Correction séance 3 (28 janvier)

Feuille de TD 1

Exercice 11.
1. Pour $r, r' \in R$ et $m, m' \in M$, on a
   - $1.m = f(1).m = 1.m = m$
   - $(rr').m = f(rr').m = (f(r)f(r')).m = f(r).(f(r').m) = r(r'.m)$
   - $(r + r').m = f(r + r').m = (f(r) + f(r')).m = f(r).m + f(r').m = r.m + r'.m$
   - $r.(m + m') = f(r).(m + m') = f(r).m + f(r).m' = r.m + r.m'$.

2. Pour $m, m' \in M$ et $r \in R$, on a

$$\varphi(r.m + m') = \varphi(f(r).m + m') = f(r).\varphi(m) + \varphi(m') = r.\varphi(m) + \varphi(m')$$

et donc φ est bien un morphisme de $\mathbb{R}$-modules.

3. On a vu dans l'exercice précédent que tout anneau est une $\mathbb{Z}$-algèbre, ce qui entraîne que tout R-module admet une structure de $\mathbb{Z}$-module, autrement dit est un groupe abélien, ce qui était déjà présent dans la définition de module.

Exercice 12.
1.Pour $P, Q \in R$ et $x, y \in E$, on a
   - $1.x = 1(u)(x) = Id(x) = x$
   - $(PQ).x = (PQ)(u)(x) = (P(u) \circ Q(u))(x) = P(u)(Q(u)(x)) = P.(Q.x)$
   - $(P + Q).x = (P(u) + Q(u))(x) = P(u)(x) + Q(u)(x) = P.x + Q.x$
   - $P.(x + y) = P(u)(x + y) = P(u)(x) + P(u)(y) = P.x + P.y$ car $P(u)$ est un endomorphisme (linéaire) de E.

2. Comme R est une $\Bbbk$-algèbre, tout R-module est un $\Bbbk$-module par l'exercice précédent. Ensuite, on a

$$X.(\lambda v + v') = \lambda X.v + X.v'$$

donc $u : v \mapsto X.v$ est bien un endomorphisme de $\Bbbk$-espace vectoriel.

3. Cela découle directement de la question précédente : une structure de R-module sur M revient à la donnée d'un $\Bbbk$-espace vectoriel E, où l'on déclare que l'action de X est celle d'un endomorphisme linéaire u de M (l'action de X^n est alors celle de $u^n = u \circ u \circ u \cdots \circ u$, étendue par linéarité).

4. Montrons le lemme suivant

Lemme. Un morphisme de R-modules $\varphi : (E, u) \to (E, v)$ est une application $\Bbbk$-linéaire $\varphi : E \to E$ respectant $\varphi \circ u = v \circ \varphi$.

Démonstration. Soit $\varphi : (E, u) \to (E, v)$ un morphisme de R-modules. Comme R est une $\Bbbk$ algèbre, φ doit (par l'exercice précédent) être un morphisme de $\Bbbk$-espace vectoriel. Ensuite, on a en particulier

$$\varphi(X.w) = \varphi(u(w)) = X.\varphi(w) = v(\varphi(w))$$

donc $v \circ \varphi = \varphi \circ u$.
Réciproquement, si $\varphi \circ u = v \circ varphi$, on a

$$v^n \circ \varphi = \varphi \circ u^n \quad \text{et} \quad P(v) \circ \varphi = \varphi \circ P(u) \forall P \in R$$

Et donc $\varphi(P.w) = (\varphi \circ P(u))(w) = (P(v) \circ \varphi)(w) = P.(\varphi(w))$, et φ est bien un morphisme de R-modules. □

À présent, $\varphi : (E,u) \to (E,v)$ est un isomorphisme de R-modules si et seulement si φ est bijectif, donc si et seulement si c'est un isomorphisme de $\Bbbk$-espace vectoriels (autrement dit, un élément de $\mathrm{Gl}(E)$). On a donc que $(E,u) \to (E,v)$ sont isomorphes si et seulement si il existe $\varphi \in \mathrm{Gl}(E)$ tel que $\varphi \circ u = v \circ \varphi$, i.e $\varphi \circ u \circ \varphi^{-1} = v$ ce qui est bien le résultat attendu.

5.a) L'application $P \mapsto P.v$ est un morphisme de R-modules de R vers E, surjectif justement parce que E est monogène. Son noyau est un sous-module de R, donc un idéal de R, donc de la forme (P_0) pour un certain polynôme unitaire P_0 (car R est principal). Par le premier théorème d'isomorphisme, on a donc $E \simeq R/(P_0)$ pour un certain polynôme unitaire $P_0 \in \Bbbk[X]$.
b) Par définition, P_0 engendre le noyau de $P \mapsto P.v = P(u)(v)$, comme (E,u) est engendré (comme R-module) par v, on a

$$P(u)(v) = 0 \Leftrightarrow P(u) = 0 \in \mathrm{End}_{\Bbbk}(E)$$

Donc P_0 engendre en fait l'idéal des polynômes annulateurs de u sur E, c'est la définition du polynôme minimal.
c). Notons B la famille $v, u(v), \cdots, u^{n-1}(v)$.
La famille F est libre car

$$\sum_{i=0}^{n-1} \lambda_i u^i(v) = 0 \Rightarrow \left(\sum_{i=0}^{n-1} \lambda_i X^i\right)(u)(v) = 0$$

Donc $Q(X) = \sum_{i=0}^{n-1} \lambda_i X^i$ est un polynôme annulateur de u de degré $n-1$, donc $Q = 0$ (car le polynôme minimal P_0 doit diviser Q) : les λ_i sont tous nuls et F est libre.
Ensuite, F est génératrice : dire que (E,u) est engendré par v comme R-module signifie que tout élément de E s'écrit $Q(u)(v)$ pour un certain $Q \in R$. En écrivant la division euclidienne $Q = DP + \widetilde{Q}$, on obtient que

$$Q(u)(v) = (DP + \widetilde{Q}(u))(v) = \widetilde{Q}(u)(v)$$

comme $\deg \widetilde{Q} < n$, cet élément est bien une combinaison linéaire de la famille F, qui est donc génératrice.
d). Le polynôme P_0 est le polynôme minimal d'un endomorphisme u d'un $\Bbbk$-ev de dimension n, comme $\deg P_0 = n$, par le théorème de Cayley Hamilton (P_0 divise le polynôme caractéristique de u), on a bien que P_0 est le polynôme caractéristique de u.

Feuille de TD 1bis

Exercice 1.
1. Soit $y = p(x) \in \mathrm{Im}\, p$, si y est en plus dans $\mathrm{Ker}\, p$, on a $p(y) = 0$, mais par hypothèse, $p(y) = p(p(x)) = p(x) = y = 0$, d'où le résultat.
2. Si $y = p(x) \in \mathrm{Im}\, p$, alors $p(y) = p(p(x)) = p(x) = y$, réciproquement, si $p(y) = y$, alors $y \in \mathrm{Im}\, p$ par définition (puisque c'est l'image de y).
3. On a $p(x - p(x)) = p(x) - p(p(x)) = p(x) - p(x) = 0$.
4. Pour tout $x \in M$, on a $x = x - p(x) + p(x)$, avec $x - p(x) \in \mathrm{Ker}\, p$ et $p(x) \in \mathrm{Im}\, p$, donc $\mathrm{Ker}\, p + \mathrm{Im}\, p = M$, et cette somme est directe d'après la question 1.

Exercice 2.
1. Si G est un supplémentaire de F, alors $F \cap G = \{0\}$ et tout $x \in E$ s'écrit de manière unique sous la forme $f + g$ avec $f \in F$ et $g \in G$.
On considère la restriction de $E \twoheadrightarrow E/F$ à G, on obtient un morphisme $\varphi : G \to E/F$, envoyant g sur $\overline{g}$. Soit $\overline{x} \in E/F$.
Comme $E = F \oplus G$, on a $x = f + g$, donc $\overline{x} = \overline{f} + \overline{g} = \overline{g}$ et φ est surjective. Ensuite, on a $g \in \mathrm{Ker}\ \varphi$ si et seulement si $\overline{g} = 0$, autrement dit $g \in F$, mais alors $g \in G \cap F = \{0\}$, donc φ est injective : c'est un isomorphisme.

2.a) L'intersection $G \cap \mathrm{Ker}\, \partial$ est triviale : si P est un polynôme constant, alors $P(0) = 0$ entraîne $P = 0$. Ensuite, soit $P(X) \in \Bbbk[X]$, on a

$$P(X) = (P(X) - P(0)) + P(0)$$

qui est bien une décomposition sur $G + \operatorname{Ker}\partial$, d'où la somme directe.
b) Par le théorème d'isomorphisme, on sait que $\mathbb{k}[X]/\operatorname{Ker} p \simeq \operatorname{Im}\partial = \mathbb{k}[X]$, par la question 1, ceci est isomorphe à G, qui est donc un sous-espace strict de $\mathbb{k}[X]$ (il ne contient pas le polynôme 1), qui lui est pourtant isomorphe.

Exercice 3.
1. On a $u : E \to E$, en composant par la projection $p : E \to E/F$, on obtient un morphisme $p \circ u : E \to E/F$. Soit $x \in f$, on a $u(x) \in f$, donc $p(u(x)) = 0$ et $x \in \operatorname{Ker} p \circ u$, donc $F \subset \operatorname{Ker} p \circ u$, d'où une factorisation $\overline{u} : E/F \to E/F$, envoyant $\overline{x}$ sur $\overline{u(x)}$.

2. Par définition, on a $\overline{u} \circ p = p \circ u$, donc p induit un morphisme $(E, u) \to (E/F, \overline{u})$ qui est un morphisme de $\mathbb{k}[X]$-module. Ce morphisme est surjectif, et son noyau est $(F, u_{|F})$, d'où le résultat.

3. Commençons par montrer que $\overline{\mathcal{E}}$ est une famille libre de E/F : soit une combinaison linéaire

$$0 = \sum_{i=r+1}^{n} \lambda_i \overline{e_i} = \overline{\sum_{i=r+1}^{n} \lambda_i e_i}$$

(la dernière égalité vient du fait que la projection $E \to E/F$ est une application linéaire). Ceci équivaut à $\sum_{i=r+1}^{n} \lambda_i e_i \in F$, mais comme $\operatorname{Vect}(e_{r+1}, \cdots, e_n)$ est un supplémentaire de F, ceci entraine $\sum_{i=r+1}^{n} \lambda_i e_i = 0$, d'où $\lambda_i = 0$ car $\mathcal{E}$ est une base par hypothèse.
Ensuite, on doit montrer que $\overline{\mathcal{E}}$ est une famille génératrice : soit $\overline{x} \in E/F$, on sait que x s'écrit sous la forme $x = \sum_{i=1}^{r} \lambda_i f_i + \sum_{i=r+1}^{n} \lambda_i e_i$, et on a

$$\overline{x} = \overline{\sum_{i=1}^{r} \lambda_i f_i + \sum_{i=r+1}^{n} \lambda_i e_i} = \sum_{i=1}^{r} \lambda_i \overline{f_i} + \sum_{i=r+1}^{n} \lambda_i \overline{e_i} = \sum_{i=r+1}^{n} \lambda_i \overline{e_i}$$

donc x est bien engendré par $\overline{\mathcal{E}}$, qui forme donc une base de E/F.

4. Soit $f_i \in \mathcal{F}$, comme F est u-stable, on a $u(f_i) \in F$, donc

$$u(f_j) = \sum_{i=1}^{r} A_{i,j} f_j + \sum_{i=r+1}^{n} 0 e_i$$

Soit ensuite $e_j \in \mathcal{E}$, on a $\overline{u(e_j)} = \overline{u}(\overline{e_j})$, donc le coefficients de $u(e_j)$ en e_i est le même que celui de $\overline{u}(\overline{e_j})$ en $\overline{e_i}$. D'où le résultat voulu.

Exercice 4.
1. Premièrement, p est un morphisme :

$$p(rx + x') = (rx + x').m = r.(x.m) + x'.m = r.p(x) + p(x')$$

par définition, on a $\operatorname{Im} p = \{r.m \mid r \in R\}$, donc p est surjectif si et seulement si M est monogène.
2. Si $a \in I$ est dans l'idéal annulateur de M, on a en particulier $a.m = 0 = p(a)$ par hypothèse. Réciproquement si $a \in \operatorname{Ker} p$, alors $p(a) = a.m = 0$, mais alors, pour $m' \in M$, il existe $r \in R$ tel que $m' = r.m$ et on a

$$a.m' = a.(r.m) = r.(a.m) = r.0 = 0$$

donc a est dans l'idéal annulateur de M.
3. C'est le théorème d'isomorphisme appliqué au morphisme p.