Correction TD 2

Exercice 1. Soient $P, Q \in R[X]$ et $\lambda \in \Bbbk$, on a

$$\deg(P+Q) \leqslant \min(\deg P, \deg Q) \quad \text{et} \quad \deg(\lambda P) \leqslant \deg P$$

Donc, si $\{P_1, \cdots, P_m\}$ est une famille finie de polynôme, de degré maximal n, le sous-module de $R[X]$ qu'elle engendre ne contient que des polynômes de degré au plus n, donc ne peut être égal à $R[X]$.

Exercice 2. On doit montrer que M n'admet pas de base finie. S'il est libre de rang 1, il admet une base de la forme $\{P(X,Y)\}$. Dans ce cas, M est alors monogène, mais on sait que ceci est faux.
Si M est libre de rang $m \geqslant 2$, alors il admet une base de la forme $\{P_1(X,Y), \cdots, P_m(X,Y)\}$. Mais dans ce cas, on a

$$P_1(X,Y)P_2(X,Y) = P_2(X,Y)P_1(X,Y)$$

ceci donne une combinaison linéaire (à coefficients dans $\mathbb{C}[X,Y]$) nulle et non triviale : notre base n'est pas une base ! Donc M n'est pas un module libre, même si c'est un sous-module du $\mathbb{C}[X,Y]$-module libre $\mathbb{C}[X,Y]$. Un sous-module d'un module libre n'est pas forcément libre (c'est vrai si l'anneau de base est principal, ce qui n'est justement pas le cas de $\mathbb{C}[X,Y]$).

Exercice 3. (a). Considérons dans $\mathbb{Z}^2$ la famille $\left\{\binom{1}{0}, \binom{0}{2}, \binom{0}{3}\right\}$, il est clair que cette famille ne contient pas de base, et pourtant $\binom{0}{3} - \binom{0}{2} = \binom{0}{1}$ donc elle est génératrice.
(b). Considérons dans $\mathbb{Z}^2$ la famille $\left\{\binom{2}{0}\right\}$, il s'agit d'une famille libre comme singleton (non nul) dans un module libre, mais qui ne peut pas être complété en une base, en effet pour $\binom{x}{y} \in \mathbb{Z}^2$, on a

$$\det \begin{pmatrix} 2 & x \\ 0 & y \end{pmatrix} = 2y \notin \{\pm 1\}$$

Exercice 4. Un supplémentaire de N serait un module libre de rang 1, donc engendré par un certain vecteur $\binom{x}{y}$, dire que $N' = (x,y)\mathbb{Z}$ est un supplémentaire de N revient à dire que le générateur de N et $\binom{x}{y}$ forment une base de N.
Si $N = (1,1)\mathbb{Z}$, on calcule

$$\det \begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix} = y - x$$

qui devrait être égal à ± 1, on pose donc $\binom{x}{y} = \binom{0}{1}$, qui convient : $N' = (0,1)\mathbb{Z}$ est un supplémentaire de N.
Si $N = (2,3)\mathbb{Z}$, on calcule

$$\det \begin{pmatrix} 2 & x \\ 3 & y \end{pmatrix} = 2y - 3x$$

qui devrait être égal à ± 1, on pose donc $\binom{x}{y} = \binom{1}{1}$, qui convient : $N' = (1,1)\mathbb{Z}$ est un supplémentaire de N.
Si $N = (6,1)\mathbb{Z}$, on calcule

$$\det \begin{pmatrix} 6 & x \\ 1 & y \end{pmatrix} = 6y - x$$

qui devrait être égal à ± 1, on pose donc $\binom{x}{y} = \binom{5}{1}$, qui convient : $N' = (5,1)\mathbb{Z}$ est un supplémentaire de N.
On remarque que l'on a pas du tout unicité du supplémentaire : $(0,1)\mathbb{Z}$ est supplémentaire de $(1,1)\mathbb{Z}$, qui est par ailleurs supplémentaire à $(2,3)\mathbb{Z}$.

Exercice 5.
1. Si $M \neq 0$ est un $\Bbbk$-espace vectoriel de dimension $\geqslant 2$, alors tout vecteur non nul y engendre un sous-espace vectoriel de dimension 1, donc un sous-module propre, donc M n'est pas simple. Ensuite si M est de dimension 1, tout sous-espace de M est de dimension 0 ou 1 : c'est soit l'espace vectoriel trivial $\{0\}$, soit M tout entier. Autrement dit M est simple.

2. Soit $M \leqslant \mathbb{Z}/p\mathbb{Z}$ un sous module non trivial, il contient un élément $\overline{k}$ non nul, mais comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il existe $k' \in \mathbb{Z}$ tel que $k'\overline{k} = \overline{k'k} = \overline{1}$, donc $\overline{1} \in M$. Comme $\mathbb{Z}/p\mathbb{Z}$ est engendré par $\overline{1}$ comme $\mathbb{Z}$-module, on a bien $M = \mathbb{Z}/p\mathbb{Z}$, qui est donc simple.

3. Posons I l'annulateur de M, défini par

$$r \in I \Leftrightarrow \forall m \in M, r.m = 0$$

On va montrer que R/I est un corps, soit $r+I \in R/I$ un élément non nul (autrement dit, soit $r \in R \setminus I$). Comme $r \notin I$, il existe un $m \in M$ tel que $r.m \neq 0$, et comme M est simple, il est engendré par $r.m$ et il existe $a \in R$ tel que $a.(r.m) = (ar).m = m$, donc $(ar-1).m = 0$. Comme $m \neq 0$ et M est simple, ceci entraine $(ar-1)M = 0$ et $ar - 1 \in I$, autrement dit $ar = 1$ dans R/I, donc r y est inversible, d'où le résultat.

4. Soit $m \neq 0$ dans M, par hypothèse $\langle m \rangle = M$. On considère l'application $R \to M$ donnée par $r \mapsto r.m$, il s'agit d'un morphisme de module, surjectif car m engendre M, et de noyau I (par définition). On conclut par le premier théorème d'isomorphisme.

5. Supposons que φ est non nul, on sait que $\operatorname{Ker}\varphi$ est un sous-module de M, comme $\varphi \neq 0$, $\operatorname{Ker}\varphi \neq M$ donc $\operatorname{Ker}\varphi = \{0\}$ et φ est injectif. De même, $\operatorname{Im}\varphi$ est un sous-module de M', différent de $\{0\}$ car φ est non nul, donc $\operatorname{Im}\varphi = M'$ et φ est surjectif. Donc φ est un isomorphisme.

Exercice 6. Soit $\widetilde{M}$ un sous-module de M/N, comme p est un morphisme de modules, $p^{-1}(\widetilde{M})$ est un sous-module de M, qui contient N car $\widetilde{M}$ contient 0. Soit maintenant $M' \subset M$ un sous-module qui contient N, son image $p(M')$ est un sous-module de M/N. Comme p est une surjection, on a $p(p^{-1}(\widetilde{M})) = \widetilde{M}$, et enfin, on a

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

mais comme $N \subset M'$, $x - m' \in N \Rightarrow x - m' \in M' \Rightarrow x \in M'$ car M' est un sous-module, donc $p^{-1}(p(M')) = M'$ comme annoncé.

Exercice 7. L'application φ est un morphisme de modules, comme composée de deux morphismes : l'inclusion $M \hookrightarrow M+N$ et le quotient $M+N \twoheadrightarrow {}^{M+N}/_{N}$. Ce morphisme de modules est surjectif, en effet pour $m+n \in M+N$, on a $\overline{m+n} = \overline{m} + \overline{n} = \overline{m} = \varphi(m)$, il reste à décrire le noyau de ce morphisme :

$$\operatorname{Ker}\varphi = \{m \in M \mid \overline{m} = 0\} = \{m \in M \mid m \in N\} = M \cap N$$

et on conclut par le premier théorème d'isomorphisme.

Exercice 8. On commence par montrer que la définition de $\varphi(m+P)$ ne dépend pas du choix d'un représentant. Soit $m + P = m' + P$, autrement dit $m - m' \in P \subset N$, donc $m + N = m' + N$ donc $\varphi(m+P)$ est bien défini, il s'agit clairement d'un morphisme de modules :

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

Ce morphisme est surjectif : si m est un représentant de $m+N$, alors $m+P$ est un antécédent de $m+N$ par φ. Enfin, $m+P$ est dans le noyau de ce morphisme si et seulement si $m \in N$, autrement dit si $m+P \in N/P$, d'où le résultat.

† *Propriétés universelles*

Exercice 9.
1. Supposons qu'un tel morphisme φ existe, soit $e \in E$ et $\varphi(e) := (m, n)$, on a par hypothèse $m = p_1 \circ \varphi(e) = u(e)$ et $n = p_2 \circ \varphi(e) = v(e)$, donc $\varphi(e) = (u(e), v(e))$, il y a effectivement au plus une possibilité. Montrons maintenant que l'application $\varphi : e \mapsto (u(e), v(e))$ est effectivement un morphisme de R-modules :

$$\varphi(e + e') = (u(e + e') + v(e + e')) = (u(e) + u(e'), v(e) + v(e')) = (u(e), v(e)) + (u(e'), v(e')) = \varphi(e) + \varphi(e')$$

$$\varphi(r.e) = (u(r.e), v(r.e)) = (r.u(e), r.v(e)) = r.(u(e), v(e)) = r.\varphi(e)$$

donc φ est bien l'unique morphisme de R-module qui convient.

2. Soit $\varphi : P \to M \times N$ un morphisme de module, les morphismes $p_1 \circ \varphi$ et $p_2 \circ \varphi$ sont deux morphismes $P \to M$ et $P \to N$. La réciproque est donnée par la question précédente : un couple de morphismes $u, vP \to M, P \to N$ induit un unique morphisme $\varphi : P \to M \times N$ tels que $p_1 \circ \varphi = u$ et $p_2 \circ \varphi = v$.

Exercice 10. Supposons qu'un tel morphisme φ existe, et soit $e+F \in E/F$. On doit avoir $\varphi(e+F) = \varphi(\pi(e)) = p(e)$, donc les valeurs de φ sont entièrement déterminées, montrons que φ est ainsi bien défini : si $e+F = e'+F$, alors $e - e' \in F$, donc

$$\varphi(e) = p(e) = p(e') = \varphi(e')$$

justement car $p(e - e') = 0$ par hypothèse ($F \subset \operatorname{Ker} p$). Il est clair que φ ainsi défini est un morphisme de modules.

2. Soit $\varphi : E/F \to M$, on obtient un morphisme $p := \varphi \circ \pi : E \to M$, qui admet F dans son noyau. La question précédente donne la réciproque, un morphisme $p : E \to M$ admettant F dans son noyau se factorise par E/F.

Exercice 11.
1. Pour $x \in M$, on a $f(x) \in \operatorname{Im} f = \operatorname{Ker} p$, donc $p(f(x)) = 0$.

2. Par définition, on a $p \circ f = 0$ si et seulement si $\operatorname{Im} f \subset \operatorname{Ker} P$, par propriété universelle du quotient, il existe un unique $\varphi : N/\operatorname{Im} f \to P$ tel que $\varphi \circ \pi = p$, ce qui est exactement le résultat voulu.