Correction TD1

Exercice 1.
(a) Ce n'est pas un $\Bbbk$-module : il ne contient pas 0 car celui-ci n'est pas un polynôme de degré 4.
(b) Notons M l'ensemble des polynômes de degré au plus 4. Premièrement, M contient 0. Ensuite, pour P, Q de degré au plus 4, et $\lambda, \mu \in \Bbbk$, on sait que $\lambda P + \mu Q$ est aussi de degré au plus 4 car

$$\deg(\lambda P + \mu Q) \leqslant \max(\deg(P), \deg(Q))$$

Donc M est stable par combinaison linéaire : il s'agit d'un sous-module de $\Bbbk[X]$.
(c) Ce n'est pas un $\Bbbk$-module : il ne contient pas 0.
(d) Si on ajoute 0 ça se complique : si $\Bbbk \neq \mathbb{F}_2$, alors $\Bbbk$ contient un élément λ différent de 1 et de 0. Dans ce cas, le polynôme λX est une combinaison linéaire de polynômes unitaire qui n'est pas unitaire : l'ensemble étudié n'est pas un sous-module de $\Bbbk[X]$. Si $k = \mathbb{F}_2$, l'ensemble étudié est alors égal à $\Bbbk[X]$, il s'agit donc bien d'un $\Bbbk$-module.
(e) Ce n'est pas un sous-module : la différence de deux polynômes de degré pair peut ne pas être de degré pair : par exemple prenons $X^2 + X$ et X^2, qui sont de degré pair.

$$(X^2 + X) - X^2 = X$$

ce dernier polynôme n'est pas de degré pair.

Exercice 2. Soit I un sous-R-module de R, il doit être stable par somme :

$$\forall x, y \in I, x + y \in I$$

et il doit être stable par multiplication scalaire (en particulier $x \in I \Rightarrow -x \in I$, donc I est un sous-groupe de R) :

$$\forall x \in I, r \in R,\ r.i = ri \in I$$

C'est bien la définition d'un idéal de R.

Exercice 3. Pour tout $r \in R$, on a $r = r.1_R$. Si $f : R \to R$ est un morphisme de R-module, on doit avoir

$$f(r) = f(r.1_R) = rf(1_R)$$

Donc f ne dépend que de $f(1_R)$. Par ailleurs, pour tout $r_0 \in R$, en posant $f(r) = rr_0$, on obtient bien un morphisme de R-module car

$$f(r.r' + r'') = (r.r' + r'')r_0 = rr'r_0 + r''r_0 = rf(r') + f(r'')$$

Donc les morphismes de modules $f : R \to R$ sont en bijection avec R (par le choix de $f(1_R)$).
(On voit une grosse différence avec les morphismes d'anneaux.)

Exercice 4. De façon générale, les ensemble de fonctions régulières auront toujours une structure de module (en fait d'algèbre, mais on verra ça un peu plus tard).
Ici, on sait que 0 est une fonction constante, donc lisse, et comme on a $(f + g)' = f' + g'$ et $(rf)' = rf'$, la dérivabilité d'une somme ou d'une multiplication scalaire est la même que celle des facteurs, donc $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ est bien stable par somme et multiplication scalaire : il s'agit d'un $\mathbb{R}$-module.
Ensuite, ∂ forme bien un morphisme de $\mathbb{R}$-module : pour $r \in \mathbb{R}, f, g \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ on a

$$\partial(rf + g) = (rf + g)' = rf' + g' = r\partial(f) + \partial(g)$$

de plus, comme la dérivée d'une fonction infinment dérivable est elle-même infiniment dérivable, le morphisme ∂ est bien à valeur dans $\mathcal{C}^\infty(\mathbb{R},\mathbb{R})$.
Une fonction f est dans $\operatorname{Ker}\partial$ si et seulement si $\partial(f)=f'=0$, autrement dit si f est constante, donc $\operatorname{Ker}\partial$ est un $\mathbb{R}$-module de dimension 1 (engendré par la fonction constante 1).
Pour l'image, on a

$$f\in\operatorname{Im}\partial\Leftrightarrow\exists F\in\mathcal{C}^\infty(\mathbb{R},\mathbb{R})\mid F'=f$$

autrement dit, $\operatorname{Im}\partial$ est formé des fonctions admettant des primitives, ce qui est le cas de toute fonction continue (en particulier, de toute fonction $\mathcal{C}^\infty$), donc $\operatorname{Im}\partial=\mathcal{C}^\infty(\mathbb{R},\mathbb{R})$.
On constate que l'on n'a plus du tout $\mathcal{C}^\infty(\mathbb{R},\mathbb{R})=\operatorname{Ker}\partial\oplus\operatorname{Im}\partial$ comme en dimension finie...

Exercice 5.
1. Par définition, on a

$$E\cap(F+G)=\{f+g\in F+G\mid f+g\in E\}\quad\text{et}\quad(E\cap F)+(E\cap G)=\{f+g\in F+G\mid f\in E\text{ et }g\in E\}$$

Comme E est un module, si $f,g\in E$, en particulier $f+g\in E$, donc $(E\cap F)+(E\cap G)\subset E\cap(F+G)$, mais pour la réciproque, il faudrait avoir quelque chose comme $f+g\in E\Rightarrow f,g\in E$, ce qui est faux :
On se place dans $\mathbb{R}^2$, et on pose $E=\operatorname{Vect}\binom{1}{0},F=\operatorname{Vect}\binom{1}{1},G=\operatorname{Vect}\binom{1}{-1}$, on a $E\cap F$ et $E\cap G=\{0\}$, donc $(E\cap F)+(E\cap G)=\{0\}$. Cependant, on a $\binom{1}{0}=\frac{1}{2}\left(\binom{1}{-1}+\binom{1}{1}\right)$, donc $E\subset F+G$ et $E\cap(F+G)$ est non trivial.

2. Ici, on a $E\cap F\subset F$, donc $(E\cap F)+(E\cap G)\subset F+(E\cap G)$, de plus $E\cap F,E\cap G\subset E$ entraîne $(E\cap F)+(E\cap G)\subset E$, d'où

$$(E\cap F)+(E\cap G)\subset E\cap(F+(E\cap G))$$

Réciproquement, un élément de $E\cap(F+(E\cap G))$ est de la forme $f+g$, avec $f\in F,g\in E\cap G$ et $f+g\in E$. Mais comme $f+g,g\in E$, on a $f+g-g=f\in E$, donc f appartient en fait à $E\cap F$, d'où

$$E\cap(F+(E\cap G))\subset(E\cap F)+(E\cap G)$$

Donc les deux ensembles sont en fait égaux.

Exercice 6.
On rappelle à toute fin utile que

$$\operatorname{Vect}(A)=\bigcap_{\substack{F\leqslant E\\A\subset F}}F=\left\{\sum_{a\in A}\lambda_a a\right\}$$

$\operatorname{Vect}(A)$ est le plus petit sous-espace vectoriel de E contenant A, c'est aussi l'ensemble des combinaisons linéaires (finies) d'éléments de A.
1. Comme $A,B\subset A\cup B$, on a $\operatorname{Vect}(A)\cup\operatorname{Vect}(B)\subset\operatorname{Vect}(A\cup B)$, mais la réciproque est en général fausse : dans $\mathbb{R}^2$, considérant $A=\binom{1}{0}$ et $B=\binom{0}{1}$, on a que $A\cup B$ est une base, donc $\operatorname{Vect}(A\cup B)=\mathbb{R}^2$, et pourtant $\operatorname{Vect}(A)\cup\operatorname{Vect}(B)$ est une union de deux droites, jamais égale à tout le plan...

2. À nouveau, comme $A\cap B\subset A,B$, on a $\operatorname{Vect}(A\cap B)\subset\operatorname{Vect}(A)\cap\operatorname{Vect}(B)$, mais à nouveau la réciproque est fausse : dans R^2, pour

$$A=\left\{\binom{1}{0},\binom{0}{1}\right\}\quad\text{et}\quad B=\left\{\binom{1}{1},\binom{-1}{1}\right\}$$

On a que A et B sont deux bases de $\mathbb{R}^2$, avec $A\cap B=\varnothing$, donc $\operatorname{Vect}(A)\cap\operatorname{Vect}(B)=\mathbb{R}^2\cap\mathbb{R}^2=\mathbb{R}^2$ et $\operatorname{Vect}(A\cap B)=\{0\}$.

3. Là encore, on a $A\subset\operatorname{Vect}A$ donc $\operatorname{Vect}A\subset\operatorname{Vect}(\operatorname{Vect}(A))$. Mais ici on a la réciproque, revenons à la définition : $\operatorname{Vect}(A)$ est le plus petit sev de E qui contient A, et $\operatorname{Vect}(\operatorname{Vect}(A))$ est le plus petit sev de E qui contient $\operatorname{Vect}(A)$, or $\operatorname{Vect}A$ contient $\operatorname{Vect}(A)$ et c'est un sev, donc il contient $\operatorname{Vect}(\operatorname{Vect}(A))$: $\operatorname{Vect}(\operatorname{Vect}(A))\subset\operatorname{Vect}(A)$ et on a terminé.

Exercice 7. Montrons que $\varphi(M')$ est un sous-module de N : on a

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

- $\varphi(M')$ 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

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

Pour $m, m' \in \varphi^{-1}(M)$ et $r \in R$, on a

$$\varphi(rm + m') = r\varphi(m) + \varphi(m') \in N'$$

car $\varphi(m), \varphi(m') \in N'$ et que c'est un sous-module de N.

Exercice 8.

1. Soit F une primitive de f, on a $\varphi(f)(x) = F(x + 1) - F(x - 1)$. Comme F est une fonction continue, la fonction $\varphi(f)$ est elle aussi continue, donc φ est bien à valeurs dans $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$, et φ est linéaire par linéarité de l'intégrale.

2. Une fonction f est dans $\operatorname{Ker}\varphi$ si et seulement si

$$\forall x \in \mathbb{R}, F(x - 1) = F(x + 1)$$

autrement dit, si les primitives de f sont 2-périodiques, en particulier, si on part d'une fonction F 2 périodique (par exemple, $F(x) = \sin(\pi x)$), on a $F'(x) = \pi\cos(\pi x)$ est non nulle et dans le noyau de φ, qui n'est donc pas injective.
Pour la surjectivité, on remarque que $\varphi(f)(x) = F(x+1) - F(x-1)$ est une fonction $\mathcal{C}^1$ comme primitive d'une fonction continue), donc $\operatorname{Im}\varphi \subset \mathcal{C}^1(\mathbb{R}, \mathbb{R})$, et φ n'est pas surjective.

Exercice 9.

1. Soient $a, b \in I$, on a par hypothèse

$$\forall m \in M, am = 0 = bm$$

donc en particulier $(a - b)m = am - bm = 0$ et $a - b \in I$, ensuite, pour $r \in R$, $(ra).m = r.(am) = 0$, donc $ra \in I$, qui est bien un idéal de R.

2. Soit $k \in \mathbb{Z}$, k est dans l'annulateur de $\mathbb{Z}$ si et seulement si

$$\forall n \in \mathbb{Z}, kn = 0$$

ce qui entraîne bien sur $k = 0$ car $\mathbb{Z}$ est intègre, donc l'annulateur de $\mathbb{Z}$ est (0).

3. Soit $n \in \mathbb{Z}$, et calculons l'annulateur de $\mathbb{Z}/n\mathbb{Z}$. Comme $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\overline{1}$, on a que $k \in \mathbb{Z}$ est annulateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si

$$k.\overline{1} = \overline{k} = 0 \Leftrightarrow k \equiv 0[n] \Leftrightarrow n|k \Leftrightarrow k \in n\mathbb{Z}$$

Donc l'annulateur de $\mathbb{Z}/n\mathbb{Z}$ est $n\mathbb{Z}$.

3. Un élément $k \in \mathbb{Z}$ est annulateur de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ si et seulement si

$$\forall (a, b, c) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad k(a, b, c) = (ka, kb, kc) = (0, 0, 0)$$

autrement dit si k est annulateur de $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$. Autrment dit, on obtient que l'annulateur de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est donné par

$$2\mathbb{Z} \cap 3\mathbb{Z} \cap 4\mathbb{Z} = (PPCM(2, 3, 4))\mathbb{Z} = 12\mathbb{Z}$$

Exercice 10. On note $\sum_{i=1}^{n} g$ la somme de n fois g. On a, pour m, n positifs

- $1.g = \sum_{i=1}^{1} g = g$
-
$$(mn).g = \sum_{i=1}^{mn} g = \sum_{i=1}^{m} \left(\sum_{i=1}^{n} g \right) = m.(n.g)$$
-
$$(m+n).g = \sum_{i=1}^{m+n} g = \sum_{i=1}^{m} g + \sum_{i=m+1}^{m+n} g = \sum_{i=1}^{m} g + \sum_{i=1}^{n} g = m.g = n.g$$
-
$$m.(g+g') = \sum_{i=1}^{m} g + g' = \sum_{i=1}^{m} g + \sum_{i=1}^{m} g' = m.g + m.g'$$

Il reste à généraliser ces relations au cas $m, n \in \mathbb{Z}$ en mettant des signes moins quand c'est nécessaire.

Exercice 11.

1.a) On sait déjà que $(S, +)$ est un groupe abélien, il reste à vérifier que $\times_S$ le munit bien d'une structure d'anneau commutatif unitaire :

- L'associativité, la commutativité et l'unitarité sont déjà inclues dans la définition de R-algèbre.
- La distributivité à gauche et à droite est un cas particulier de la R-bilinéarité.

On a donc bien une structure d'ACU $(S, +, \times_S)$.

b). Premièrement on a $f(1_R) = 1_R.1_S = 1_S$ grâce à la définition de R-module. Le reste provient de la R-bilinéarité. Soient $r, r' \in R$, on a

$$f(r+r') = (r+r').1_S = r.1_S + r'.1_S = f(r) + f(r')$$

$$f(r) \times_S f(r') = (r.1_S) \times_S (r'.1_S) = rr'(1_S \times_S 1_S) = (rr').1_S = f(rr')$$

Donc f donne bien un morphisme d'anneaux $R \to S$.

2. On sait d'emblée que $(S, +)$ est un groupe abélien, ensuite, on a

- $1_R.s = f(1)s = s$
- $(r+r').s = f(r+r')s = f(r)s + f(r')s = r.s + r'.s$
- $r.(s+s') = f(r)(s+s') = f(r)s + f(r)s' = r.s + r.s'$.
- $(rr').s = f(rr')s = f(r)f(r') = r.(r'.s)$

Donc S est bien un R-module. Le fait que S soit alors une S-algèbre en est une conséquence immédiate le seul point non trivial est

$$r.(ss') = (r.s)s' = s(r.s')$$

mais il découle de

$$r.(ss') = f(r)ss', \quad (r.s)s' = (f(r)s)s', \quad s(r.s') = s(f(r)s')$$

3,4 A chaque fois, on a un sous-anneau, donc un morphisme d'anneau d'inclusion, qui donne une structure d'algèbre $(R \subset R[X], \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C})$

5. Soit $f : \mathbb{Z} \to R$ un morphisme d'anneaux, pour $n \in \mathbb{Z}$, on a

$$f(n) = f(1+1+1+\cdots+1) = f(1) + f(1) + f(1) + \cdots + f(1) = 1_R + 1_R + 1_R + \cdots + 1_R$$

et cette application est clairement un morphisme d'anneaux : il y a un unique morphisme $f : \mathbb{Z} \to R$ donné par $f(n) = n.1_R$. Comme un morphisme d'anneau $\mathbb{Z} \to R$ équivaut à une structure de $\mathbb{Z}$-algèbre sur R, il existe une unique structure de $\mathbb{Z}$-algèbre sur tout anneau (commutatif unitaire).

Exercice 12.

1. On sait déjà que $(M,+)$ est un groupe abélien. Ensuite, pour $r,r' \in R$ et $m,m' \in M$, on a

- $1.m = f(1).m = 1.m = m$
- $(rr').m = f(rr').m = (f(r)f(r')).m = f(r).(f(r').m) = r(r'.m)$
- $(r+r').m = f(r+r').m = (f(r)+f(r')).m = f(r).m + f(r').m = r.m + r'.m$
- $r.(m+m') = f(r).(m+m') = f(r).m + f(r).m' = r.m + r.m'$.

Donc M est bien muni d'une structure de R-module.

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 13.

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. $\square$

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.