 1$$

d'où

$$(a, b) \in \{(1, 0), (-1, 0)\}$$

La réciproque est immédiate et on conclut

$$\boxed{U(\mathbb{Z}[i\sqrt{5}]) = \{(1, 0), (-1, 0)\}}$$

3. Sans difficulté, on constate l'égalité

$$(1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \times 3$$

Un élément p de A est dit *irréductible* si $p \notin U(A)$ et si

$$\forall (a, b) \in A^2 \quad p = ab \implies a \in U(A) \quad \text{ou} \quad b \in U(A)$$

C'est exactement la même notion que celle vue dans $\mathbb{K}[X]$. Vérifions que $1 + i\sqrt{5}$ est irréductible. Supposons que $1 + i\sqrt{5} = uv$ avec $(u, v) \in A^2$. Il vient

$$N(1 + i\sqrt{5}) = 6 = N(uv) = N(u)N(v) \implies N(u) \in \{1, 2, 3, 6\}$$

On vérifie sans difficulté que $N(u) \notin \{2, 3\}$ ce qui impose u ou v dans $U(A)$ et prouve donc que $1 + i\sqrt{5}$ est irréductible. De même, on établit que 2 et 3 sont irréductibles. Supposons A principal. Alors, il existe $x \in A$ tel que $(x) = (1 + i\sqrt{5}) + (2)$ d'où $x|1 + i\sqrt{5}$ et $x|2$. On en déduit $x \in U(A)$ et par conséquent

$$(1 + i\sqrt{5}) + (2) = A$$

On dispose alors de $(u, v) \in A^2$ tel que

$$(1 + i\sqrt{5})u + 2v = 1$$

puis

$$(1 + i\sqrt{5})3u + 6v = (1 + i\sqrt{5})(3v + (1 - i\sqrt{5})v) = 3$$

d'où $1 + i\sqrt{5}|3$ ce qui est faux. On conclut

$$\boxed{\text{L'anneau } A \text{ n'est pas principal.}}$$

Remarque : En fait, l'égalité $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \times 3$ prouve que l'anneau A n'est pas *factoriel*, *i.e.* intègre et tel que tout élément non nul admet une décomposition en facteurs irréductibles, unique à l'ordre près. On peut démontrer qu'un anneau principal est factoriel.

Exercice 3 (***)

Soit $(\mathbb{K}, +, \times, \cdot)$ une $\mathbb{R}$ -algèbre commutative, intègre, de dimension finie $n \geq 2$. On note 0 et 1 les éléments neutres de $\mathbb{K}$ et pour alléger les notations, on confond $\mathbb{R}$ et $\mathbb{R}1$.

1. Soit a un élément non nul de $\mathbb{K}$. Pour $x \in \mathbb{K}$, on pose $f_a(x) = ax$. Montrer que f est un automorphisme linéaire de $\mathbb{K}$.
2. Soit $a \in \mathbb{K} \setminus \mathbb{R}$. Montrer que la famille $(1, a)$ est libre mais pas $(1, a, a^2)$.
3. Montrer que l'on peut trouver $i \in \mathbb{K}$ tel que $i^2 = -1$. En déduire que $\mathbb{K}$ est une $\mathbb{R}$ -algèbre isomorphe à $\mathbb{C}$.

Corrigé : 1. On rappelle que $(\mathbb{K}, +, \cdot)$ est un $\mathbb{R}$ -ev de dimension finie, $(\mathbb{K}, +, \times)$ est un anneau et qu'on a

$$\forall (\lambda, x, y) \in \mathbb{R} \times \mathbb{K}^2 \quad (\lambda \cdot x)y = \lambda \cdot (xy) = x(\lambda \cdot y)$$

Ainsi

$$\forall (\lambda, x, y) \in \mathbb{R} \times \mathbb{K}^2 \quad f_a(x + \lambda y) = a(x + \lambda \cdot y) = ax + \lambda \cdot (ay) = f_a(x) + \lambda \cdot f_a(y)$$

Puis, par intégrité de $\mathbb{K}$, il vient

$$\forall x \in \mathbb{K} \quad f_a(x) = 0 \iff ax = 0 \iff x = 0$$

L'application f_a est donc un endomorphisme injectif dans un $\mathbb{R}$ -ev de dimension finie et par conséquent

$$\boxed{\forall a \in \mathbb{K}^* \quad f_a \in \text{GL}(\mathbb{K})}$$

Remarque : On en déduit notamment que $\mathbb{K}$ est un corps puisque pour tout $a \in \mathbb{K}^*$, on dispose, par surjectivité de f_a , de $b \in \mathbb{K}$ tel que $f_a(b) = 1$, c'est-à-dire $ab = 1$.

2. Soit $a \in \mathbb{K} \setminus \mathbb{R}$. Ce choix est possible puisque $\mathbb{K}$ est un $\mathbb{R}$ -ev de dimension $n \geq 2$. La famille $(1, a)$ n'est pas liée, sans quoi on aurait a colinéaire à 1 puisque 1 est non nul, ce qui impliquerait a réel. La famille $(a^k)_{k \in [0; n]}$ est une famille de $n + 1$ vecteurs dans $\mathbb{K}$ qui est un $\mathbb{R}$ -ev de dimension n . Il s'agit donc d'une famille liée d'où l'existence de $(\alpha_k)_{k \in [0; n]} \in \mathbb{R}^{n+1} \setminus \{0_{\mathbb{R}^{n+1}}\}$ tel que $\sum_{k=0}^n \alpha_k a^k = 0$. Ainsi, posant $R = \sum_{k=0}^n \alpha_k X^k$, on a montré

$$\boxed{\text{Il existe un polynôme non nul } R \in \mathbb{R}[X] \text{ tel que } R(a) = 0.}$$

Considérant l'écriture de R comme produit de facteurs irréductibles dans $\mathbb{R}[X]$, on en déduit, par intégrité de $\mathbb{K}$, qu'il existe $P_a \in \mathbb{R}[X]$ irréductible tel que $P_a(a) = 0$. On a $\deg P_a > 1$ par liberté de $(1, a)$ et comme les polynômes irréductibles de $\mathbb{R}[X]$ sont de degré 1 ou 2, on conclut $\deg P_a = 2$ d'où

$$\boxed{\text{La famille } (1, a) \text{ est libre mais pas } (1, a, a^2).}$$

3. On peut choisir P_a unitaire. On note $P_a = X^2 + \alpha X + \beta$ avec α, β réels tels que $\alpha^2 - 4\beta < 0$. Puis, il vient

$$\begin{aligned} P_a(a) = 0 &\iff a^2 + \alpha a + \beta = 0 \iff \left(a + \frac{\alpha}{2}\right)^2 + \frac{4\beta - \alpha^2}{4} = 0 \\ &\iff \left(\frac{2}{\sqrt{4\beta - \alpha^2}} \left(a + \frac{\alpha}{2}\right)\right)^2 + 1 = 0 \end{aligned}$$

On pose

$$b = \frac{2}{\sqrt{4\beta - \alpha^2}} \left(a + \frac{\alpha}{2}\right)$$

L'élément b vérifie alors $b^2 + 1 = 0$. La famille $(1, b)$ est libre sans quoi b serait réel et on note $A = \text{Vect}(1, b)$. Montrons $A = \mathbb{K}$. On procède par l'absurde en considérant $c \in \mathbb{K} \setminus A$. En particulier, on a $c \in \mathbb{K} \setminus \mathbb{R}$ et en procédant comme pour la construction de b , on obtient l'existence de $d \in \text{Vect}(1, c)$ tel que $d^2 + 1 = 0$. Il s'ensuit $d^2 = b^2$ puis $(d - b)(d + b) = 0$ par commutativité de $\mathbb{K}$ et par intégrité $d = b$ ou $d = -b$. Il en résulte que $b = \pm d = \lambda + \mu c$ avec λ, μ réels et $\mu \neq 0$ sinon b réel d'où $c \in \text{Vect}(1, b) = A$ ce qui est faux. On en déduit que $\mathbb{K} = \text{Vect}(1, b)$. Enfin, on considère

$$\varphi: \begin{cases} \mathbb{C} \longrightarrow \mathbb{K} \\ z \longmapsto \text{Re } z + b \text{Im } z \end{cases}$$

et on vérifie sans difficulté que φ est un isomorphisme d'algèbres. On conclut

La $\mathbb{R}$ -algèbre $\mathbb{K}$ est isomorphe à $\mathbb{C}$.

Exercice 4 (***)

Déterminer dans $\mathbb{K}[X]$ les polynômes divisibles par leur polynôme dérivé.

Corrigé : Soit $P \in \mathbb{K}[X]$. Si P' divise P , alors comme $\deg P = 1 + \deg P'$, on a $P = \lambda(X - \alpha)P'$. Donc P admet une racine α . Soit m son ordre et notons $P = \lambda(X - \alpha)^m Q$ avec $Q(\alpha) \neq 0$. Ainsi $P' = (X - \alpha)^{m-1} Q$. Mais par dérivation

$$P' = \lambda(X - \alpha)^{m-1} [mQ + (X - \alpha)Q']$$

d'où

$$Q = \lambda [mQ + (X - \alpha)Q']$$

En évaluant pour $X = \alpha$, on trouve $\lambda m = 1$ puis

$$(X - \alpha)Q' = 0 \implies Q' = 0$$

On conclut Si P' divise P , alors P de la forme $\lambda(X - \alpha)^m$ avec $\alpha \in \mathbb{K}$ et m entier.

Variantes : 1. Dans l'ensemble des fractions rationnelles $\mathbb{C}(X)$, on sait que $\frac{P'}{P} = \sum_{i=1}^r \frac{m_i}{X - \alpha_i}$ avec α_i les racines et m_i leurs multiplicités. Or, on a P' divise P d'où $P = \lambda(X - \alpha)P'$ d'où $\frac{P'}{P} = \frac{1}{\lambda(X - \alpha)}$ et on en déduit $r = 1$. On retrouve le résultat précédent.

2. Si $\mathbb{K} = \mathbb{R}$, on peut aussi montrer, par l'absurde, qu'un polynôme P solution possède une unique racine. En effet, sinon, on pourrait, avec le théorème de Rolle, trouver une racine de P' entre deux racines consécutives de P qui serait alors racine de P , ce qui est absurde.

Exercice 5 (****)

Pour P dans $\mathbb{C}[X]$, on note $Z(P)$ l'ensemble des racines de P .

1. Soit P dans $\mathbb{C}[X]$ avec $\deg P \geq 1$. Montrer

$$\text{Card } Z(P) = \deg P - \deg(P \wedge P')$$

2. Soient P, Q des polynômes non constants de $\mathbb{C}[X]$ tels que $Z(P) = Z(Q)$ et $Z(P - 1) = Z(Q - 1)$. Montrer que $P = Q$.

Corrigé : 1. Notons $P = \lambda \prod_{i=1}^r (X - \alpha_i)^{m_i}$ avec λ, α_i des complexes et m_i des entiers non nuls. Comme α_i racine de P' de multiplicité $m_i - 1$, on a

$$P \wedge P' = \prod_{i=1}^r (X - \alpha_i)^{m_i-1}$$

et
$$\deg(P \wedge P') = \sum_{i=1}^r (m_i - 1) = \deg P - r$$

Ainsi

$$\boxed{\text{Card } Z(P) = \deg P - \deg(P \wedge P')}$$

2. Notons $n = \deg P$ et $m = \deg Q$. On suppose $n \geq m$. Posons $R = P - Q$. On a $Z(R) \supset Z(P) \cup Z(P - 1)$ et $Z(P) \cap Z(P - 1) = \emptyset$ d'où

$$\text{Card } Z(R) \geq \text{Card } Z(P) + \text{Card } Z(P - 1)$$

D'après le résultat de la question précédente, on a

$$\text{Card } Z(P) = n - \deg(P \wedge P') \quad \text{et} \quad \text{Card } Z(P - 1) = n - \deg((P - 1) \wedge P')$$

Les polynômes P et $P - 1$ sont premiers entre eux car sans racine commune et par conséquent, on a $P \wedge P'$ et $(P - 1) \wedge P'$ diviseurs de P' qui sont premiers entre eux d'où $(P \wedge P')((P - 1) \wedge P') | P'$ et par conséquent

$$\deg(P \wedge P') + \deg((P - 1) \wedge P') \leq \deg P' = n - 1$$

Il s'ensuit
$$\text{Card } Z(R) \geq 2n - (n - 1) = n + 1 \quad \text{et} \quad \deg R \leq n$$

On en déduit $R = 0$ et par conséquent

$$\boxed{P = Q}$$

Exercice 6 (***)

Soient P, Q deux polynômes de $\mathbb{C}[X]$ non constants avec $\deg P = n$ et $\deg Q = m$. On pose

$$\Phi: \begin{cases} \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X] & \longrightarrow \mathbb{C}_{n+m-1}[X] \\ (U, V) & \longmapsto UP + VQ \end{cases}$$

1. Montrer que Φ est bien définie, linéaire puis déterminer sa matrice dans les bases canoniques des espaces de départ et d'arrivée. On notera $\text{Res}[P, Q]$ le déterminant de cette matrice appelé *résultant* de P et Q .
2. Établir
$$\Phi \text{ bijective} \iff P \wedge Q = 1$$
3. Soit $P = X^3 + px + q$ avec $p, q \in \mathbb{C}$. Montrer que P admet une racine double si et seulement si $4p^3 + 27q^2 = 0$.

Corrigé : 1. Soit $(U, V) \in \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X]$. On a $\deg UP \leq n + m - 1$ et $\deg VQ \leq n + m - 1$ d'où $\deg UP + VQ \leq n + m - 1$. Par ailleurs, l'application Φ est linéaire par linéarité de la somme et du produit d'où

$$\boxed{\Phi \in \mathcal{L}(\mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X], \mathbb{C}_{n+m-1}[X])}$$

Supposons Φ bijective. En particulier, on a Φ surjective d'où

$$\exists (U, V) \in \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X] \quad | \quad \Phi(U, V) = UP + VQ = 1$$

La base canonique de $\mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X]$ est constituée de $(X^i, 0)_{0 \leq i \leq m-1}$ suivi de $(0, X^{i-m})_{m \leq i \leq n+m-1}$.
On trouve

$$\begin{pmatrix} a_0 & 0 & \dots & 0 & b_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ a_n & & & a_0 & b_m & & & b_0 \\ 0 & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & a_n & 0 & \dots & 0 & b_m \end{pmatrix}$$

Sur ce schéma, on a supposé $n = m$ pour des raisons pratiques mais la forme obtenue a lieu pour tout couple d'entiers non nuls (n, m) .

2. Supposons Φ bijective. D'après le théorème de Bézout, on en déduit $P \wedge Q = 1$. Supposons $P \wedge Q = 1$. On a

$$\Phi(U, V) = 0 \iff UP = -VQ$$

D'après le lemme de Gauss, on en déduit $P|V$ et $Q|U$ mais $\deg V < \deg P$ et $\deg U < \deg P$ d'où $(U, V) = (0, 0)$. Ainsi, l'application Φ est injective et comme on a

$$\dim \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X] = \dim \mathbb{C}_{m-1}[X] + \dim \mathbb{C}_{n-1}[X]$$

l'injectivité de Φ équivaut à sa bijectivité. Ainsi

$$\boxed{\Phi \text{ bijective} \iff P \wedge Q = 1}$$

3. On considère Φ associée à P et P' . On a

$$P \text{ admet une racine double} \iff P \wedge P' \neq 1 \iff \det \Phi = 0$$

On trouve

$$\det \Phi = \begin{vmatrix} q & 0 & p & 0 & 0 \\ p & q & 0 & p & 0 \\ 0 & p & 3 & 0 & p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = q \begin{vmatrix} q & 0 & p & 0 \\ p & 3 & 0 & p \\ 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 3 \end{vmatrix} + p \begin{vmatrix} p & q & p & 0 \\ 0 & p & 0 & p \\ 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 3 \end{vmatrix}$$

En développant le premier déterminant sur la 3-ième ligne et le deuxième déterminant sur la première colonne, on trouve

$$\det \Phi = 4p^3 + 27q^2$$

Ainsi

$$\boxed{P \text{ admet une racine double} \iff 4p^3 + 27q^2 = 0}$$