FEUILLE DE TD N° 10

Déterminants, Endomorphismes orthogonaux, Anneaux

6 mai 2022

■ *Pour commencer . . .*

Exercice 1.
Soit E un $\mathbb{R}$-espace vectoriel. Soit (u, v, w) une famille libre de vecteurs de E et soit $(\alpha, \beta, \gamma) \in \mathbb{R}^3$. On définit $s = \alpha u + \beta v + \gamma w$. Donner une condition nécessaire et suffisante sur α, β, γ pour que la famille $(u + s, v + s, w + s)$ soit libre.

On définit $F = \text{vect}(u, v, w)$. F est un sous-espace vectoriel de dimension 3 de E, une base de F est $\mathcal{B} = (u, v, w)$. La famille $(u + s, v + s, w + s)$ est une famille de vecteurs de F, donc elle est libre si et seulement si c'est une base de F, c'est-à-dire si et seulement si $\det_{\mathcal{B}}(u + s, v + s, w + s) \neq 0$. Or

$$\begin{aligned}
\det_{\mathcal{B}}(u+s, v+s, w+s) &= \begin{vmatrix} 1+\alpha & \alpha & \alpha \\ \beta & 1+\beta & \beta \\ \gamma & \gamma & 1+\gamma \end{vmatrix} \\
&\underset{C_2 \leftarrow C_2 - C_1}{=} \begin{vmatrix} 1+\alpha & -1 & \alpha \\ \beta & 1 & \beta \\ \gamma & 0 & 1+\gamma \end{vmatrix} \\
&\underset{C_3 \leftarrow C_3 - C_1}{=} \begin{vmatrix} 1+\alpha & -1 & -1 \\ \beta & 1 & 0 \\ \gamma & 0 & 1 \end{vmatrix} \\
&= 1 + \alpha + \beta + \gamma.
\end{aligned}$$

Ainsi, la famille est libre si et seulement si $1 + \alpha + \beta + \gamma \neq 0$.

Exercice 2. Soit E un sous-espace vectoriel de dimension 2 ou 3 de $\mathbb{R}^3$. Si G est un sev de E, on définit $G^\perp = \{x \in E \mid \forall y \in G,\, x \cdot y = 0\}$.
Soit u un endomorphisme orthogonal de E. Soit F un sev de E.

1. Montrer que $(u(F))^\perp = u\left(F^\perp\right)$.
2. Montrer que si $u(F) \subset F$, alors $u\left(F^\perp\right) \subset F^\perp$.

---

1. Procédons par double inclusion. Soit d'abord $x \in (u(F))^\perp$, montrons que $x \in u\left(F^\perp\right)$. u est un automorphisme, donc $x = u\left(u^{-1}(x)\right)$. Il reste à montrer que $u^{-1}(x) \in F^\perp$. Soit $y \in F$, puisque u est orthogonal, on a
$$u^{-1}(x) \cdot y = u\left(u^{-1}(x)\right) \cdot u(y) = x \cdot u(y) = 0,$$
car $x \in (u(F))^\perp$ et $y \in F$. Donc $(u(F))^\perp \subset u\left(F^\perp\right)$.
Réciproquement, soit $x \in u\left(F^\perp\right)$, montrons que $x \in (u(F))^\perp$. On a $x = u(y)$ avec $y \in F^\perp$. Soit $z \in u(F)$, c'est-à-dire $z = u(s)$ avec $s \in F$. Alors
$$x \cdot z = u(y) \cdot u(s) = y \cdot s = 0.$$
D'où l'inclusion réciproque.
2. Puisque u est bijective, si $u(F) \subset F$, on a en fait $u(F) = F$ (par égalité des dimensions). Donc
$$u\left(F^\perp\right) = (u(F))^\perp = F^\perp.$$
Ceci montre l'inclusion demandée.

Exercice 3. (Formule de Cramer)
Soit $A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \in \mathrm{GL}_3(\mathbb{R})$. Soit $B = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \in \mathbb{R}^3$, on note X l'unique solution du système linéaire $AX = B$. Montrer que $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, avec

$$x = \frac{\begin{vmatrix} b_1 & a_{1,2} & a_{1,3} \\ b_2 & a_{2,2} & a_{2,3} \\ b_3 & a_{3,2} & a_{3,3} \end{vmatrix}}{\det A}, \quad y = \frac{\begin{vmatrix} a_{1,1} & b_1 & a_{1,3} \\ a_{2,1} & b_2 & a_{2,3} \\ a_{3,1} & b_3 & a_{3,3} \end{vmatrix}}{\det A} \quad \text{et } z = \frac{\begin{vmatrix} a_{1,1} & a_{1,2} & b_1 \\ a_{2,1} & a_{2,2} & b_2 \\ a_{3,1} & a_{3,2} & b_3 \end{vmatrix}}{\det A}.$$

On ne fait que le calcul pour x. On a

$$\begin{aligned}
\begin{vmatrix} b_1 & a_{1,2} & a_{1,3} \\ b_2 & a_{2,2} & a_{2,3} \\ b_3 & a_{3,2} & a_{3,3} \end{vmatrix} &= \begin{vmatrix} xa_{1,1} + ya_{1,2} + za_{1,3} & a_{1,2} & a_{1,3} \\ xa_{2,1} + ya_{2,2} + za_{2,3} & a_{2,2} & a_{2,3} \\ xa_{3,1} + ya_{3,2} + za_{3,3} & a_{3,2} & a_{3,3} \end{vmatrix} \\
&= x \begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} + y \begin{vmatrix} a_{1,2} & a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,2} & a_{3,3} \end{vmatrix} + z \begin{vmatrix} a_{1,3} & a_{1,2} & a_{1,3} \\ a_{2,3} & a_{2,2} & a_{2,3} \\ a_{3,3} & a_{3,2} & a_{3,3} \end{vmatrix} \\
&= x \det A.
\end{aligned}$$

On obtient bien la formule demandée.

Pour aller plus loin . . .

Exercice 4. Soit $f : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}$. On dit que f est *bilinéaire* si pour tous u, v, $w \in \mathbb{R}^2$ et pour tout $\lambda \in \mathbb{R}$, $f(u + \lambda v, w) = f(u, w) + \lambda f(u, w)$ et $f(u, v + \lambda w) = f(u, v) + \lambda f(u, w)$. On dit que f est *alternée* si pour tout $u \in \mathbb{R}^2$, $f(u, u) = 0$. On dit que f est *antisymétrique* si pour tous u, $v \in \mathbb{R}^2$, $f(u, v) = -f(v, u)$.

1. Supposons que f est bilinéaire. Montrer que f est alternée si et seulement si f est antisymétrique.
2. Supposons que f est bilinéaire et alternée. Montrer qu'il existe $\alpha(f) \in \mathbb{R}$ tel que, pour tous u, $v \in \mathbb{R}^2$,

$$f(u, v) = \alpha(f) \det_{\mathcal{C}}(u, v),$$

où $\mathcal{C}$ est la base canonique de $\mathbb{R}^2$.

---

1. Supposons que f est bilinéaire et alternée. Soient u, $v \in \mathbb{R}^2$, on a

$$\begin{aligned} f(u+v, u+v) &= 0 \\ &= f(u,u) + f(u,v) + f(v,u) + f(v,v) \\ &= f(u,v) + f(v,u). \end{aligned}$$

D'où $f(u, v) = -f(v, u)$, donc f est antisymétrique.
Réciproquement, supposons que f est bilinéaire et antisymétrique. Alors pour tout u, $f(u, u) = -f(u, u) = 0$. Donc f est alternée.

2. Soient $u = \begin{pmatrix} x \\ y \end{pmatrix}$ et $v = \begin{pmatrix} x' \\ y' \end{pmatrix}$. On note $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, on a donc $u = xe_1 + ye_2$ et $v = x'e_1 + y'e_2$. Par bilinéarité,

$$f(u, v) = xyf(e_1, e_1) + xy'f(e_1, e_2) + x'yf(e_2, e_1) + x'y'f(e_2, e_2).$$

Or f est alternée donc

$$f(u, v) = xy'f(e_1, e_2) + x'yf(e_2, e_1).$$

Pour finir, f est antisymétrique donc

$$f(u, v) = (xy' - x'y)f(e_1, e_2).$$

En notant $\alpha(f) = f(e_1, e_2)$, on obtient le résultat.

Un peu d'Algèbre . . .

Exercice 5.

1. Soit $n \geq 2$. Donner un exemple d'anneau à n éléments.
2. Donner un second exemple d'anneau à 4 éléments.
3. Soit $m \geq 2$. Donner un second exemple d'anneau à m^n éléments.
4. Est-ce que $\mathbb{Z}/6\mathbb{Z}$ est un anneau intègre ? (Démontrer la réponse)
5. Soient A, B deux anneaux. Montrer que l'anneau produit $A \times B$ n'est pas intègre.

---

1. $\mathbb{Z}/n\mathbb{Z}$ convient.
2. L'anneau produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un autre anneau à $4 = 2 \times 2$ éléments.
3. L'ensemble $Fonct(\{1, \ldots, m\}, \mathbb{Z}/n\mathbb{Z})$ des fonctions $f : \{1, \ldots, m\} \to \mathbb{Z}/n\mathbb{Z}$ est un anneau. Il contient m^n éléments.

4. $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre. En effet, on a $\overline{23} = \overline{6} = \overline{0}$.
5. On a $(1_A, 0_B) \times (0_A, 1_B) = (1_A.0_A, 0_B.1_B) = (0_A, 0_B) = 0_{A\times B}$. Donc cet anneau n'est pas intègre.

Exercice 6.
Soit A un anneau commutatif.

1. Soit $n \geq 1$. Soit $a \in A$ tel que $a^n = 1$.
Montrer que a est inversible. Combien vaut a^{-1} ?
2. Soit $b \in A$. Soit P un polynôme unitaire tel que $P(0) \in A^\times$ et $P(a) = 0$.
Montrer que a est inversible, et calculer a^{-1}.
3. On suppose que l'ensemble des éléments inversibles $A^\times$ est fini.
Trouver un polynôme P unitaire tel que $P(c) = 0$, pour tout $c \in A^\times$.

---

1. On pose $a' = a^{n-1}$. On a alors $aa' = a'a = 1$, donc a est inversible, et $a^{-1} = a^{n-1}$.
2. Le polynôme s'écrit $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, avec $a_0, \ldots, a_{n-1} \in A$.
On a $a_0 = P(0) \in A^\times$.
On a $0 = P(b) = b^n + \ldots + a_1b + a_0 = b(b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1) + a_0$.

Donc, on a $-a_0 = b(b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1)$.
Comme a_0 est inversible, on a $1 = b(b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1)(-a_0^{-1})$. En posant $b' = (b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1)(-a_0^{-1})$, on a $b'b = bb' = 1$.
Donc b est inversible, d'inverse b'.

3. Si $A^\times$ est fini, on a donc un groupe fini. Pour $Card(A^\times) = n$, le chapitre sur les Groupes nous dit que pour $c \in A^\times$, on a $c^n = 1$.
Donc, $P(X) = X^n - 1$ convient.

Exercice 7. 1. Soit A un anneau commutatif fini. Trouver un polynôme P tel que $P(a) = 0$ pour tout $a \in A$.

2. Dans $\mathbb{Z}/p\mathbb{Z}$, montrer que $Q(X) = X^p - X$ convient.
On pourra s'aider de l'exercice précédent.

3. Dans $\mathbb{Z}/6\mathbb{Z}$, trouver un polynôme R, avec $\deg(R) < 6$, tel que $R(a) = 0$ pour tout $a \in \mathbb{Z}/6\mathbb{Z}$.
On pourra chercher un polynôme qui ressemble à Q.

---

1. Comme A est fini on écrit $A = \{a_0, \ldots, a_n\}$. On pose alors $P(X) = (X - a_0)(X - a_1)\ldots(X - a_n)$. Ce polynôme P convient.

2. Dans $\mathbb{Z}/p\mathbb{Z}$, tout élément non-nul est inversible. $\mathbb{Z}/p\mathbb{Z} = \{0\} \cup (\mathbb{Z}/p\mathbb{Z})^\times$.
On a vu dans l'exercice précédent que pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, a est annulé par le polynôme $X^{p-1} - 1$.
Il reste 0, qui est annulé par le polynôme X.
Donc, le polynôme $X(X^{p-1} - 1) = X^p - X$ est un polynôme qui est annulé par tous les éléments de $\mathbb{Z}/p\mathbb{Z}$.

3. Dans $\mathbb{Z}/6\mathbb{Z}$, on cherche un polynôme de la forme $X^m - X$. On regarde donc les puissances de chaque élément.
On remarque que $\overline{k}^3 = \overline{k}$, pour tout $\overline{k}$.
Donc, le polynôme $R(X) = X^3 - X$ convient.