TD2 : Généralités sur les anneaux et les modules

Diego Izquierdo

Les exercices 1, 3, 4, 6, 7, 8 ont été traités pendant la séance. Nous avons laissé les questions 3 de l'exercice 4 et 5 de l'exercice : nous les traiterons au prochain TD. Nous parlerons dans un TD ultérieur de l'exercice 13.

Exercice 1 (à préparer) : Radical d'un idéal (ex. 15 du TD1)
Soient A un anneau et I un idéal de A. On appelle radical de I l'ensemble $\sqrt{I} = \{a \in A | \exists n \in \mathbb{N}^*, a^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal.

2. Reconnaître $\sqrt{A}$ et $\sqrt{(0)}$.

3. Soit J un idéal de A. Déterminer si les assertions suivantes sont vraies ou fausses. Corriger celles qui sont fausses.

(a) $\sqrt{\sqrt{I}} = \sqrt{I}$.

(b) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(c) $\sqrt{IJ} = \sqrt{I} \cdot \sqrt{J}$.

(d) $\sqrt{I + J} = \sqrt{I} + \sqrt{J}$.

4. Montrer que $\sqrt{I}$ est l'intersection des idéaux premiers contenant I. On pourra utiliser le lemme de Zorn.

5. Prenons $A = \mathbb{Z}$ et $I = N\mathbb{Z}$. Calculer $\sqrt{I}$.

Exercice 2 : Idéaux comaximaux
Soient A un anneau et I et J deux idéaux.

1. On suppose que $I + J = A$. Montrer que $I^n + J^n = A$ pour tout $n > 0$.

> **Indications :** Il existe $i \in I$ et $j \in J$ tels que $i + j = 1$. Du coup, $1 = (i+j)^{2n} = \sum_{k=0}^{2n} C_{2n}^k i^k j^{2n-k} \in I^n + J^n$. Cela montre que $I^n + J^n = A$.

2. On suppose que $I + J = A$. Soit L un idéal tel que $IL \subseteq J$. Montrer que $L \subseteq J$.

> **Indications :** Il existe $i \in I$ et $j \in J$ tels que $i + j = 1$. Du coup, si on se donne $x \in L$, alors $x = xi + xj \in IL + J \subseteq J$. D'où $L \subseteq J$.

3. On suppose que $I \cap J = IJ$. A-t'on forcément $I + J = A$?

> **Indications :** Non : il suffit de choisir $A = \mathbb{C}[X, Y]$, $I = (X)$ et $J = (Y)$.

Exercice 3 (à préparer) : Idéaux premiers
Soit A un anneau.

1. Soient $\mathfrak{p}$ un idéal premier et $I_1, ..., I_n$ des idéaux. On suppose que $\mathfrak{p}$ contient $\prod_{k=1}^n I_k$. Montrer que $\mathfrak{p}$ contient l'un des I_k.

2. Soient I un idéal et $\mathfrak{p}_1, ..., \mathfrak{p}_n$ des idéaux premiers. On suppose que I est contenu dans $\bigcup_{k=1}^{n} \mathfrak{p}_k$. Montrer que I est contenu dans l'un des $\mathfrak{p}_k$.

Exercice 4 (à préparer) : Vrai ou faux ?
Soit A un anneau.

1. Si a, b et u sont trois éléments A tels que $(a) = (b)$ et $a = bu$, alors $u \in A^\times$.

2. Si A est intègre, I est un idéal principal et A/I est un anneau principal, alors A est principal.

3. Dans $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, l'idéal (3) n'est pas premier, mais il est contenu dans exactement deux idéaux premiers, qui sont maximaux.

Exercice 5 : Vrai ou faux ? Le retour
Soit A un anneau.

1. Tout idéal du quotient d'un anneau principal par un idéal est principal.

> **Indications :** VRAI : Soient A un anneau principal et I un idéal. Notons $p : A \to A/I$ la projection canonique. Si J est un idéal de A/I, on pose $\tilde{J} = p^{-1}(J)$. Comme A est principal, il existe $x \in A$ tel que $\tilde{J} = (x)$. On vérifie alors immédiatement que $J = (p(x))$.

2. La somme de deux idéaux non principaux d'un anneau est soit un idéal non principal soit l'anneau tout entier.

> **Indications :** FAUX : Dans $\mathbb{C}[X, Y]$, la somme des idéaux (X^2, XY) et $(X^2 + X, XY)$ est (X).

3. L'idéal (89) est premier dans $\mathbb{Z}[i]$.

> **Indications :** FAUX : On a $89 = 5^2 + 8^2 = (5 + 8i)(5 - 8i)$, donc 89 n'est pas irréductible dans $\mathbb{Z}[i]$.

4. L'anneau des nombres décimaux est isomorphe à $\mathbb{Z}[X]/(10X - 1)$.

> **Indications :** VRAI : Soit $\mathbb{D}$ l'anneau des nombres dédimaux. Soit $\phi : \mathbb{Z}[X] \to \mathbb{D}, X \mapsto \frac{1}{10}$. C'est un morphisme surjectif. Soit K son noyau. Il est évident que K contient $(10X - 1)$. Réciproquement, soit $P \in K$. En écrivant la division euclidienne de P par $10X - 1$, on voit qu'il existe $R \in \mathbb{Q}[X]$ tel que $P = (10X - 1)R$. A chaque polynôme $S \in \mathbb{Q}[X]$ de degré d, on peut associer le polynôme $\tilde{S}(X) = X^d S(1/X)$. On a alors $\tilde{P} = -(X - 10)\tilde{R}$. Comme $\tilde{P} \in \mathbb{Z}[X]$ et $X - 10 \in \mathbb{Z}[X]$ est unitaire, on déduit que $\tilde{R} \in \mathbb{Z}[X]$. Cela prouve que $R \in \mathbb{Z}[X]$ et donc que $K = (10X - 1)$.
>
> **Remarque :** Plus tard dans le cours, on pourra vérifier que R est à coefficients dans $\mathbb{Z}$ plus facilement. En effet, l'anneau $\mathbb{Z}$ est factoriel. Du coup, on peut utiliser le notion du contenu d'un polynôme à coefficients dans $\mathbb{Z}$. On a :
>
> $$ct(P) = ct(10X - 1)ct(R) = ct(R),$$
>
> et $ct(P) \in \mathbb{Z}$. Cela prouve que $R \in \mathbb{Z}[X]$.

Exercice 6 : Quotients d'anneaux

Soit k un corps.

1. Montrer que la k-algèbre $k[X,Y]/(X^2-Y^3)$ est isomorphe à $k[T^2,T^3]$.

2. Montrer que la k-algèbre $k[X,Y]/(X^2-Y)$ est isomorphe à $k[T]$.

3. Plus généralement, soient a et b deux entiers naturels non nuls. Réaliser l'anneau $k[T^a,T^b]$ comme quotient de $k[X,Y]$.

4. Montrer que la k-algèbre $k[X,Y]/(XY-1)$ n'est pas isomorphe à $k[T]$.

5. Réaliser les anneaux $\mathbb{Z}[i\sqrt{7}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ comme quotients de $\mathbb{Z}[X]$.

Exercice 7 : Idéaux dans un anneau principal

Soient A un anneau principal et $x \in A$ non nul. Montrer que les assertions suivantes sont équivalentes :

(i) l'élément x est irréductible ;

(ii) l'idéal (x) est premier, c'est-à-dire que $A/(x)$ est un anneau intègre ;

(iii) l'idéal (x) est maximal, c'est-à-dire que $A/(x)$ est un corps.

Exercice 8 : Idéaux d'un quotient

Soient A un anneau commutatif unitaire et I un idéal.

1. Montrer que les idéaux de A/I sont en bijection avec les idéaux de A contenant I.

2. Soit $J \supseteq I$ un idéal de A. Montrer que A/J est canoniquement isomorphe au quotient de A/I par J/I.

3. On dit que I est un idéal premier (resp. maximal) si A/I est intègre (resp. un corps). Montrer que les idéaux premiers (resp. maximaux) de A/I sont en bijection avec les idéaux premiers (resp. maximaux) de A contenant I.

4. Déterminer les idéaux des anneaux suivants :

$$\mathbb{R}[X]/(X^2+X+1), \mathbb{R}[X]/(X^3-6X^2+11X-6), \mathbb{R}[X]/(X^4-1), \mathbb{R}[X]/(X^5).$$

Lesquels sont premiers ? Et maximaux ?

5. Combien l'anneau $\mathbb{R}[X]/(X^5(X^4-1))$ possède-t'il d'idéaux ? d'idéaux premiers ? d'idéaux maximaux ?

Exercice 9 : Un contre-exemple

Soit A un anneau.

1. Supposons A intègre. Rappeler pourquoi, si a et b sont deux éléments de A tels que $(a) = (b)$, alors il existe $u \in A^\times$ tel que $a = bu$.

> **Indications :** Si $a = 0$ ou $b = 0$, la propriété est évidente. Supposons $a \neq 0$ et $b \neq 0$. Comme $(a) = (b)$, il existe $u, v \in A$ tels que $a = bu$ et $av = b$. On a alors $auv = a$. Par intégrité, $uv = 1$, et $u \in A^\times$.

Prenons maintenant $A = \mathbb{Q}[X,Y,Z]/(X - XYZ)$. On note x, y et z les classes de X, Y et Z dans A.

2. Vérifier que A n'est pas intègre.

> **Indications :** On a $x(1-yz) = 0$, mais $x \neq 0$ et $1 - yz \neq 0$.

3. Montrer que $(x) = (xy)$.

> **Indications :** On remarque que x divise xy et xy divise x car $xyz = x$. Donc $(x) = (xy)$.

4. Montrer qu'il n'existe pas d'élément $u \in A^\times$ tel que $xu = xy$.

> **Indications :** Supposons qu'un tel u existe. Soit $U \in \mathbb{Q}[X,Y,Z]$ un relèvement de u. On a alors $X(U - Y) \in (X - XYZ)\mathbb{Q}[X,Y,Z]$. Donc $U - Y \in (1 - YZ)\mathbb{Q}[X,Y,Z]$. On en déduit qu'il existe $H \in \mathbb{Q}[X,Y,Z]$ tel que $U = Y + (1 - YZ)H$. Dire que u est une unité dans A équivaut à dire que $(U, X - XYZ) = \mathbb{Q}[X,Y,Z]$. On a donc $(Y + (1-YZ)H, X) = \mathbb{Q}[X,Y,Z]$. Par ailleurs, on dispose d'un morphisme surjectif d'anneaux :
>
> $$\varphi : \mathbb{Q}[X,Y,Z] \to \mathbb{Q}[T], X \mapsto 0, Y \mapsto T, Z \mapsto T.$$
>
> On en déduit que $(T + (1-T^2)H(0,T,T)) = \mathbb{Q}[T]$, c'est-à-dire que $T + (1 - T^2)H(0,T,T) \in \mathbb{Q}$: c'est impossible !

Exercice 10 : Corps et idéaux

Soit A un anneau commutatif unitaire.

1. On suppose A intègre et que A possède un nombre fini d'idéaux. Montrer que A est un corps.

> **Indications :** Soit $x \in A \setminus \{0\}$. Pour chaque entier naturel n, notons $I_n = (x^n)$. Par hypothèse, il existe $n < m$ tels que $I_n = I_m$. Comme A est intègre, on en déduit qu'il existe $u \in A^\times$ tel que $x^n u = x^m$. On en déduit que $u = x^{m-n}$, et donc que $x \in A^\times$.

2. On suppose que A possède un nombre fini d'idéaux. Montrer que tout idéal premier de A est maximal.

> **Indications :** Soit I un idéal premier de A. L'anneau A/I possède un nombre fini d'idéaux et est intègre. Donc c'est un corps, et I est maximal.

3. On suppose que tout idéal propre de A est premier. Montrer que A est un corps.

> **Indications :** Soit $x \in A \setminus \{0\}$. Si $(x^2) = A$, alors x^2 est inversible et donc x l'est aussi. Supposons maintenant que $(x^2) \neq A$. Alors (x^2) est un idéal premier, et donc $x \in (x^2)$: il existe $u \in A$ tel que $x = ux^2$. Or A est intègre, puisque l'idéal (0) est premier. On en déduit que $ux = 1$, c'est-à-dire que x est inversible : absurde ! On en déduit que x est inversible et que A est un corps.

Exercice 11 : Idéaux premiers de $\mathcal{C}([0,1], \mathbb{R})$

1. Soient A un anneau et I un idéal de A. Notons J l'intersection des idéaux premiers de A contenant I. Le but de cette question est de montrer que $\sqrt{I} = J$.

(a) Montrer que $\sqrt{I}$ est contenu dans J.

> **Indications :** Soit $x \in \sqrt{I}$. Il existe $n \in \mathbb{N} \setminus \{0\}$ tel que $x^n \in I$. Soit $\mathfrak{p}$ un idéal premier de A contenant I. Alors $x^n \in \mathfrak{p}$, et donc $x \in \mathfrak{p}$. Cela étant vrai pour tout $\mathfrak{p}$, on en déduit que $x \in J$, et donc que $\sqrt{I} \subseteq J$.

(b) Réciproquement, soit $a \in A \setminus \sqrt{I}$, et considérons $\mathcal{E}$ la famille constituée des idéaux qui contiennent I mais qui ne contiennent aucune puissance de a. Montrer que $\mathcal{E}$ possède un élément maximal (pour l'inclusion), qui est un idéal premier de A. En déduire que $a \notin J$.

> **Indications :** La famille $\mathcal{E}$ est non vide puisqu'elle contient I. De plus, l'inclusion est un ordre inductif sur $\mathcal{E}$: en effet, si (I_i) est une famille totalement ordonnée d'éléments de $\mathcal{E}$, alors $\bigcup_i I_i$ est dans $\mathcal{E}$. Le lemme de Zorn permet donc de conclure que $\mathcal{E}$ possède un élément maximal I_0. Supposons que I_0 ne soit pas premier. Soient $b, c \in A$ tels que $bc \in I_0$ mais $b \notin I_0$ et $c \notin I_0$. Alors il existe n et m des entiers naturels tels que $a^n \in I_0 + (b)$ et $a^m \in I_0 + (c)$. On en déduit que $a^{n+m} \in I_0$: absurde ! Donc I_0 est premier. De plus, $a \notin I_0$ et $I \subseteq I_0$. Donc $a \notin J$.

(c) Conclure.

> **Indications :** On a $\sqrt{I} = J$.

Soit $\mathcal{C}$ l'anneau des fonctions continues de $[0, 1]$ dans $\mathbb{R}$.

2. Quels sont les idéaux maximaux de $\mathcal{C}$? Sont-ils principaux ?

> **Indications :** Notons $M_x = \{f \in \mathcal{C} \mid f(x) = 0\}$ pour tout $x \in [0, 1]$. C'est un idéal de $\mathcal{C}$. Et le morphisme d'anneaux $\mathcal{C} \to \mathbb{R}, f \mapsto f(x)$ est surjectif, de noyau M_x ; donc M_x est maximal. Réciproquement, soit M un idéal maximal de $\mathcal{C}$. Supposons $\bigcap_{f \in M}\{x \in X | f(x) = 0\} = \varnothing$. Dit autrement, les $f^{-1}(\mathbb{R} \setminus \{0\})$ pour $f \in M$ sont des ouverts qui recouvrent $[0, 1]$. Par compacité on extrait une famille finie $f_1, \dots, f_n \in M$ vérifiant
>
> $$f_1^{-1}(\mathbb{R} \setminus \{0\}) \cup f_2^{-1}(\mathbb{R} \setminus \{0\}) \cup \dots \cup f_n^{-1}(\mathbb{R} \setminus \{0\}) = [0, 1].$$
>
> De ce fait, la fonction $\sum_i f_i^2$ est un élément de M qui ne s'annule nulle part et est donc inversible dans $\mathcal{C}$. Mais alors, M est égal à $\mathcal{C}$, ce qui est absurde. En conclusion, il existe $x \in [0, 1]$ tel que l'on ait $M \subseteq M_x$; et on a égalité par maximalité de M.

3. Soit $I = \{f : [0, 1] \to \mathbb{R} \mid \forall m \in \mathbb{N}, \lim\limits_{x \to 0} \frac{f(x)}{x^m} = 0\}$. Montrer que $I = \sqrt{I}$ (on dit que I est un idéal radical). L'idéal I est-il premier ?

> **Indications :** Soient $f \in \mathcal{C}$ et $n \in \mathbb{N} \setminus \{0\}$ tels que $f^n \in I$. Alors $\lim\limits_{x \to 0} \left(\frac{f(x)}{x^m}\right)^n = 0$ pour tout m. Donc $f \in I$ et $I = \sqrt{I}$. L'idéal I n'est pas premier, puisqu'il est possible de construire $f, g \in \mathcal{C}$ telles que $fg = 0$ et $\frac{f(x)}{x}$ et $\frac{g(x)}{x}$ n'ont pas de limite en 0 (faire un dessin !).

4. En déduire que $\mathcal{C}$ possède des idéaux premiers non maximaux.

> **Indications :** Supposons que tous les idéaux premiers de A soient maximaux. Alors d'après la question 1., I serait une intersection d'idéaux maximaux. Mais le seul idéal maximal contenant I est M_0, et $I \neq M_0$. Absurde !

Exercice 12 : Lemme de Schur

Soit A un anneau. Un A-module est dit *simple* s'il est non nul et ne possède pas de sous-module propre non trivial.

1. Prouver que tout module simple est isomorphe à un $A/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal de A.

> **Indications :** Soit M un A-module simple. Soit $m \in M$. Alors $Am = M$. Donc le morphisme de a-modules $f : A \to M, a \mapsto am$ est surjectif. Soit I son noyau : c'est un idéal de A. On en déduit que M est isomorphe à A/I. Comme M est simple, cela impose que A/I n'a pas d'idéaux autres que (0) et (1) : donc A n'a pas d'idéaux contenant I autres que I et A. Par conséquent I est un idéal maximal de A.

2. Montrer que tout morphisme $f : M_1 \to M_2$ entre deux A-modules simples est soit nul, soit un isomorphisme.

> **Indications :** Soit $f : M_1 \to M_2$ un morphisme de A-modules simples. Soient N_1 sont noyau et N_2 son image. Comme M_1 est simple, $N_1 = 0$ ou $N_1 = M$. Comme M_2 est simple, $N_2 = 0$ ou $N_2 = M_2$. Dans tous les cas, on trouve que f est soit nul, soit un isomorphisme.

Exercice 13 : Sous-module de torsion

Soit A un anneau. Soit M un A-module. On dit qu'un élément $x \in M$ est de torsion s'il existe $a \in A$ non nul tel que $ax = 0$. On note M_{tor} l'ensemble des éléments de torsion de M. On dit que M est sans torsion si $M_{tor} = 0$.

1. Montrer que M_{tor} est le plus petit sous-module de M tel que M/M_{tor} est sans torsion.

2. Le sous-module M_{tor} a-t'il toujours un supplémentaire dans M ?

Exercice 14 : Sous-groupes du groupe des racines de l'unité

Faire la liste des sous-groupes du groupe des racines de l'unité dans $\mathbb{C}^\times$.

> **Indications :** Soit U le groupe des racines de l'unité. Soit V un sous-groupe. Les groupes U et V sont de torsion. On a donc :
>
> $$U = \bigoplus_p U\{p\},$$
>
> $$V = \bigoplus_p V\{p\},$$
>
> et pour chaque premier p, $V\{p\}$ est un sous-groupe de $U\{p\}$. Soit p un nombre premier. On vérifie aisément que, pour tout $r \geq 1$, si $V\{p\}$ possède un élément d'ordre p^r, alors $V\{p\}$ contient $U[p^r]$. On en déduit que $V\{p\} = U\{p\}$ ou $V\{p\} = U[p^r] = \mu_{p^r}$ pour un certain $r \geq 0$. Par conséquent, les sous-groupes de U sont donc les $\bigoplus_p V_p$ avec $V_p = U\{p\}$ ou $V_p = \mu_{p^{r_p}}$ pour un certain $r_p \geq 0$.

Exercice 15 : Chasses au diagramme

1. Soit A un anneau. Soient $f : M \to N$ et $g : N \to P$ des morphismes de A-modules. Montrer qu'il existe une suite exacte :

$$0 \to \mathrm{Ker}(f) \to \mathrm{Ker}(g \circ f) \to \mathrm{Ker}(g) \to \mathrm{Coker}(f) \to \mathrm{Coker}(g \circ f) \to \mathrm{Coker}(g) \to 0.$$

2. On considère un diagramme commutatif de A-modules à lignes exactes :

$$\begin{tikzcd} M_1 \arrow[r] \arrow[d, "f_1"] & M_2 \arrow[r] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & M_4 \arrow[r] \arrow[d, "f_4"] & M_5 \arrow[d, "f_5"] \\ N_1 \arrow[r] & N_2 \arrow[r] & N_3 \arrow[r] & N_4 \arrow[r] & N_5. \end{tikzcd}$$

On suppose que les morphismes f_1, f_2, f_4, f_5 sont des isomorphismes. Montrer que f_3 est un isomorphisme.

Exercice 16 : Déterminant

Soient R un anneau et n un entier naturel non nul. Soit $f : R^n \to R^n$ un morphisme de R-modules. Soit A la matrice de f dans la base canonique de R^n.

1. Montrer que les assertions suivantes sont équivalentes :

(i) f est surjectif ;

(ii) f est un isomorphisme ;

(iii) $\det(A) \in R^\times$.

> **Indications :** Les implications $(iii) \Rightarrow (ii) \Rightarrow (i)$ sont évidentes. Supposons (i) et notons $(e_1, ..., e_n)$ la base canonique de R^n. Soient $x_1, ..., x_n \in R^n$ tels que $f(x_i) = e_i$ pour chaque i. Soit $g : R^n \to R^n, e_i \mapsto x_i$. On a alors $f \circ g = Id$. Par conséquent, en notant B la matrice de g, on a $\det(A)\det(B) = 1$, et donc $\det(A) \in R^\times$. Cela prouve aussi que f est un isomorphisme.

2. Montrer que les assertions suivantes sont équivalentes :

(i) f est injectif ;

(ii) $\det(A)$ n'est pas un diviseur de 0 dans R.

> **Indications :** La formule ${}^t\mathrm{Com}(A)A = \det(A)I_n$ montre que $(ii) \Rightarrow (i)$. Supposons maintenant (i). Supposons que $\det(A)$ est un diviseur de 0 dans R. Soit $b \in R$ non nul tel que $b\det(A) = 0$. Soit N une sous-matrice carrée de taille maximale de A telle que $b\det(N) \neq 0$. Soit r la taille de N. Comme f est injectif, $r \geq 1$. Quitte à réordonner les lignes et les colonnes de A, on peut supposer que N est situé en haut à gauche de A. En notant $A = (a_{ij})$, on considère pour chaque $i \in \{1, ..., n\}$ la matrice :
>
> $$A_i = \begin{pmatrix} a_{1,1} & \cdots & a_{1,r+1} \\ \vdots & & \vdots \\ a_{r,1} & \cdots & a_{r,r+1} \\ a_{i,1} & \cdots & a_{i,r+1} \end{pmatrix}.$$
>
> On vérifie alors que $b\det A_i = 0$ pour tout i. Par conséquent, pour chaque i, en développant par rapport à la dernière ligne, on a $b\sum_{j=1}^{r+1}(-1)^j a_{i,j}\mu_j = 0$ où μ_j désigne le mineur correspondant au coefficient de position $(r+1, j)$. Cela montre que le vecteur $(-b\mu_1, b\mu_2, ..., (-1)^{r+1}b\mu_{r+1}, 0, ..., 0)$ est dans le noyau de f. Or $b\mu_{r+1} \neq 0$: absurde ! Donc $\det(A)$ n'est pas un diviseur de 0 dans R.

Exercice 17 : Le groupe $\mathbb{Z}^{\mathbb{N}}$ n'est pas abélien libre

On considère le groupe abélien $M = \mathbb{Z}^{\mathbb{N}}$. Le but de cet exercice est de montrer que M n'est pas abélien libre. On procède par l'absurde en supposant que M admet une base B. Pour $n \in \mathbb{N}$, on note e_n l'élément de M dont tous les termes sont nuls, sauf le n-ème qui vaut 1. On écrit alors e_n comme combinaison linéaire d'une partie finie B_n de B, et on note N le sous-groupe de M engendré par les éléments de $\bigcup_{n \in \mathbb{N}} B_n$.

1. Soit $S = \{(\epsilon_n n!)_{n \in \mathbb{N}} \mid \epsilon_n \in \{-1, 1\}\}$. Montrer qu'il existe $s \in S$ tel que $s \notin N$.

> **Indications :** Le groupe N est infini dénombrable alors que S ne l'est pas. Donc il existe $s \in S$ tel que $s \notin N$.

2. Montrer que, pour chaque $k \in \mathbb{N}^*$, il existe $y \in M/N$ tel que $\overline{s} = ky$.

> **Indications :** Notons $s = (\epsilon_n n!)_{n \in \mathbb{N}}$. Comme $e_0, ..., e_{k-1}$ sont dans N, on remarque que $\overline{s}$ coïncide avec la classe de $(\delta_n n!)_{n \in \mathbb{N}}$ où $\delta_n = 0$ si $n < k$ et $\delta_n = \epsilon_n$ sinon. On voit immédiatement que $(\delta_n n!)_{n \in \mathbb{N}}$ est multiple de k dans M, ce qui achève la preuve.

3. En déduire une contradiction.

> **Indications :** Le groupe abélien M/N est libre, mais possède un élément divisible non nul !

Exercice 18 (culturel) : Sous-groupes d'un groupe abélien libre

Dans cet exercice, nous allons montrer que tout sous-groupe d'un groupe abélien libre est abélien libre. Considérons donc A un groupe abélien libre, et soit X une base de A. Soit A_0 un sous-groupe de A. Soit $\mathcal{E}$ l'ensemble des triplets (Y, B, ϕ), où Y est une partie de X telle que $A_0 \cap A^{(Y)}$ est abélien libre, B est une base de $A_0 \cap A^{(Y)}$ et $\phi : B \to X$ une injection. Si (Y, B, ϕ) et (Y', B', ϕ') sont deux éléments de $\mathcal{E}$, on dira que $(Y, B, \phi) \preceq (Y', B', \phi')$ si $Y \subseteq Y'$, $B \subseteq B'$ et $\phi = \phi'|_B$. Cela définit une relation d'ordre sur $\mathcal{E}$.

1. Montrer que $\mathcal{E}$ possède un élément maximal pour $\preceq$.

2. En déduire que A_0 est abélien libre.

Nous allons maintenant appliquer ce résultat pour montrer que le groupe $\mathbb{Z}^{\mathbb{N}}$ n'est pas abélien libre par une méthode différente de celle de l'exercice 19. Pour chaque entier x, on note $v_2(x)$ la valuation 2-adique de x (avec la convention $v_2(0) = +\infty$).

3. Soit N le sous-groupe de $\mathbb{Z}^{\mathbb{N}}$ constitué des suites $(x_n)_{n \in \mathbb{N}}$ telles que $\lim_{n \to +\infty} v_2(x_n) = +\infty$. Montrer que $N/2N$ est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension dénombrable.

4. En déduire que $\mathbb{Z}^{\mathbb{N}}$ n'est pas abélien libre.