Algèbre et théorie de Galois - TD5

Définition 1. Une catégorie C est la donnée

a) d'une classe $\mathcal{O}b(C)$ appelés les objets de C,

b) pour chaque couple d'objets X, Y d'un ensemble $\mathrm{Hom}(X, Y)$ appelé ensemble des morphismes,

c) pour chaque objet X d'un morphisme $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ appelé identité,

d) pour chaque triplet d'objets X, Y, Z, d'une loi de composition des morphismes

$$\circ : \mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, Z) \to \mathrm{Hom}(X, Z).$$

On suppose de plus que la composition est associative, i.e., $f \circ (g \circ h) = (f \circ g) \circ h$ et que l'identité est une unité, i.e., $f \circ \mathrm{id} = f$ et $\mathrm{id} \circ f = f$.

Définition 2. Une propriété universelle [1] pour un objet Y de C est une description explicite (et compatible aux morphismes[2]) de $\mathrm{Hom}(X, Y)$ (ou $\mathrm{Hom}(Y, X)$) pour tout objet X de C.

Exemple 1. Voici quelques exemples que vous connaissez déjà bien.

a) (Ens) dont les objets sont les ensembles et les morphismes les applications.

b) (Grp) dont les objets sont les groupes et les morphismes les morphismes de groupes.

c) (Grab) dont les objets sont les groupes abéliens et les morphismes les morphismes de groupes.

d) (Anneaux) dont les objets sont les anneaux unitaires munis des morphismes d'anneaux.

e) (Top) dont les objets sont les espaces topologiques et les morphismes les applications continues.

Principe 1. *(Grothendieck)*

Ce qui compte, ce ne sont pas les objets mathématiques,
mais les relations qu'ils entretiennent
(i.e., les morphismes).

Exercice 1 : (Propriétés universelles) Quelle est la propriété universelle de

a) l'ensemble vide ?

b) l'ensemble à un point ?

c) $\mathbb{Z}$ comme groupe ?

d) $\mathbb{Z}$ comme anneau commutatif unitaire ?

e) $\mathbb{Q}$ comme anneau commutatif unitaire ?

f) l'anneau commutatif unitaire nul ?

Solution de l'exercice 1.

a) On a $\mathrm{Hom}_{(\mathrm{Ens})}(\emptyset, X) = \{\emptyset \subset X\}$ est réduit à un morphisme donné par l'inclusion canonique. C'est la propriété universelle à gauche de l'ensemble vide. On dit que c'est l'ensemble initial. On peut aussi écrire $\mathrm{Hom}_{(\mathrm{Ens})}(X, \emptyset) = \emptyset$ si X est non vide et $\mathrm{Hom}_{(\mathrm{Ens})}(\emptyset, \emptyset) = \{\emptyset \subset \emptyset\}$ est réduit à l'inclusion canonique. C'est l'autre propriété universelle de l'ensemble vide, mais comme elle est plus compliquée, elle est moins intéressante.

[1] Tout objet a exactement deux propriétés universelles, mais on n'écrira souvent uniquement la plus simple.
[2] Pour plus de précisions sur ces compatibilités, voir la page web [Wikipedia : lemme de Yoneda].

b) On a $\mathrm{Hom}_{(\textsc{Ens})}(X, \{.\}) = \{.\}$ est réduit à un morphisme donné par la projection canonique $X \to \{.\}$. On dit que le point est l'ensemble final.

c) On a $\mathrm{Hom}_{(\textsc{Grp})}(\mathbb{Z}, G) \cong \mathrm{Hom}_{(\textsc{Ens})}(\{.\}, G) \cong G$, la bijection étant obtenue en envoyant un morphisme $f : \mathbb{Z} \to G$ sur l'élément $f(1)$, qui détermine complètement G. On dit que $\mathbb{Z}$ est le groupe libre sur l'ensemble $\{.\}$ à un élément.

d) On a $\mathrm{Hom}_{(\textsc{Anneaux})}(\mathbb{Z}, A) = \{i_A : \mathbb{Z} \to A\} \cong \mathrm{Hom}_{(\textsc{Ens})}(\emptyset, A)$ pour A commutatif et $i_A : \mathbb{Z} \to A$ l'application canonique donnée par $i(n) = n.1_A$. On dit que $\mathbb{Z}$ est l'anneau commutatif unitaire initial.

e) L'anneau $\mathbb{Q}$ est le corps de fractions de $\mathbb{Z}$. On a donc $\mathrm{Hom}_{(\textsc{Anneaux})}(\mathbb{Q}, A) = \{f : \mathbb{Z} \to A | f(n) \in A^\times \forall n \in \mathbb{Z} - \{0\}\}$ est égal à $\emptyset$ si il existe un entier non nul non inversible dans A et à $\mathrm{Hom}_{(\textsc{Anneaux})}(\mathbb{Z}, A) = \{i_A\}$ sinon.

f) On a $\mathrm{Hom}_{(\textsc{Anneaux})}(A, 0) = \{0_A : A \to 0\}$ est réduit à un morphisme donné par $0_A(a) = 0$. En effet, on a nécessairement $1 = 0$ dans l'anneau nul et $0_A(a) = 0_A(a.1) = 0_A(a).0 = 0$ pour tout $a \in A$. On dit que l'anneau nul est l'anneau commutatif unitaire final.

Exercice 2 : (Objets libres) Soit C une catégorie dont les objets sont décrits par des ensembles munis de structures supplémentaires (par exemple, (Ens), (Grp), (Grab), (Anneaux) ou (Top)). Soit X un ensemble. Un objet libre de C sur X est un objet $L(X)$ de C tel que pour tout objet Z, on ait une bijection naturelle

$$\mathrm{Hom}(L(X), Z) \cong \mathrm{Hom}_{\mathrm{Ens}}(X, Z).$$

Soit X un ensemble donné. Décrire explicitement

a) le groupe libre sur X,

b) le groupe abélien libre sur X,

c) le $\mathbb{R}$-module libre sur X,

d) l'anneau commutatif unitaire libre sur X,

e) la $\mathbb{C}$-algèbre commutative unitaire libre sur X,

f) la $\mathbb{C}$-algèbre associative unitaire libre sur X.

Solution de l'exercice 2.

a) Le groupe libre sur X est donné par les mots dont les lettres sont dans l'ensemble $X \coprod X^{-1}$ formés d'éléments de X et d'éléments notés x^{-1} pour $x \in X$, et muni de la loi donnée par la concaténation des mots. On vérifie que $\mathrm{Hom}_{(\textsc{Grp})}(L(X), G) = \mathrm{Hom}_{(\textsc{Ens})}(X, G)$, c'est à dire que pour définir un morphisme du groupe libre sur X dans le groupe G, il suffit de définir l'image des générateurs. En effet, si $f : X \to G$ est une application, on peut donner l'image d'un mot en les lettre dans $X \coprod X^{-1}$ en prenant le mot en les images $f(x)$ et $(f(x))^{-1}$ des éléments de X et de leur inverse.

b) Le groupe abélien $L(X) = \mathbb{Z}^{(X)}$ libre sur X est donné par les applications $a : X \to \mathbb{Z}$ à support fini (nulles en dehors d'un ensemble fini). On peut aussi les voir comme des sommes $\sum_{x \in X} a_x\{x\}$ avec $a_x \in \mathbb{Z}$ presque tous nuls. On voit aussi que pour définir un morphisme $L(X) \to M$ vers un groupe abélien M, il suffit de définir l'image de ses éléments, d'où la bijection $\mathrm{Hom}_{(\textsc{Grab})}(L(X), M) \cong \mathrm{Hom}_{(\textsc{Ens})}(X, M)$ pour tout groupe abélien M.

c) Même chose qu'avant : $L(X) = \mathbb{R}^{(X)}$ est donné par les applications $f : X \to \mathbb{R}$ à support fini. C'est le $\mathbb{R}$-espace vectoriel de base X.

d) L'anneau commutatif unitaire libre sur X est l'anneau $\mathbb{Z}[X]$ des polynômes ayant leurs variables dans l'ensemble X. On peut commencer par définir le monoide libre $\mathbb{N}^{(X)}$ sur X qui est donné par les monômes sur X, i.e., les mots en des éléments de X avec la condition de commutation de toutes les lettres, i.e., par des produits finis $x_1^{n_1} \dots x_n^{m_n}$. On définit ensuite l'anneau commutatif unitaire libre sur X comme le $\mathbb{Z}$-module libre sur $\mathbb{N}^{(X)}$, i.e. l'ensemble des applications $a : \mathbb{N}^{(X)} \to \mathbb{Z}$ à

support fini (qui représentent les coefficients du polynôme $P(X) = \sum_{i \in \mathbb{N}^{(X)}} a_i x^i$), muni de son addition canonique et de la multiplication polynômiale. Si X est un ensemble fini, on retrouve les polynômes en un nombre fini de variables. On vérifie en combinant la propriété universelle du monoide libre et celle du module libre que c'est bien l'anneau commutatif unitaire libre sur X, i.e. , qu'on a une bijection

$$\mathrm{Hom}_{(\textsc{Anneaux})}(\mathbb{Z}[X] \to A) \cong \mathrm{Hom}_{(\textsc{Ens})}(X, A)$$

pour tout anneau commutatif unitaire A. On remarque au passage que l'algèbre symétrique sur le $\mathbb{Z}$-module libre $\mathbb{Z}^{(X)}$ sur X vérifie aussi cette propriété universelle, ce qui montre que l'algèbre symétrique du $\mathbb{Z}$-module libre $\mathbb{Z}^{(X)}$ est aussi l'algèbre commutative unitaire libre sur l

e) Comme avant, on définit la $\mathbb{C}$-algèbre commutative unitaire libre sur X comme le $\mathbb{C}$-module libre sur les monômes $\mathbb{N}^{(X)}$. Ce sont simplement les polynômes à variables dans l'ensemble X et à coefficients complexes.

f) Par définition de l'algèbre tensorielle, on sait que si $M(X) = \mathbb{C}^{(X)}$ est le $\mathbb{C}$-module libre sur X et que A est une $\mathbb{C}$-algèbre associative unitaire, on a un isomorphisme naturel

$$\mathrm{Hom}_{\mathbb{C}-Alg}(T_{\mathbb{C}}(M(X)), A) \cong \mathrm{Hom}_{\mathbb{C}-mod}(M(X), A)$$

et par la propriété universelle du module libre, on a

$$\mathrm{Hom}_{\mathbb{C}-mod}(M(X), A) \cong \mathrm{Hom}_{(\textsc{Ens})}(X, A)$$

donc l'algèbre tensorielle sur le $\mathbb{C}$-module libre sur X est la $\mathbb{C}$-algèbre associative libre sur l'ensemble X.

Exercice 3 : (Produits et sommes) Le produit (resp. la somme) de deux objets X et Y est est un objet $X \times Y$ (resp. $X \coprod Y$, parfois noté $X \oplus Y$) tel que pour tout objet Z, soit donné une bijection naturelle en Z (compatible aux morphismes $f : Z_1 \to Z_2$)

$$\mathrm{Hom}(Z, X \times Y) \cong \mathrm{Hom}(Z, X) \times \mathrm{Hom}(Z, Y)$$
$$(\text{resp. } \mathrm{Hom}(X \coprod Y, Z) \cong \mathrm{Hom}(X, Z) \times \mathrm{Hom}(Y, Z)).$$

Décrire explicitement

a) les sommes et produits de deux ensembles,

b) les sommes et produits de deux groupes abéliens, puis celles de deux groupes,

c) les sommes et produits de deux anneaux commutatifs unitaires.

Solution de l'exercice 3.

a) On va donner juste la somme, le produit étant déjà bien connu. On définit $X \coprod Y$ comme l'union disjointe de X et Y, c'est à dire un ensemble composé exclusivement des éléments de X et de ceux de Y. On a deux inclusions naturelles $i_X : X \to X \coprod Y$ et $i_Y : Y \to X \coprod Y$ et si $f \in \mathrm{Hom}_{(\textsc{Ens})}(X \coprod Y, Z)$ est une application définie sur l'union disjointe, le couple $(f \circ i_X, f \circ i_Y)$ détermine f de manière unique. Ceci donne une application injective

$$\mathrm{Hom}(X \coprod Y, Z) \to \mathrm{Hom}(X, Z) \times \mathrm{Hom}(Y, Z).$$

Si (h, k) sont dans le terme de droite, on peut définir une application $f : X \coprod Y \to Z$ par $f(x) = h(x)$ si $x \in X$ et $f(y) = k(y)$ si $y \in Y$. Ceci montre la surjectivite de l'application entre ensembles de morphismes, et donc sa bijectivité. On a ainsi montré que l'union disjointe de deux ensembles vérifie la propriété universelle de la somme de deux ensembles.

b) Pour X et Y deux groupes abéliens, leur somme est définie comme un quotient du groupe abélien libre $\mathbb{Z}^{(X \coprod Y)}$ sur la somme des ensembles sous-jacents. On définit ce quotient en imposant que les applications canoniques $i_X : X \to \mathbb{Z}^{(X \coprod Y)}$ et $i_Y : Y \to \mathbb{Z}^{(X \coprod Y)}$ soient des morphismes de groupes, i.e., $\{x\} + \{x'\} = \{x + x'\}$ pour (x, x') dans X^2 ou Y^2 et $0_X = 0_Y = 0$. La combinaison de la propriété universelle de la somme de deux ensembles, de celle du groupe abélien libre et de celle du quotient nous montre qu'on a une bijection

$$\mathrm{Hom}_{(\mathrm{GRAB})}(X \coprod\!\!\!\!\coprod Y, Z) \cong \mathrm{Hom}_{(\mathrm{GRAB})}(X, Z) \times \mathrm{Hom}_{(\mathrm{GRAB})}(Y, Z).$$

Le groupe abélien $X \coprod\!\!\!\!\coprod Y$ obtenu est aussi noté $X \oplus Y$ et appelé la somme directe des deux groupes abéliens. Pour les groupes, on procède de manière similaire, mais il faut utiliser le groupe libre (non abélien, i.e., les mots, sur l'union disjointe $X \coprod Y$ des ensembles sous-jacents aux groupes considérés). Le groupe obtenu $X \coprod\!\!\!\!\coprod Y$ est appelé le produit libre des deux groupes X et Y et souvent noté $X * Y$. On note que ce n'est pas un produit mais une somme du point de vue des propriétés universelles, mais les traditions linguistiques ont la peau dure.

Exercice 4 : (Produits fibrés et sommes amalgamées) Le produit fibré (resp. la somme amalgamée) de deux morphismes $f : X \to S$ et $g : Y \to S$ (resp. $f : S \to X$ et $f : S \to Y$) est est un objet $X \times_S Y$ (resp. $X \coprod_S Y$, parfois noté $X \oplus_S Y$) tel que pour tout objet Z, soit donné une bijection naturelle en Z (compatible aux morphismes $f : Z_1 \to Z_2$)

$$\begin{array}{rcl} \mathrm{Hom}(Z, X \times_S Y) & \cong & \{(h,k) \in \mathrm{Hom}(Z,X) \times \mathrm{Hom}(Z,Y) | f \circ h = g \circ k\} \\ (\text{resp. } \mathrm{Hom}(X \coprod_S Y, Z) & \cong & \{(h,k) \in \mathrm{Hom}(X,Z) \times \mathrm{Hom}(Y,Z) | h \circ f = k \circ g\}). \end{array}$$

a) Répondre succintement aux mêmes questions que l'exercice précédent pour les produits et sommes amalgamées.

b) Soit $a < b < c < d$ trois nombres réels. Décrire explicitement les ensembles

$$]a, c[\times_{]a,d[}]b, d[\qquad \text{et} \qquad]a, c[\coprod\!\!\!\!\coprod_{]b,c[}]b, d[.$$

c) Décrire explicitement le groupe abélien

$$\mathbb{Z} \times_{\mathbb{Z}} \mathbb{Z}$$

où $f, g : \mathbb{Z} \to \mathbb{Z}$ sont données par $f : n \mapsto 2n$ et $g : n \mapsto 3n$.

Solution de l'exercice 4.

a) Laissé au lecteur. C'est similaire aux produits et sommes.

b) Le produit fibré donne l'intersection et la somme amalgamée donne la réunion (recollement) des deux intervalles considérés.

c) C'est $6\mathbb{Z}$, muni des deux projections $6\mathbb{Z} \xrightarrow{.3} \mathbb{Z}$ et $6\mathbb{Z} \xrightarrow{.3} \mathbb{Z}$. En effet, si $h : M \to \mathbb{Z} \times_{\mathbb{Z}} \mathbb{Z}$ est un morphisme de groupes abéliens tel que $h \circ f = g \circ f$ alors $f(x) = (n_x, m_x)$ avec $3 | n_x$ et $2 | m_x$ et $n_x = m_x \in 6\mathbb{Z}$. Ceci montre que

$$\mathrm{Hom}_{(\mathrm{GRAB})}(M, Z \times_{\mathbb{Z}} \mathbb{Z}) \cong \mathrm{Hom}_{(\mathrm{GRAB})}(M, 6\mathbb{Z})$$

donc $6\mathbb{Z} \cong \mathbb{Z} \times_{\mathbb{Z}} \mathbb{Z}$.

Exercice 5 : (Limites projectives) Soit $(I, \leq)$ un ensemble partiellement ordonné. Un système projectif d'objets indexé par I est une famille

$$A_\bullet = ((A_i)_{i \in I}, (f_{i,j})_{i \leq j})$$

d'objets et pour chaque $i \leq j$ de morphismes $f_{i,j} : A_j \to A_i$ tels que $f_{i,i} = \mathrm{id}_{A_i}$ et $f_{i,k} = f_{i,j} \circ f_{j,k}$ (une telle donnée est aussi appelée un foncteur de $A_\bullet : I \to C$ dans la catégorie considérée C). Une limite projective pour $A_\bullet$ est un objet $\varprojlim_I A_\bullet$ tel que pour tout objet Z, on ait une bijection naturelle

$$\mathrm{Hom}(Z, \varprojlim_I A_\bullet) \cong \varprojlim_I \mathrm{Hom}(A_i, Z)$$

où $\varprojlim_I \mathrm{Hom}(A_i, Z) \subset \prod_i \mathrm{Hom}(A_i, Z)$ désigne les familles de morphismes h_i telles que $f_{i,j} \circ h_j = h_i$. On définit les limites inductives $\varinjlim A_\bullet$ de manières similaires en inversant les but et sources des morphismes.

a) Montrer que les produits et produits fibrés sont des cas particuliers de cette définition.

b) Décrire l'anneau $\varprojlim_n \mathbb{C}[X]/(X^n)$.

c) Décrire l'anneau $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Solution de l'exercice 5.

a) Soient $f : X \to S$ et $g : Y \to S$ deux morphismes dont on veut prendre le produit fibré. Soit I l'ensemble à trois éléments $\{X, Y, S\}$ avec pour seule inégalités non triviales $X \leq S$ et $Y \leq S$. Le couple donné par $X \to S$ et $Y \to S$ est donc un système projectif indexé par l'ensemble partiellement ordonné I. La condition imposée à la limite projective L est que si Z est un objet, la donnée d'un morphisme $Z \to L$ est équivalente à celle d'une famille de trois morphismes $(i : Z \to X, j : Z \to Y, k : Z \to S)$ qui vérifient les conditions $f \circ i = g \circ j = k$, ce qui est exactement la propriété universelle du produit fibré (car k est déterminé par i ou j).

b) C'est l'anneau des séries formelles $\mathbb{C}[[X]]$. On a pour tout n une application de réduction modulo X^n $\mathbb{C}[[X]] \to \mathbb{C}[X]/(X^n)$ et une série formelle S est représentée dans le produit $\prod_n \mathbb{C}[X]/(X^n)$ par la famille $(S \mod X^n)_n$ de toutes ses réductions. On voit qu'une telle série vérifie bien les conditions de compatibilité avec les morphismes du système projectifs puisque ces morphismes sont des réductions et que les réductions sont toutes celles d'une série donnée. On montre que ceci donne tous les éléments de la limite projective par utilisation de la division euclidienne. On remarque que le polynôme $1 - X$ n'est pas inversible dans $\mathbb{C}[X]$ mais il le devient dans $\mathbb{C}[[X]]$ car la série $\sum_{i \geq 0} X^i$ est un élément de la limite projective qui donne un inverse pour $1 - X$.

c) On peut voir les éléments de la limite projective, notée $\mathbb{Z}_p$ comme des familles infinies d'entiers $(m_n)_n$ indexées par les entiers telles que $m_{n+1} \mod p^n = m_n$. Par division euclidienne successive, une telle famille de nombres peut être décrite par une série $s = \sum_{i \geq 0} a_i p^i$ avec $a_i \in \{0, \ldots, p-1\}$. On remarque que le nombre $\frac{1}{1-p}$ n'est pas un entier, i.e., pas dans $\mathbb{Z}$, mais c'est un entier p-adique, il est dans $\mathbb{Z}_p$, car on peut l'écrire $\sum_{i \geq 0} p^i$ et cette série converge clairement dans $\mathbb{Z}_p$ par définition de la limite projective.

Exercice 6 : Soit A un anneau commutatif unitaire, $S \subset A$ un ensemble multiplicatif (stable par multiplication et contenant 1_A). La localisation $A[S^{-1}]$ de A par rapport à S est défini par la propriété universelle

$$\mathrm{Hom}_{(\textsc{Anneaux})}(A[S^{-1}], B) = \{f \in \mathrm{Hom}_{(\textsc{Anneaux})}(A, B) | \forall s \in S,\, f(s) \in B^\times\},$$

où $B^\times$ est l'ensemble des éléments inversibles dans un anneau B.

a) Décrire $\mathbb{Z}[1/2] := \mathbb{Z}[\{2^{\mathbb{Z}}\}^{-1}]$.

b) Le morphisme $\mathbb{Z} \to \mathbb{Z}[1/2]$ est-il fini (i.e. $\mathbb{Z}[1/2]$ est t'il un $\mathbb{Z}$-module de type fini, i.e. engendré par un nombre fini d'éléments) ? De type fini (i.e. $\mathbb{Z}[1/2]$ peut-il être décrit comme un quotient d'un anneau de polynômes sur $\mathbb{Z}$ en un nombre fini de variables) ?

c) Construire un morphisme $\mathbb{Z}[1/2] \to \mathbb{Z}_3$ où $\mathbb{Z}_3$ sont les entiers 3-adiques définis dans l'exercice précédent.

d) Existe-t'il un morphisme $\mathbb{Z}[1/3] \to \mathbb{Z}_3$?

Solution de l'exercice 6.

a) Tout élément de $\mathbb{Z}[1/2]$ s'écrit sous la forme $n.2^m$ avec $n \in \mathbb{Z}$ non divisible par 2 et $m \in \mathbb{Z}$.

b) Le morphisme $\mathbb{Z} \to \mathbb{Z}[1/2]$ n'est pas fini. En effet, supposons qu'on dispose d'un système générateur fini F, i.e. d'un morphisme surjectif de $\mathbb{Z}$-modules $\mathbb{Z}^{(F)} \to \mathbb{Z}[1/2]$. Alors, il existe m_0 tel que tout $f \in F$ a pour dénominateur une puissance de 2 inférieure strictement à m_0. Ceci montre que l'application $\mathbb{Z}^{(F)} \to \mathbb{Z}$ n'est pas surjective car $\frac{1}{2^{m_0}}$ n'est pas dans son image. C'est une contradiction donc $\mathbb{Z}[1/2]$ n'est pas finie sur $\mathbb{Z}$. Par contre, on a un morphisme naturel $\mathbb{Z}[X] \to \mathbb{Z}[1/2]$ donné par $X \mapsto 1/2$ et ce morphisme est surjectif donc $\mathbb{Z} \to \mathbb{Z}[1/2]$ est de type fini.

c) On remarque que le nombre 3-adique donnée par les polynômes $S_n = -\sum_{i=0}^{n} 3^i$ (qui sont bien dans la limite projective $\mathbb{Z}_3$ de l'exercice précédent puisque $S_{n+1} = S_n \mod 3^{n+1}$) est un inverse du nombre $3-1=2$. En effet, on a $(1-3)S_n = 1-3^{n+1} = 1 \mod 3^{n+1}$. Par la propriété universelle de la localisation, on obtient un morphisme naturel $\mathbb{Z}[1/2] \to \mathbb{Z}_3$.

d) D'après la propriété universelle de la localisation, la donnée d'un morphisme $\mathbb{Z}[1/3] \to \mathbb{Z}_3$ est équivalente à celle d'un morphisme $\mathbb{Z} \to \mathbb{Z}_3$ tel que l'image de 3 soit inversible. Par la propriété universelle de $\mathbb{Z}$, il n'existe qu'un morphisme $\mathbb{Z} \to \mathbb{Z}_3$ donc il suffit de vérifier que l'image de 3 dans $\mathbb{Z}_3$ n'est pas inversible pour montrer qu'il n'existe pas de morphisme $\mathbb{Z}[1/3] \to \mathbb{Z}_3$. Comme le passage aux éléments inversibles est compatible aux morphismes d'anneaux, on devrait avoir un morphisme $\mathbb{Z}_3^\times \to (\mathbb{Z}/3\mathbb{Z})^\times$ or l'image de 3 dans $\mathbb{Z}/3\mathbb{Z}$ est nulle donc n'est pas inversible, ce qui donnerait une contradiction si 3 était inversible dans $\mathbb{Z}_3$, d'où la conclusion.

Exercice 7 : L'idéal $I = (X_1, \dots, X_n, \dots)$ engendré par toutes les variables de l'anneau de polynôme $A = \mathbb{Z}[\mathbb{N}] := \mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ est il de type fini ? L'anneau A est-il noetherien ? *Solution de l'exercice* 7. Si l'idéal considéré n'est pas de type fini, l'anneau A ne peut être noetherien. Supposons donné un système F fini de générateurs pour le A-module $I = (X_1, \dots, X_n, \dots)$. Rappelons qu'on a par définition explicite de l'anneau $\mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ un isomorphisme de $\mathbb{Z}$-modules

$$\mathbb{Z}^{\{(\mathbb{N}^{(X_i)_{i\in\mathbb{N}}})\}} \to \mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$$

qui peut-être résumé en disant que tout polynôme $P \in A$ peut s'écrire sous la forme

$$P = \sum_{\underline{i}\in\mathbb{N}^{\{(X_i)_{i\in\mathbb{N}}\}}} a_{\underline{i}} \underline{X^i}$$

avec $\underline{X^i} := \prod_{n_i\in\underline{i}} X_i^{n_i}$. Maintenant, on se donne un système F fini de générateurs et on suppose que leur écriture ne fait intervenir que des variables parmi $X_0, \dots, X_M$. On peut alors supposer pour simplifier que $F = \mathbb{N}^{(\{X_0,\dots,X_M\})}$ est l'ensemble de tous les monômes en les variables considérées (c'est le monoïde libre sur l'ensemble des variables). Le système F est générateur si et seulement si l'application canonique $A^{(F)} \to I$ est un morphisme surjectif de A-modules. On devrait donc pouvoir écrire

$$X_{M+1} = \sum_{j=0}^{M} P_j X_i$$

avec $P_j \in A$. Si on décompose les P_j dans la $\mathbb{Z}$-base de $\mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ donnée par les monômes, on obtient

$$X_{M+1} = \sum_{j=0}^{M} \sum_{\underline{i}_j\in I_j\subset\mathbb{N}^{\{(X_i)_{i\in\mathbb{N}}\}}} a_{\underline{i}_j} \underline{X^{i_j}} X_j$$

avec $a_{\underline{i}_j} \in \mathbb{Z}$. On considère alors dans l'expression de droite les monômes qui contiennent la variable X_{M+1} et on les passe de l'autre coté de l'égalité pour obtenir

$$X_{M+1}(1 - \sum_{\underline{i}_j \in I_j, X_{M+1} | \underline{X}^{\underline{i}_j}} a_{\underline{i}_j} \frac{\underline{X}^{\underline{i}_j}}{X_{M+1}} X_j) = \sum_{\underline{i}_j \in I_j, X_{M+1} \nmid \underline{X}^{\underline{i}_j}} a_{\underline{i}_j} \underline{X}^{\underline{i}_j} X_j.$$

Si le polynôme de droite est non nul, X_{M+1} le divise, mais il n'apparaît par définition pas dans son écriture et on obtient une contradiction. Si le polynôme de droite est nul, celui de gauche aussi donc

$$\sum_{\underline{i}_j \in I_j, X_{M+1} | \underline{X}^{\underline{i}_j}} a_{\underline{i}_j} \frac{\underline{X}^{\underline{i}_j}}{X_{M+1}} X_j) = 1,$$

ce qui est impossible car les monômes sont des multiples de X_j donc de degré strictement supérieur à 0. On conclut que $X_{M+1} \notin I$ donc F n'est pas un système générateur et c'est une contradiction. Donc I n'admet pas de système générateur fini et A n'est pas noethérien.

Exercice 8 : (**Algèbre de Clifford)** Soit A un anneau commutatif unitaire, M un A-module et $q \in \text{Bilsym}(M, M; A)$ une forme A-bilinéaire symétrique sur $M \times M$ à valeurs dans A. L'algèbre de Clifford $\text{Cliff}(M, q)$ de (M, q) est la A-algèbre associative unitaire qui vérifie la propriété universelle

$$\text{Hom}_{A-alg}(\text{Cliff}(M, q), B) \cong \{j \in \text{Hom}_{A-Mod}(M, B) | j(v).j(w) + j(w).j(v) = q(v, w).1_B\}$$

pour toute A-algèbre associative B.

a) Définir l'algèbre de Clifford explicitement en utilisant l'algèbre associative libre (i.e. l'algèbre tensorielle).

b) Montrer que l'automorphisme $v \mapsto -v$ de (M, q) induit un automorphisme $\alpha : \text{Cliff}(M, q) \to \text{Cliff}(M, q)$ et une décomposition $\text{Cliff}(M, q) = \text{Cliff}^0(M, q) \oplus \text{Cliff}^1(M, q)$.

c) On note $\text{GSpin}(M, q)$ le groupe des inversibles de l'algèbre $Q(M, q)$ tels que $xv\alpha(x)^{-1} \in M$ pour tout $m \in M$. Définir un morphisme naturel

$$\text{GSpin}(M, q) \to O(M, q)$$

vers le groupe orthogonal de (M, q).

d) On suppose maintenant que $M = A^n$ est libre et q non dégénérée. On définit le groupe $\text{Spin}(M, q)$ comme le noyau du déterminant $\det : \text{GSpin}(M, q) \to O(M, q) \to A^\times = \text{GL}_1(\wedge^n M)$. On note $V = \text{Cliff}(M, q)$. Montrer que l'action naturelle de $\text{Spin}(M, q)$ sur V commute à l'automorphisme α de V. En déduire que la décomposition $V = V_0 \oplus V_1$ est munie d'une action du groupe $\text{Spin}(M, q)$. Une composante irréductible de cette représentation est appelée représentation de Spin demi-entier.

e) (difficile) Soit $(M, q) = (\mathbb{R}^{3,1}, q)$ l'espace de Minkowski sur $\mathbb{R}$ donné par la forme quadratique $q(t, x, y, z) = -c^2t^2 + x^2 + y^2 + z^2$ sur $M = \mathbb{R}^4$. On note $\text{Cliff}_{3,1}(\mathbb{R})$ l'algèbre de Clifford de M. Construire un isomorphisme entre le groupe spinoriel [3] correspondant $\text{Spin}_{3,1}(\mathbb{R})$ et le groupe réel $\text{SL}_2(\mathbb{C})$. Décrire l'action correspondante de $\text{SL}_2(\mathbb{C})$ sur $\mathbb{R}^{3,1}$.

Solution de l'exercice 8. Voir [Wikipedia : Clifford algebra].

[3] On remarque qu'en physique, un type de particule élémentaire libre relativiste est décrite par une représentation de $\text{Spin}_{3,1}(\mathbb{R})$. Par exemple, le photon correspond à l'action de ce groupe sur $\mathbb{R}^{3,1}$ et l'électron correspond à la représentation de spin demi-entier.