Correction séance 2 (26 janvier)

† *Premiers exemples*

Exercice 3. Montrons que $\varphi(M')$ est un sous-module de N : on a

$$\varphi(M') = \{\varphi(m) \mid m \in M'\}$$

- $\varphi(M')$ est non vide car il contient $\varphi(0_M) = 0_N$.
- $\varphi(M')$ est stable par somme : $\varphi(m) + \varphi(m') = \varphi(m + m')$ et $m + m' \in M$ car c'est un sous-module de M.
- $\varphi(M')$ est stable par multiplication scalaire : $r\varphi(m) = \varphi(rm)$ et $rm \in M$ car c'est un sous-module de M.

Montrons ensuite que $\varphi^{-1}(N')$ est un sous-module de M : on a

$$\varphi^{-1}(N') = \{m \in M \mid \varphi(m) \in N'\}$$

Cet ensemble est non vide : il contient 0_M. Soient ensuite $m, m' \in \varphi^{-1}(M)$ et $\lambda, \mu \in R$, on a

$$\varphi(\lambda m + \mu m') = \lambda\varphi(m) + \mu\varphi(m') \in N'$$

car $\varphi(m), \varphi(m') \in N'$ et que c'est un sous-module de N. On a donc $\lambda m + \mu m' \in \varphi^{-1}(N')$ par définition.

En particulier, cet exercice prouve que $\operatorname{Ker}\varphi = \varphi^{-1}(\{0\})$ et $\operatorname{Im}\varphi = \varphi(M)$ sont des sous-modules respectifs de M et de N.

† *Quelques situations fondamentales*

Exercice 5.
1. On pouvait clairement admettre que l'application "polynôme d'endomorphisme" est un morphisme d'anneaux. Je vais (beaucoup) détailler la preuve ici tout de même.

Partie 1 : L'ensemble $\mathrm{End}_k(E)$, muni de l'addition des morphismes et de la composition est un anneau.

Soient $f, g \in \mathrm{End}_k(E)$, la somme $f + g$ est l'application $E \to E$ définie par

$$\forall x \in E,\ (f + g)(x) := f(x) + g(x).$$

On vérifie facilement que $f + g$ est encore une application k-linéaire. Comme l'addition de E est associative et commutative, l'addition de $\mathrm{End}_k(E)$ est associative et commutative elle aussi. Ensuite, on note $0_{\mathrm{End}} \in \mathrm{End}_k(E)$ l'application nulle, qui envoie tout $x \in E$ sur $0_E \in E$. Pour $f \in \mathrm{End}_k(E)$, on a

$$\forall x \in E, (f + 0_{\mathrm{End}})(x) = f(x) + 0_{\mathrm{End}}(x) = f(x) + 0_E = f.$$

Donc $f + 0_{\mathrm{End}} = f$. De même, $0_{\mathrm{End}} + f = f$ et 0_{End} est un neutre dans $\mathrm{End}_k(E)$ pour la loi $+$. Ensuite, un opposé à $f \in \mathrm{End}_k(E)$ est donné par l'application $x \mapsto -f(x)$ pour $x \in E$ (il s'agit bien d'une application linéaire). Donc $(\mathrm{End}_k(E), +)$ est un groupe abélien.

Ensuite, la composition $f \circ g$ quant à elle, est l'application $E \to E$ définie par

$$\forall x \in E,\ (f \circ g)(x) = f(g(x)).$$

Là aussi, $f \circ g$ est à nouveau k-linéaire. La loi $\circ$ est associative car

$$\forall f, g, h \in \mathrm{End}_k(E), x \in E,\ ((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x).$$

Donc les application $(f \circ g) \circ h$ et $f \circ (g \circ h)$ sont égales. Ensuite, l'application $\mathrm{Id}_E : x \mapsto x$ est un neutre pour la composition. En effet, pour $f \in \mathrm{End}_k(E)$ et $x \in E$, on a

$$(f \circ \mathrm{Id}_E)(x) = f(\mathrm{Id}_E(x)) = f(x) = \mathrm{Id}_E(f(x)) = (\mathrm{Id}_E \circ f)(x)$$

Donc $f \circ \mathrm{Id}_E = f = \mathrm{Id}_E \circ f$.
ATTENTION : la loi $\circ$ n'est pas commutative (comme le produit des matrices), on doit donc montrer la distributivité à droite et à gauche. Soient $f, g, h \in \mathrm{End}_k(E)$, et $x \in E$. On a

$$\begin{aligned}
((f+g) \circ h)(x) &= (f+g)(h(x)) \\
&= f(h(x)) + g(h(x)) \\
&= (f \circ h)(x) + (g \circ h)(x) \\
&= (f \circ h + g \circ h)(x) \\
(h \circ (f+g))(x) &= h((f+g)(x)) \\
&= h(f(x) + g(x)) \\
&= h(f(x)) + h(g(x)) \\
&= (h \circ f)(x) + (h \circ g)(x) \\
&= (h \circ f + h \circ g)(x)
\end{aligned}$$

Donc $(f+g) \circ h = f \circ h + g \circ h$ et $h \circ (f+g) = h \circ f + h \circ g$.
Au total $(\mathrm{End}_k(E), +, \circ)$ est bien un anneau unitaire non commutatif.

Partie 2 : La composition dans $\mathrm{End}_k(E)$ est k-bilinéaire Déjà, on a une action de k sur $\mathrm{End}_k(E)$ par

$$\forall f \in \mathrm{End}_k(E), \lambda \in k, x \in E, \quad (\lambda.f)(x) = \lambda.(f(x))$$

(de fait, $\mathrm{End}_k(E)$ est un k-espace vectoriel pour cette action). Cette structure supplémentaire est compatible avec la composition en ce sens que, si $f, g, h \in \mathrm{End}_k(E)$ et $\lambda, \mu \in k$, on a

$$(\lambda f + \mu g) \circ h = \lambda(f \circ h) + \mu(g \circ h) \text{ et } h \circ (\lambda f + \mu g) = \lambda(h \circ f) + \mu(h \circ g)$$

Partie 3 : Fixons $u \in \mathrm{End}_k(E)$. L'application $\pi : P(X) \mapsto P(u)$ de $k[X]$ dans $\mathrm{End}_k(E)$ est un morphisme d'anneaux

On y arrive enfin. Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in k[X]$. Par définition, le polynôme $P(u)$ est défini par $\sum_{i=0}^{n} a_i u^i$, où $u^i = u \circ u \circ \ldots \circ u$ es t u composé avec lui-même i fois (et $u^0 = \mathrm{Id}_E$). Ceci a du sens car c'est une combinaison k-linéaire de puissances de u (donc d'éléments de $\mathrm{End}_k(E)$).
Par définition, on a $\pi(1) = \pi(X^0) = u^0 = \mathrm{Id}_E$. Ensuite, soient

$$P(X) = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad Q(X) = \sum_{j=0}^{m} b_j X^j$$

On a alors

$$\begin{aligned}
\pi(P(X)+Q(X)) &= \pi\left(\sum_{i=0}^{\max(m,n)}(a_i+b_i)X^i\right)\\
&= \sum_{i=0}^{\max(m,n)}(a_i+b_i)u^i\\
&= \sum_{i=0}^{n}a_iu^i+\sum_{i=0}^{m}b_iu^i\\
&= \pi(P(X))+\pi(Q(X))\\
\pi(P(X)Q(X)) &= \pi\left(\sum_{i=0}^{n}a_iX^i\right)\left(\sum_{j=0}^{m}b_jX^j\right)\\
&= \pi\left(\sum_{i=0}^{n}\sum_{j=0}^{m}a_ib_jX^{i+j}\right)\\
&= \sum_{i=0}^{n}\sum_{j=0}^{m}a_ib_ju^{i+j}\\
&= \sum_{i=0}^{n}a_iu^i\circ\sum_{j=0}^{m}b_ju^j\\
&= \pi(P(X))\circ\pi(Q(X))
\end{aligned}$$

Donc π est bien un morphisme d'anneaux.

Revenons à nos moutons Par définition, la loi de composition est définie par $P(X).x := P(u)(x) = \pi(P(X))(x)$ avec les notations précédentes.

Comme E est un k-espace vectoriel, il s'agit en particulier d'un groupe abélien. Ensuite,

- Soient $P(X), Q(X) \in k[X]$ et $x, y \in E$, on a

$$\begin{aligned}
(P(X)+Q(X)).x &= \pi(P(X)+Q(X))(x)\\
&= (\pi(P(X))+\pi(Q(X)))(x)\\
&= \pi(P(X))(x)+\pi(Q(X))(x)\\
&= P(X).x+Q(X).x
\end{aligned}$$

- Soien $P(X), Q(X) \in k[X]$ et $x \in E$, on a

$$\begin{aligned}
(P(X)Q(X)).x &= \pi(P(X)Q(X))(x)\\
&= (\pi(P(X))\circ\pi(Q(X)))(x)\\
&= \pi(P(X))(\pi(Q(X))(x))\\
&= P(X).(\pi(Q(X)).x)\\
&= P(X).(Q(X).x).
\end{aligned}$$

- Soit $x \in E$. On a $\pi(1).x = \mathrm{Id}_E(x) = x$,
- Soient $P(X) \in k[X]$ et $x, y \in E$, on a

$$P(X).(x+y) = \pi(P(X))(x+y) = \pi(P(X))(x)+\pi(P(X))(y) = P(X).x+P(X).y$$

Au final, la loi considérée donne bien une structure de $k[X]$-module sur E.

2. Par hypothèse, M est un R-module, donc en particulier un groupe abélien. On doit encore définir la multiplication scalaire par les éléments de k. On pose $\iota : k \to k[X]$ l'inclusion canonique (qui envoie $\lambda \in k$ sur le polynôme constant égal à λ). Pour $\lambda \in k$ et $x \in M$, on définit alors

$$\lambda \cdot x := \iota(\lambda).x$$

Ceci a du sens car $\iota(\lambda) \in k[X]$. (attention, on distingue le point en bas $P.x$ qui dénote l'action de $k[X]$, du point médian $\lambda \cdot x$, qui dénote l'action de k que l'on vient de définir). On montre que la loi $\cdot$ donne bien une structure de k-espace vectoriel sur M.

- Soient $\lambda, \mu \in k$ et $x \in M$. On a

$$\begin{aligned}(\lambda+\mu)\cdot x &= \iota(\lambda+\mu).x\\ &= (\iota(\lambda)+\iota(\mu)).x\\ &= \iota(\lambda).x+\iota(\mu).x\\ &= \lambda\cdot x+\mu\cdot x\end{aligned}$$

- Soient $\lambda, \mu \in k$ et $x \in M$. On a

$$\begin{aligned}(\lambda\mu)\cdot x &= \iota(\lambda\mu).x\\ &= (\iota(\lambda)\iota(\mu)).x\\ &= \iota(\lambda).(\iota(\mu).x)\\ &= \lambda\cdot(\mu\cdot x)\end{aligned}$$

- Soit $x \in M$. On a $1 \cdot x = \iota(1).x = 1.x = x$.
- Soient $\lambda \in k$ et $x, y \in M$. On a

$$\begin{aligned}\lambda\cdot(x+y) &= \iota(\lambda).(x+y)\\ &= \iota(\lambda).x+\iota(\lambda).y\\ &= \lambda\cdot x+\lambda\cdot y\end{aligned}$$

On a donc bien une structure de k-espace vectoriel sur M. Ensuite, pour $\lambda, \mu \in k$ et $x, y \in M$, on a

$$\begin{aligned}X.(\lambda x+\mu y) &= X.(\iota(\lambda).x+\iota(\mu).y)\\ &= X.\iota(\lambda).x+X.\iota(\mu).y\\ &= (X\iota(\lambda)).x+(X\iota(\mu)).y\\ &= (\iota(\lambda)X).x+(\iota(\mu)X).y\\ &= \iota(\lambda).(X.x)+\iota(\mu).(X.y)\\ &= \lambda\cdot(X.x)+\mu\cdot(X.y)\end{aligned}$$

L'action de X est donc bien une application k-linéaire comme annoncé.

3. Soit M un R-module. On munit M d'une structure de k-espace vectoriel comme à la question précédente. On note E ce k-espace vectoriel pour éviter la confusion (mais on n'oublie pas que E et M ont le même ensemble sous-jacent !). On pose également

$$\forall x \in E, u(x) := X.x$$

On a montré que u est un endomorphisme k-linéaire de E. D'après la question 1), le couple (E, u) induit une structure de $k[X]$-module sur E, définie par $P(X).x = P(u)(x)$. Soit $P(X) = \sum_{i=0}^{n} a_i X^i$. On a

$$P(u)(x) = \sum_{i=0}^{n} a_i u^i(x) = \sum_{i=0}^{n} a_i X^i.x = \left(\sum_{i=0}^{n} a_i X^i\right).x = P(X).x$$

La structure de module associée à (E, u) et la structure de départ sur M sont donc les mêmes (tous les polynômes agissent de la même manière).

4. D'abord, soit φ un isomorphisme entre les $k[X]$-modules associés à (E, u) et (E, v). Il s'agit en particulier d'une application bijective, et pour $\lambda, \mu \in k$ $x, y \in E$, on a

$$\varphi(\lambda x + \mu y) = \varphi(\iota(\lambda).x + \iota(\mu).y) = \iota(\lambda).\varphi(x) + \iota(\mu).\varphi(y) = \lambda\varphi(x) + \mu\varphi(y)$$

L'application φ est donc un endomorphisme k-linéaire bijectif de E, autrement dit un élément de $\mathrm{GL}(E)$. Ensuite, on a

$$\forall x \in E,\ (\varphi \circ u)(x) = \varphi(u(x)) = \varphi(X.x) = X.\varphi(x) = v(\varphi(x)) = (v \circ \varphi)(x)$$

Donc $\varphi \circ u = v \circ \varphi$ et $\varphi \circ u \circ \varphi^{-1} = v$: les endomorphismes u et v du k-espace vectoriel E sont donc conjugués par un élément de $\mathrm{GL}(E)$.

Réciproquement, supposons qu'il existe un élément ψ de $\mathrm{GL}(E)$ tel que $\psi \circ u \circ \psi^{-1} = v$. On a $\psi \circ u = v \circ \psi$. Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in k[X]$. On a

$$\begin{aligned}
\psi(P(X).x) &= \psi\left(\left(\sum_{i=0}^{n} a_i X^i\right).x\right) \\
&= \psi\left(\sum_{i=0}^{n} a_i (X^i.x)\right) \\
&= \psi\left(\sum_{i=0}^{n} a_i u^i(x)\right) \\
&= \sum_{i=0}^{n} a_i \psi(u^i(x)) \\
&= \sum_{i=0}^{n} a_i v^i(\psi(x)) \\
&= \sum_{i=0}^{n} a_i X^i.\psi(x) = P(X).\psi(x)
\end{aligned}$$

Comme on sait déjà que $\psi(x + y) = \psi(x) + \psi(y)$ pour $x, y \in E$ par hypothèse (ψ est k-linéaire), on obtient bien que ψ est un morphisme de $k[X]$-modules. Comme on sait par ailleurs que ψ est bijective, on obtient bien que les $k[X]$-modules induits par (E, u) et (E, v) sont isomorphes.