ALGÈBRE COMMUTATIVE

ANNA CADORET

COURS DE MASTER 1 À SORBONNE UNIVERSITÉ - VERSION 2023 (EN COURS D'ACTUALISATION)

Contents

References

[AM69] M.F. Atiyah et I.G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.
[L02] S. Lang, *Algebra (3rd ed.)*, G.T.M. **211**, Springer, 2002.
[S10] P. Schapira, *Categories and homological algebra*, disponible sur http://people.math.jussieu.fr/~schapira/lectnotes/

On utilisera les notations $X \twoheadrightarrow Y$, $X \hookrightarrow Y$, $X \tilde{\to} Y$ (ou $X \xrightarrow{\sim} Y$) pour une application ensembliste $X \to Y$ respectivement surjective, injective, bijective.

On aura parfois recours à l'axiome du choix sous l'une des formulations équivalentes suivantes:

- Un produit cartésien d'ensembles finis non vides est non vide.
- (Lemme de Zorn) tout ensemble non vide ordonné inductif admet un élément maximal. (On rappelle qu'un ensemble ordonné est dit inductif si toute suite croissante admet un majorant).

L'algèbre commutative est en gros la théorie des anneaux commutatifs et des modules sur les anneaux commutatifs. On retrouve ces structures dans toutes les branches des mathématiques, ce qui en fait un

outil absolument fondamental. L'objectif de ce cours est d'introduire les propriétés et constructions de base avec une légère coloration "catégorielle" (le langage "moderne" désormais utilisé).

Part 1. Anneaux - généralités

1. Définitions

1.1. **Monoïdes, groupes.** On rappelle qu'un monoïde (unitaire) est un couple $(M, \cdot)$ formé d'un ensemble M et d'une application $\cdot : M \times M \to M$ qui vérifient les axiomes suivants:

(1) Associativité: $(l \cdot m) \cdot n = l \cdot (m \cdot n)$, $l, m, n \in M$;
(2) Élément neutre: il existe $e_M \in M$ tel que $m \cdot e_M = m = e_M \cdot m$, $m \in M$;

On dit qu'un élément $m \in M$ est inversible s'il existe $n \in M$ tel que $m \cdot n = e_M = n \cdot m$. L'élément n est alors unique (si $m \cdot n' = e_M = n' \cdot m$, alors $n = n \cdot e_M = n \cdot (m \cdot n') = (n \cdot m) \cdot n' = e_M \cdot n' = n'$); on dit que c'est l'inverse de m et on le note m^{-1}. On notera $M^\times \subset M$ le sous-ensemble des éléments inversibles de M. On dit qu'un monoïde $(M, \cdot)$ est un groupe si, de plus:

(3) Inverse: $M = M^\times$.

Soit $(M, \cdot)$ un monoïde (resp. un groupe), un sous-monoïde (resp. un sous-groupe) de $(M, \cdot)$ est un sous-ensemble $M' \subset M$ tel que $e_M \in M'$ et $m_1, m_2 \in M'$ implique $m_1 \cdot m_2 \in M'$ (resp. $e_M \in M'$, $m_1, m_2 \in M'$ implique $m_1^{-1} \cdot m_2 \in M'$). En particulier, $(M', \cdot)$ est un monoïde (resp. un groupe). Pour un monoïde $(M, \cdot)$ arbitraire, $M^\times \subset M$ est un sous-monoïde tel que $(M^\times, \cdot)$ est un groupe et c'est le plus grand sous-monoïde ayant cette propriété.

Etant donnés deux monoïdes M, N, un morphisme de monoïdes est une application $\phi : M \to N$ qui vérifie:

(1) $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$, $m, n \in M$;
(2) $\phi(e_M) = e_N$.

On remarquera que l'application identité $Id : M \to M$ est un morphisme de monoïdes et que si $\phi : L \to M$ et $\psi : M \to N$ sont des morphismes de monoïdes alors $\psi \circ \phi : L \to N$ est un morphisme de monoïdes. On notera $Hom_{Mono}(M, N)$ l'ensemble des morphismes de monoïdes $\phi : M \to N$ et, si $M = N$, $End_{Mono}(M) := Hom_{Mono}(M, M)$. Etant donnés deux groupes M, N, un morphisme de groupes $\phi : M \to N$ est un morphisme entre les monoïdes sous-jacents. Dans ce cas, on notera plutôt $Hom_{Grp}(M, N)$ et $End_{Grp}(M)$ que $Hom_{Mono}(M, N)$, $End_{Mono}(M)$.

On dit qu'un monoïde $(M, \cdot)$ est abélien ou commutatif si $m \cdot n = n \cdot m$, $m, n \in M$. On note alors en général plutôt $(M, +) = (M, \cdot)$, $-m := m^{-1}$, $0_M := e_M$.

1.2. **Anneaux.** Un anneau est un triplet $(A, +, \cdot)$ formé d'un ensemble A et de deux applications $+, \cdot : A \times A \to A$ - appelées respectivement l'addition et la multiplication - vérifiant les axiomes suivants:

(1) $(A, +)$ est un groupe abélien; on note 0_A son élément neutre (appelé zéro) et $-a$ l'inverse d'un élément $a \in A$;
(2) $(A, \cdot)$ est un monoïde; on note 1_A son élément neutre (appelé unité).
(3) La multiplication est distributive par rapport à l'addition *i.e.* $a \cdot (b + c) = a \cdot b + a \cdot c$ et $(b + c) \cdot a = b \cdot a + c \cdot a$, $a, b, c \in A$.

Dans la suite, on écrira presque toujours ab au lieu de $a \cdot b$, $0 := 0_A$, $1 := 1_A$. On omettra presque toujours les données $+, \cdot$ des notations.

Un anneau A est dit commutatif si le monoïde $(A, \cdot)$ l'est.

1.3. **Groupe des inversibles.** Le monoïde $(A, \cdot)$ n'est pas un groupe en général; on note $A^\times \subset A$ le groupe des éléments inversibles du monoïde $(A, \cdot)$ et $a^{-1} \in A^\times$ l'inverse d'un élément de $a \in A^\times$.

On dit qu'un anneau A est un anneau à division ou un corps gauche si $1 \neq 0$ et $A \setminus \{0\} = A^\times$. Si A est de plus commutatif, on dit simplement que A est un corps.

Exemples.
- L'anneau nul $A = \{0\}$ (on n'a pas exclu $1 \neq 0$ dans la définition d'anneau).
- L'anneau $\mathbb{Z}$ des entiers. Dans ce cas $\mathbb{Z}^\times = \{\pm 1\}$.
- Les corps commutatifs, par exemple $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Dans ce cas $K^\times = K \setminus \{0\}$.
- Si M est un groupe abélien, l'ensemble $End_{Grp}(M)$ des endomorphismes du groupe abélien M muni de $(\phi+\psi)(m) = \phi(m)+\psi(m)$ et $(\psi\cdot\phi)(m) = \psi\circ\phi(m)$ est un anneau (non commutatif en général) de zéro l'application nulle et d'unité l'application identité. Dans ce cas, $End_{Grp}(M)^\times = Aut_{Grp}(M)$.
- Si M est un espace vectoriel sur un corps commutatif k, l'ensemble $End_k(M)$ des endomorphismes du k-espace vectoriel M muni de $(\phi+\psi)(m) = \phi(m)+\psi(m)$ et $(\psi\cdot\phi)(m) = \psi\circ\phi(m)$ est un anneau (non commutatif si M est de k-dimension ≥ 2) de zéro l'application nulle et d'unité l'application identité. Dans ce cas, $End_k(M)^\times = GL_k(M)$.
- Si A est un anneau et X un ensemble, l'ensemble $Hom_{Ens}(X, A)$ des applications ensemblistes de X dans A muni de $(\phi+\psi)(x) = \phi(x)+\psi(x)$ et $(\phi\cdot\psi)(x) = \phi(x)\cdot\psi(x)$ est un anneau de zéro l'application nulle et d'unité l'application constante égale à 1_A. Dans ce cas, $Hom_{Ens}(X, A)^\times = Hom_{Ens}(X, A^\times)$.
- On rencontre aussi beaucoup d'anneaux en analyse et en géométrie: les anneaux de fonctions continues (resp. analytique, resp. differentiable *etc.*) - à valeurs réelles ou complexes selon le cas - sur un espace topologique (resp. une variété analytique, resp. une variété differentiable *etc.*), les anneaux de fonctions intégrables sur un espace mesuré, les anneaux de séries entières *etc* .

1.4. **Morphismes d'anneaux.** Etant donnés deux anneaux A, B, un morphisme d'anneaux est une application $\phi : A \to B$ qui induit à la fois un morphisme de groupes $\phi : (A, +) \to (B, +)$ et de monoides unitaires $\phi : (A, \cdot) \to (B, \cdot)$ *i.e* qui vérifie:

(1) $\phi(a + b) = \phi(a) + \phi(b)$, $a, b \in A$;q
(2) $\phi(ab) = \phi(a)\phi(b)$, $a, b \in A$ et $\phi(1) = 1$;

On remarquera que l'application identité $Id : A \to A$ est un morphisme d'anneaux et que si $\phi : A \to B$ et $\psi : B \to C$ sont des morphismes d'anneaux alors $\psi \circ \phi : A \to C$ est un morphisme d'anneaux. On notera $Hom_{Anneau}(A, B)$ (ou simplement $Hom(A, B)$) l'ensemble des morphismes d'anneaux $\phi : A \to B$ et, si $A = B$, $End_{Anneau}(A) := Hom_{Anneau}(A, A)$ (ou simplement $End(A)$).

On dit qu'un morphisme d'anneaux $\phi : A \to B$ est injectif, (resp. surjectif, resp. un isomorphisme) si l'application d'ensembles sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $\phi : A \to B$ est un isomorphisme d'anneaux l'application inverse $\phi^{-1} : B \to A$ est automatiquement un morphisme d'anneaux. Comme un morphisme d'anneaux $\phi : A \to B$ est en particulier un morphisme de groupes, $\phi : A \to B$ est injectif si et seulement si $\ker(\phi) := \phi^{-1}(0_B) = \{0_A\}$. On notera aussi $\mathrm{im}(\phi) := \phi(A)$.

Si $\phi : A \to B$ est un morphisme d'anneaux, on vérifie que $\phi(A^\times) \subset B^\times$ et que $\phi : A \to B$ induit par restriction un morphisme de groupes $\phi : A^\times \to B^\times$.

1.5. **Sous-anneaux.** Si A est un anneau, un sous-anneau de A est un sous-ensemble $A' \subset A$ qui est à la fois un sous-groupe de $(A, +)$ et un sous-monoïde de $(A, \cdot)$ *i.e.* tel que $1_A \in A'$ et $a' - b' \in A'$, $a' \cdot b' \in A'$, $a', b' \in A'$.

Exemples.
- $\mathbb{Z}$ est un sous anneau de $\mathbb{Q}$, $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$, $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.
- Si M est un espace vectoriel sur un corps commutatif k, $End_k(M)$ est un sous-anneau de $End_{Grp}(M)$.
- $Z(A) := \{a \in A \mid a \cdot b = b \cdot a,\ b \in A\} \subset A$ est un sous-anneau de A, appelé le centre de A. Par exemple $Z(End_k(M)) = kId_M$ et $Z(A) = A$ si et seulement si A est commutatif.
- Si $\phi : A \to B$ est un morphisme d'anneaux, et $A' \subset A$ (resp. $B' \subset B$) est un sous-anneau alors $\phi(A') \subset B$ (resp. $\phi^{-1}(B') \subset A$) est un sous-anneau. En particulier, $\mathrm{im}(\phi) \subset B$ est un sous-anneau mais $\ker(\phi) \subset A$ n'est un sous-anneau que si A ou B est l'anneau nul, sinon il ne contient pas 1 (on verra un peu plus loin que $\ker(\phi)$ est ce qu'on appelle un idéal).

1.6. **A-algèbre.** Soit A un anneau commutatif. Une A-algèbre est un couple (B, ϕ) où B est un anneau et $\phi : A \to B$ est un morphisme d'anneaux tel que $\mathrm{im}(\phi) \subset Z(B)$. On notera en général $\phi : A \to B$ ou simplement (lorsque la donnée de $\phi : A \to B$ ne peut prêter à confusion) B la A-algèbre (B, ϕ). Etant données deux A-algèbres $\phi_B : A \to B$, $\phi_C : A \to C$, un morphisme de A-algèbres est un morphisme d'anneaux $\phi : B \to C$ tel que $\phi \circ \phi_B = \phi_C$. On remarquera que l'application identité $Id : B \to B$ est un morphisme de A-algèbres et que si $\phi : B \to C$ et $\psi : C \to D$ sont des morphismes de A-algèbres alors $\psi \circ \phi : B \to D$ est un morphisme de A-algèbres. On notera $Hom_{A-alg}(B, C)$ (ou simplement $Hom_A(B, C)$) l'ensemble des morphismes de A-algèbres $\phi : B \to C$ et, si $B = C$, $End_{A-alg}(B) := Hom_{A-alg}(B, C)$ (ou simplement $End_A(B)$). On dit encore qu'un morphisme de A-algèbres $\phi : B \to C$ est injectif, (resp. surjectif, resp. un isomorphisme) si l'application d'ensembles sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $\phi : B \to C$ est un isomorphisme de A-algèbres l'application inverse $\phi^{-1} : C \to B$ est automatiquement un morphisme de A-algèbres.

Remarque. On verra dans la partie II du cours, qu'une A-algèbre $\phi : A \to B$ est aussi la même chose qu'un anneau B muni d'une structure de A-module tel que $A \cdot 1_B \subset Z(B)$ et qu'avec cette terminologie un morphisme de A-algèbres est un morphisme d'anneaux qui est aussi un morphisme de A-modules.

Exemples.
- Le morphisme caractéristique $c_A : \mathbb{Z} \to A$, $1 \to 1_A$ munit tout anneau A d'une structure de $\mathbb{Z}$-algèbre canonique et tout morphisme d'anneaux $\phi : A \to B$ est automatiquement un morphisme de $\mathbb{Z}$-algèbres pour ces structures (*i.e.* $\phi \circ c_A = c_B$).
- L'inclusion $\iota_A : Z(A) \hookrightarrow A$ munit tout anneau A d'une structure de $Z(A)$-algèbre canonique.
- Si A, B sont des anneaux commutatifs, tout morphisme d'anneaux $\phi : A \to B$ munit B d'une structure de A-algèbre.

2. Premières constructions universelles

Dans cette section, nous allons construire des anneaux qui apparaissent naturellement comme "objets universels" *i.e.* représentant certains foncteurs naturels de la catégorie des anneaux vers la catégorie des ensembles ou, plus concrètement, vérifiant certaines "propriétés universelles". Il s'agit là de cas particuliers d'une procédure catégorielle générale - *cf.* 13.3.1. Si ces anneaux universels existent, ils sont toujours tautologiquement uniques à unique isomorphisme d'anneaux près. Dans la pratique, pour manipuler les anneaux universels, on n'a que rarement besoin d'en connaitre une construction explicite (c'est leur "propriété universelle" qui importe); il faut cependant en passer par là pour démontrer leur existence.

2.1. **Produits.**

2.1.1. **Lemme.** (Propriété universelle du produit) *Pour toute famille d'anneaux A_i, $i \in I$ il existe un anneau Π et une famille de morphisme d'anneaux $p_i : \Pi \to A_i$, $i \in I$, uniques à unique isomorphisme d'anneaux près*[1]*, tels que pour tout anneau A et famille de morphisme d'anneaux $\phi_i : A \to A_i$, $i \in I$, il existe un unique morphisme d'anneaux $\phi : A \to \Pi$ tel que $p_i \circ \phi = \phi_i$, $i \in I$.*

Preuve. On procède en deux temps.

- Existence / Construction. On munit le produit ensembliste $\prod_{i\in I} A_i$ d'une structure d'anneau en posant, pour $\underline{a} = (a_i)_{i\in I}$, $\underline{b} = (b_i)_{i\in I} \in \prod_{i\in I} A_i$

$$\underline{a} + \underline{b} = (a_i + b_i)_{i\in I}, \quad \underline{a} \cdot \underline{b} = (a_i \cdot b_i)_{i\in I}$$

  On a alors $0 = (0_{A_i})_{i\in I}$, $1 = (1_{A_i})_{i\in I}$. De plus, les projections $p_i : \prod_{i\in I} A_i \to A_i$, $\underline{a} \to a_i$, $i \in I$ sont automatiquement des morphismes d'anneaux.
  Vérifions que $\Pi := \prod_{i\in I} A_i$ et les $p_i : \prod_{i\in I} A_i \to A_i$, $\underline{a} \to a_i$, $i \in I$ conviennent. Si $\phi : A \to \prod_{i\in I} A_i$ existe, la condition $p_i \circ \phi = \phi_i$, $i \in I$ force $\phi(a) = (\phi_i(a))_{i\in I}$, $a \in A$. Cela montre l'unicité de ϕ sous réserve de son existence. Pour conclure, il faut vérifier que ϕ défini par $\phi(a) = (\phi_i(a))_{i\in I}$, $a \in A$ est bien un morphisme d'anneaux, ce qui résulte immédiatement des définitions.
- Unicité. Supposons que l'on ait un autre anneau Π' et une famille de morphisme d'anneaux $p'_i : \Pi' \to A_i$, $i \in I$ vérifiant aussi la propriété de 2.1.1. On a alors, formellement:
  (1) un unique morphisme d'anneaux $\phi : \Pi \to \Pi'$ tel que $p'_i \circ \phi = p_i$, $i \in I$;
  (2) un unique morphisme d'anneaux $\phi' : \Pi' \to \Pi$ tel que $p_i \circ \phi' = p'_i$, $i \in I$;
  (3) un unique morphisme d'anneaux $\psi : \Pi \to \Pi$ tel que $p_i \circ \psi = p_i$, $i \in I$;
  (4) un unique morphisme d'anneaux $\psi' : \Pi' \to \Pi'$ tel que $p'_i \circ \psi' = p'_i$, $i \in I$.
  Mais on voit que dans (3) $\psi = \phi' \circ \phi$ et $\psi = Id_\Pi$ conviennent. L'unicité de ψ dans (3) impose donc $\phi' \circ \phi = Id_\Pi$. Le même argument dans (4) montre que $\phi \circ \phi' = Id_{\Pi'}$. Autrement dit, les morphismes d'anneaux $\phi : \Pi \to \Pi'$ de (1) et $\phi' : \Pi' \to \Pi$ de (2) sont inverses l'un de l'autre. □

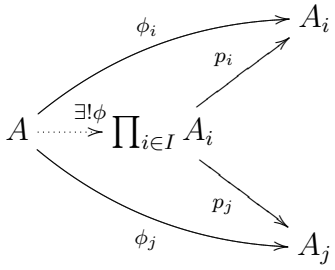
Remarques.

(1) La preuve de l'unicité de l'anneau produit $p_i : \Pi \to A_i$, $i \in I$ dans 2.1.1 est formelle et n'utilise que le caractère *uni*verselle (*i.e.* l'unicité du morphisme d'anneaux $\phi : A \to \Pi$ dans 2.1.1) de la propriété 2.1.1; nous ne reproduirons pas l'argument lorsque nous construirons d'autres objets universels (*cf.* 13.3.1 pour l'argument catégoriel général).

(2) On peut aussi réécrire 2.1.1 en disant que, pour tout anneau A l'application canonique

$$\mathrm{Hom}(A, \prod_{i\in I} A_i) \to \prod_{i\in I} \mathrm{Hom}(A, A_i), \ \phi \to (p_i \circ \phi)_{i\in I}$$

est bijective ou encore, plus visuellement:



[1] *i.e.* si $p'_i : \Pi' \to A_i$, $i \in I$ est une autre famille de morphismes d'anneaux vérifiant la propriété de 2.1.1, il existe un unique isomorphisme d'anneaux $\phi : \Pi \tilde{\to} \Pi'$ tel que $p'_i \circ \phi = p_i$, $i \in I$.

Cette réécriture fait apparaitre clairement que le foncteur (hors programme) représenté par $p_i : \Pi \to A_i$, $i \in I$ est le foncteur

$$\Pi^{\underline{A}} = \prod_{i\in I} Hom(-, A_i) : Ann^{op} \to Ens.$$

2.1.2. Soit $\phi_i : A_i \to B_i$, $i \in I$ une famille de morphismes d'anneaux. En appliquant la propriété universelle des $p_j : \prod_{i\in I} B_i \to B_j$, $j \in I$ à la famille de morphismes d'anneaux

$$\prod_{i\in I} A_i \stackrel{p_j}{\to} A_j \stackrel{\phi_j}{\to} B_j,\ j \in I$$

on obtient un unique morphisme d'anneaux $\phi := \prod_{i\in I} \phi_i : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$ tel que $p_i \circ \phi = \phi_i \circ p_i$, $i \in I$; explicitement $\phi(\underline{a}) = (\phi_i(a_i)_{i\in I}$.

2.1.3 Si $A_i = A$, $i \in I$, on note $\prod_{i\in I} A_i = A^I$. On a un isomorphisme canonique d'anneaux

$$\begin{array}{lll} Hom_{Ens}(I, A) & \tilde{\to} & A^I \\ \varphi & \to & (\varphi_i)_{i\in I} \\ i \mapsto a_i & \leftarrow & (a_i)_{i\in I} \end{array}$$

On notera qu'on a un morphisme d'anneaux injectif canonique $\Delta_A : A \hookrightarrow A^I$, $a \to (i \to a(i) = a)$ appelé morphisme diagonal (et qui, si A est commutatif, fait de A^I une A-algèbre de façon canonique).

Pour tout $\underline{a} = (a_i)_{i\in I} \in A^I$ notons $supp(\underline{a}) := \{i \in I \mid a_i \neq 0\} \subset I$ le *support* de $\underline{a}$. Notons

$$A^{(I)} := \{\underline{a} \in A^I \mid |supp(\underline{a})| < +\infty\} \subset A^I.$$

On observera que $A^{(I)} \subset A^I$ est stable par différence et produit mais que, si I est infini, ce n'est pas un sous-anneau de A^I car il ne contient pas 1_{A^I}.

2.2. **Algèbres de polynômes.** Soit A un anneau commutatif.

2.2.1. **Lemme.** (Propriété universelle de la A-algèbre des polynômes à une indéterminée) *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A : A \to P$ munie d'un élément $p \in P$, uniques à unique isomorphisme de A-algèbres près*[2]*, tels que pour toute A-algèbre $\phi : A \to B$ et $b \in B$, il existe un unique morphisme de A-algèbres $ev_b^\phi : P \to B$ tel que $ev_b^\phi(p) = b$.*

Preuve. Comme pour 2.1.1, on procède en deux temps.

- Existence / construction. Comme on vient de l'observer, le sous-ensemble $A^{(\mathbb{N})}$ de $A^{\mathbb{N}}$ est stable par différence et produit mais ce n'est pas un sous-anneau de $A^{\mathbb{N}}$ car il ne contient pas $1_{A^{\mathbb{N}}}$. En utilisant que $(\mathbb{N}, +)$ est un monoide on peut cependant faire un anneau de $A^{(\mathbb{N})}$, en le munissant d'une autre multiplication que celle héritée de $A^{\mathbb{N}}$. Notons $e_n := (\delta_{m,n}1_A)_{m\in\mathbb{N}}$, $n \in \mathbb{N}$ et pour $a \in A$, $ae_n := (\delta_{m,n}a)_{m\in\mathbb{N}}$, $n \in \mathbb{N}$; $A^{(\mathbb{N})}$ contient les ae_n, $n \in \mathbb{N}$, $a \in A$ et, par définition, tout élément $\underline{a} \in A^{(\mathbb{N})}$ s'écrit de façon unique sous la forme $\underline{a} = \sum_{n\in\mathbb{N}} a_n e_n$. Munissons donc $A^{(\mathbb{N})}$ de l'addition héritée de celle de $A^{\mathbb{N}}$ et du produit 'de convolution' $*$ défini sur les éléments e_n, $n \in \mathbb{N}$ par $e_m * e_n = e_{m+n}$ et en général par

$$(2.2.1.1)\ \ (\sum_{n\in\mathbb{N}} a_n e_n) * (\sum_{n\in\mathbb{N}} b_n e_n) = \sum_{n\in\mathbb{N}} (\sum_{i,j\in\mathbb{N}, i+j=n} a_i b_j) e_n.$$

  On vérifie facilement que $(A^{(\mathbb{N})}, +, *)$ est un anneau commutatif ayant pour unité e_0. L'application canonique $\iota_A : A \to A^{(\mathbb{N})}$, $a \to ae_0$ est un morphisme d'anneaux. On note traditionnellement cet

[2] *i.e.* si $\iota'_A{}' : A' \to P'$, $p' \in P'$ vérifient la propriété de 2.2.1, il existe un unique isomorphisme de A-algèbres $\phi : P \tilde{\to} P'$ tel que $\phi(p) = p'$.

anneau $(A[X], +, \cdot)$ et on dit que $\iota : A \to A[X]$ est la A-algèbre des polynômes à une inderminée. On pose aussi $X^n := e_n$, $n \in \mathbb{N}$ et $1 := X^0$ de sorte que (2.2.1) se réécrit de façon plus intuitive sous la forme

$$(2.2.1.2)\ \ (\sum_{n\in\mathbb{N}} a_n X^n)(\sum_{n\in\mathbb{N}} b_n X^n) = \sum_{n\in\mathbb{N}} (\sum_{i,j\in\mathbb{N}, i+j=n} a_i b_j) X^n.$$

Vérifions que $\iota_A : A \to P = A[X]$ munie de $p = X$ conviennent. Si $ev_b^\phi : A[X] \to B$ existe, on a par définition d'un morphisme de A-algèbres:

$$ev_b^\phi(\sum_{n\geq 0} a_n X^n) = \sum_{n\geq 0} ev_b^\phi(a_n) ev_b^\phi(X)^n = \sum_{n\geq 0} \phi(a_n) b^n,$$

d'où l'unicité de ev_b^ϕ sous réserve d'existence. Pour conclure, il faut vérifier que ev_b^ϕ défini par $ev_b^\phi(\sum_{n\geq 0} a_n X^n) = \sum_{n\geq 0} \phi(a_n) b^n$, est bien un morphisme d'anneaux, ce qui là encore résulte immédiatement des définitions.

- Unicité. C'est le même argument formel que celui utilisé dans 2.1.1. □

On adopte en général la notation plus intuitive $ev_b^\phi(P) = P(b)$ et on dit que ev_b^ϕ est le morphisme d'évaluation en b.

Remarque. On peut aussi réécrire 2.2.1 en disant que, pour toute A-algèbre $A \to B$ l'application canonique

$$\mathrm{Hom}_A(A[X], B) \to B,\ f \to f(X)$$

est bijective. Cette réécriture fait apparaitre clairement que le foncteur (hors programme) représenté par $(\iota_A : A \to A[X],\ X)$ est le foncteur d'oubli $A\text{-}Alg \to Ens$.

2.2.2. Soit $\phi : A \to B$ un morphisme d'anneaux commutatifs. En appliquant la propriété universelle de $\iota_A : A \to A[X]$ à la A-algèbre $A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[X]$ on obtient un unique morphisme de A-algèbres $\tilde{\phi} := ev^X_{\phi\circ\iota_B} : A[X] \to B[X]$ tel que $\iota_B \circ \phi = \phi \circ \iota_A$; explicitement $\tilde{\phi}(\sum_{n\geq 0} a_n X^n) = \sum_{n\geq 0} \phi(a_n) X^n$.

2.2.3. *Une reformulation de 2.2.1.* Ce qui nous a permis de définir le produit $*$ sur $A^{(\mathbb{N})}$ et le fait que $(\mathbb{N}, +)$ est un monoïde: on a utilisé l'addition pour définir $e_n * e_m = e_{n+m}$, l'associativité de $*$ résulte de celle de $+$ sur $\mathbb{N}$ et le fait que e_0 soit l'unité de $A^{(\mathbb{N})}$ du fait que 0 est l'unité de $\mathbb{N}$. Pour un monoïde $(M, \cdot)$ quelconque, l'application

$$\mathrm{Hom}_{Mono}(\mathbb{N}, M) \to M,\ f \to f(1)$$

est bijective d'inverse l'application qui à $m \in M$ associe le morphisme de monoïdes $f_m : (\mathbb{N}, +) \to (M, \cdot)$, $n \to m^n (= m \cdots m\ n \text{ fois})$. Dans 2.2.1, se donner $p \in P$ et $b \in B$ revient donc à se donner des morphismes de monoïdes $\nu_A : (\mathbb{N}, +) \to (P, \cdot)$, $n \to p^n$ et $\nu : (\mathbb{N}, +) \to (B, \cdot)$, $n \to b^n$ et la condition $ev_b^\phi(p) = b$ signifie que $ev_b^\phi \circ \nu_A = \nu$. Avec ce point de vue, on peut reformuler 2.2.1 comme suit.

2.2.1' **Lemme.** (Propriété universelle de la A-algèbre des polynômes à une indéterminée) *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A : A \to P$ et un morphisme de monoïdes $\nu_A : (\mathbb{N}, +) \to (P, \cdot)$, uniques à unique isomorphisme de A-algèbres près, tels que pour toute A-algèbre $\phi : A \to B$ et tout morphisme de monoïdes $\nu : (\mathbb{N}, +) \to (B, \cdot)$, il existe un unique morphisme de A-algèbres $\widetilde{\nu} : P \to B$ tel que $\widetilde{\nu} \circ \nu_A = \nu$.*

Remarque. On peut aussi réécrire 2.2.1' en disant que, pour toute A-algèbre $\phi : A \to B$ l'application canonique

$$\mathrm{Hom}_A(A[X], B) \to \mathrm{Hom}_{Mono}(\mathbb{N}, B),\ f \to f \circ \nu_A$$

est bijective. Explicitement, $\nu_A : (\mathbb{N}, +) \to (A[X], \cdot)$ est le morphisme qui envoie n sur X^n donc si $f : A[X] \to B$ est un morphisme de A-algèbres, $f \circ \nu_A : (\mathbb{N}, +) \to (B, \cdot)$ est le morphisme qui envoie n sur $f(X)^n$. Cette réécriture fait apparaitre clairement que le foncteur (hors programme) représenté par $(\iota_A : A \to A[X],\ X)$ est le foncteur

$$\mathrm{Hom}_{Mono}(\mathbb{N}, -) : A\text{-}Alg \to Ens.$$

2.2.4. Avec le point de vue développé dans 2.2.3, on peut faire la construction précédente en remplaçant $(\mathbb{N}, +)$ par n'importe quel monoïde $(N, \cdot)$ (non nécessairement commutatif, non nécessairement dénombrable) d'unité 1_N. Notons toujours $e_n := (\delta_{m,n} 1_A)_{m\in N}$, $n \in N$ et pour $a \in A$, $ae_n := (\delta_{m,n} a)_{m\in N}$, $n \in N$; $A^{(N)}$ contient les ae_n, $n \in N$, $a \in A$ et, par définition, tout élément $\underline{a} \in A^{(N)}$ s'écrit de façon unique sous la forme $\underline{a} = \sum_{n\in N} a_n e_n$. En munissant $A^{(N)}$ de l'addition héritée de celle de A^N et du produit 'de convolution' $*$ défini sur les éléments e_n, $n \in N$ par $e_m * e_n = e_{m\cdot n}$ et en général par

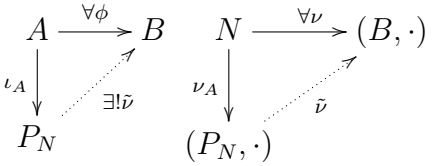
$$(2.2.4.1)\quad (\sum_{n\in N} a_n e_n) * (\sum_{n\in N} b_n e_n) = \sum_{n\in N} (\sum_{i,j\in N, i\cdot j=n} a_i b_j) e_n.$$

on obtient un anneau (commutatif si $(N, \cdot)$ est commutatif) $(A^{(N)}, +, *)$ ayant pour unité e_{1_N}. L'application canonique $\iota_A : A \to A^{(N)}$, $a \to ae_{1_N}$ est un morphisme d'anneaux et l'application $\nu_A : N \to A^{(N)}$, $n \to e_n$ prend ses valeur dans $A^{(N)} \setminus \{0\}$ et induit un morphisme de monoïdes $\nu_A : (N, \cdot) \to (A^{(N)}, *)$. On note traditionnellement cet anneau $(A[N], +, \cdot)$ et on dit que $\iota_A : A \to A[N]$ est la A-algèbre du monoïde $(N, \cdot)$. On pose aussi $n := e_n$, $n \in N$ et $1 := 1_N$ de sorte que (2.2.4.1) se réécrit de façon plus intuitive sous la forme

$$(2.2.4.2)\quad (\sum_{n\in N} a_n n) * (\sum_{n\in N} b_n n) = \sum_{n\in N} (\sum_{i,j\in N, i\cdot j=n} a_i b_j) n.$$

2.2.5. **Lemme.** (Propriété universelle de la A-algèbre du monoïde $(N, \cdot)$) *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A : A \to P_N$ et un morphisme de monoïdes $\nu_A : (N, \cdot) \to (P_N, \cdot)$, uniques à unique isomorphisme de A-algèbres près, tels que pour toute A-algèbre $\phi : A \to B$ et tout morphisme de monoïdes $\nu : (N, \cdot) \to (B, \cdot)$ il existe un unique morphisme de A-algèbres $\tilde{\nu} : P_N \to B$ tel que $\tilde{\nu} \circ \nu_A = \nu$.*

Visuellement:



Preuve. Similaire à celle de 2.2.1 en vérifiant que $\iota_A : A \to A[N]$ convient. □

Remarque. On peut aussi réécrire 2.2.5 en disant que, pour toute A-algèbre $\phi : A \to B$ l'application canonique

$$\mathrm{Hom}_A(A[N], B) \to \mathrm{Hom}_{Mono}(N, B),\ f \to f \circ \nu_A$$

est bijective. Son inverse est l'application qui à $\nu : (N, \cdot) \to (B, \cdot)$ associe l'unique morphisme de A-algèbres $\tilde{\nu} : A[N] \to B$ tel que $\tilde{\nu}(n) = \nu(n)$ (donc $\tilde{\nu}(\sum_{n\in N} a_n n) = \sum_{n\in N} \phi(a_n)\nu(n)$). Cette réécriture fait apparaitre clairement que le foncteur (hors programme) représenté par $(\iota_A : A \to A[N],\ \nu_A)$ est le foncteur

$$\mathrm{Hom}_{Mono}(N, -) : A\text{-}Alg \to Ens.$$

Exemples. Si on prend

(1) $(N,\cdot)=(\mathbb{N},+)$ on retrouve $A[\mathbb{N}]=A[X]$.

(2) $(N,\cdot)=(\mathbb{N}^r,+)$ où $+$ est l'addition termes à termes (pour $\underline{m}=(m_1,\dots,m_r),\underline{n}:=(n_1,\dots,n_r)\in\mathbb{N}^r$, $\underline{m}+\underline{n}=(m_1+n_1,\dots,m_r+n_r)\in\mathbb{N}^r$). Dans ce cas, on note $\underline{X}^{\underline{n}}:=X_1^{n_1}\cdots X_r^{n_r}:=e_{\underline{n}}$, $\underline{n}\in\mathbb{N}^r$ avec la convention $X_i^0=1$, $i=1,\dots,r$, et $1:=\underline{X}^{\underline{0}}$ de sorte que (2.2.4.1)/(2.2.4.2) se réécrit de façon plus intuitive sous la forme

$$(\sum_{\underline{n}\in\mathbb{N}^r}a_{\underline{n}}\underline{X}^{\underline{n}})(\sum_{\underline{n}\in\mathbb{N}^r}b_{\underline{n}}\underline{X}^{\underline{n}})=\sum_{\underline{n}\in\mathbb{N}}(\sum_{\underline{i},\underline{j}\in\mathbb{N}^r,\underline{i}+\underline{j}=\underline{n}}a_{\underline{i}}b_{\underline{j}})\underline{X}^{\underline{n}}.$$

On note également $A[\underline{X}]:=A[X_1,\dots,X_r]:=A[\mathbb{N}^r]$ et on dit que $\iota_A:A\to A[X_1,\dots,X_r]$ est la A-algèbre des polynômes à r inderminées. Comme, en notant

$$C_r(B):=\{\underline{b}=(b_1,\dots,b_r)\in B^r\mid b_ib_j=b_jb_i,\ 1\leq i,j\leq r\},$$

et $\epsilon_i=(\delta_{i,j})_{1\leq j\leq n}$, $i=1,\dots,n$, l'application

$$\mathrm{Hom}_{Mono}(\mathbb{N}^r,B)\to C_r(B),\ \nu\to(\nu(\epsilon_1),\dots,\nu(\epsilon_r))$$

est bijective, on peut reformuler 2.2.5 dans ce cas particulier de la façon suivante.

(Propriété universelle de la A-algèbre des polynômes à n indéterminées) *Pour tout anneau commutatif A et entier $r\geq 1$, il existe une A-algèbre $\iota_A:A\to P$ munie d'un r-uplet $\underline{p}\in P^r$, uniques à unique isomorphisme de A-algèbres près*[3]*, tels que pour toute A-algèbre $\phi:A\to B$ et $\underline{b}\in C_r(B)$, il existe un unique morphisme de A-algèbres $ev_{\underline{b}}^{\phi}:P\to B$ tel que $ev_{\underline{b}}^{\phi}(p_i)=b_i$, $i=1,\dots,r$.*

Ou encore, l'application

$$\mathrm{Hom}_A(A[X_1,\dots,X_r],B)\to C_r(B),\ f\to(f(X_1),\dots,f(X_r))$$

est bijective. Son inverse est l'application qui à $\underline{b}=(b_1,\dots,b_r)\in C_r(B)$ associe l'unique morphisme de A-algèbres $ev_{\underline{b}}^{\phi}:A[X_1,\dots,X_r]\to B$ tel que $ev_{\underline{b}}^{\phi}(X_i)=b_i$, $i=1,\dots r$ (donc $ev_{\underline{b}}^{\phi}(\sum_{\underline{n}\in\mathbb{N}^r}a_{\underline{n}}\underline{X}^{\underline{n}})=\sum_{\underline{n}\in\mathbb{N}^r}\phi(a_{\underline{n}})\underline{b}^{\underline{n}}$). On adopte en général la notation plus intuitive $ev_{\underline{b}}^{\phi}(P)=P(b_1,\dots,b_r)$ et on dit que $ev_{\underline{b}}^{\phi}$ est le morphisme d'évaluation en $\underline{b}$. Cette réécriture fait apparaitre clairement que le foncteur (hors programme) représenté par $(\iota_A:A\to A[\underline{X}],\underline{X})$ est le foncteur

$$C_r(-):A\text{-}Alg\to Ens.$$

(3) Pour $(N,\cdot)$ un groupe, pour toute A-algèbre $\phi:A\to B$, tout morphisme de monoïdes $\nu:(N,\cdot)\to(B,\cdot)$ est automatiquement à valeur dans le groupe $(B^\times,\cdot)$. On dit dans ce cas que $A[N]$ est la A-algèbre du groupe $(N,\cdot)$.

Par exemple, pour $(N,\cdot)=(\mathbb{Z},+)$, on obtient la A-algèbre (notations: $A[X,X^{-1}]:=A[\mathbb{Z}]$, $X^n:=e_n$, $n\in\mathbb{Z}$ donc en particulier $X^nX^{-n}=e_ne_{-n}=e_{n-n}=e_0=1$) des polynômes de Laurent à une indéterminée. Comme l'application

$$\mathrm{Hom}_{Mono}(\mathbb{Z},B)\to B^\times,\ \nu\to\nu(1)$$

est bijective, on peut reformuler 2.2.5 dans ce cas particulier de la façon suivante.

(Propriété universelle de la A-algèbre des polynômes de Laurent à une indéterminée) *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A:A\to P$ munie d'un élément $p\in P^\times$, uniques*

[3] *i.e.* si $\iota'_{A'}:A'\to P'$, $\underline{p''}\in P'^{\,r}$ vérifient la propriété de 2.2.5 comme reformulée ici, il existe un unique isomorphisme de A-algèbres $\phi:P\tilde{\to}P'$ tel que $\phi(p_i)=p'_i$, $i=1,\dots,r$.

à unique isomorphisme de A-algèbres près, tels que pour toute A-algèbre $\phi : A \to B$ et $b \in B^\times$, il existe un unique morphisme de A-algèbres $ev_b^\phi : P \to B$ tel que $ev_b^\phi(p) = b$.

Ou encore, l'application

$$\mathrm{Hom}_A(A[X, X^{-1}], B) \to B^\times,\ f \to f(X)$$

est bijective. Cette réécriture fait apparaitre clairement que le foncteur (hors programme) représenté par $(\iota_A : A \to A[X, X^{-1}],\ X)$ est le foncteur "groupe des inversibles"

$$(-)^\times : A\text{-}Alg \to Ens.$$

De même, pour $(N, \cdot) = (\mathbb{Z}^r, +)$, on obtient la A-algèbre (notations: $A[X_1, X_1^{-1}, \cdots, X_r, X_r^{-1}] := A[\mathbb{Z}^r]$, $\underline{X}^{\underline{n}} := X_1^{n_1} \cdots X_r^{n_r} := e_{\underline{n}}$, $\underline{n} \in \mathbb{Z}^r$ donc en particulier, $\underline{X}^{\underline{n}}\underline{X}^{-\underline{n}} = e_{\underline{n}}e_{-\underline{n}} = e_{\underline{n}-\underline{n}} = e_0 = 1$) des polynômes de Laurent à r indéterminées. Comme, en notant

$$C_r(B^\times) := \{\underline{b} = (b_1, \ldots, b_r) \in B^{\times\, r} \mid b_i b_j = b_j b_i,\ 1 \leq i, j \leq r\},$$

et $\epsilon_i = (\delta_{i,j})_{1 \leq j \leq n}$, $i = 1, \ldots, n$, l'application

$$\mathrm{Hom}_{Mono}(\mathbb{Z}^r, B) \to C_r(B^\times),\ \nu \to (\nu(\epsilon_1), \ldots, \nu(\epsilon_r))$$

est bijective, on peut reformuler 2.2.5 dans ce cas particulier de la façon suivante.

(Propriété universelle de la A-algèbre des polynômes de Laurent à n indéterminées) *Pour tout anneau commutatif A et entier $r \geq 1$, il existe une A-algèbre $\iota_A : A \to P$ munie d'un $r-$uplet$\underline{p} \in C_r(P^\times)$, uniques à unique isomorphisme de A-algèbres près, tels que pour toute A-algèbre $\phi : A \to B$ et $\underline{b} \in C_r(B^\times)$, il existe un unique morphisme de A-algèbres $ev_{\underline{b}}^\phi : P \to B$ tel que $ev_{\underline{b}}^\phi(p_i) = b_i$, $i = 1, \ldots, r$.*

Ou encore, l'application

$$\mathrm{Hom}_A(A[X_1, X_1^{-1}, \cdots, X_r, X_r^{-1}], B) \to C_r(B^\times),\ f \to (f(X_1), \ldots, f(X_r))$$

est bijective. Cette réécriture fait apparaitre clairement que le foncteur (hors programme) représenté par $(\iota_A : A \to A[X_1, X_1^{-1}, \cdots, X_r, X_r^{-1}],,\ \underline{X})$ est le foncteur

$$C_r((-)^\times) : A\text{-}Alg \to Ens.$$

2.2.6. Si $\phi : A \to B$ est un morphisme d'anneaux commutatifs et $\nu : N_1 \to N_2$ un morphisme de monoïdes, la propriété universelle de $\iota_A : A \to A[N_1]$ appliquée avec $A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[N_2]$ et $N_1 \xrightarrow{\nu} N_2 \xrightarrow{\nu_B} (B[N_2], \cdot)$ donne un unique morphisme de A-algèbres $\tilde{\phi}^\nu : A[N_1] \to B[N_2]$ tel que $\nu_B \circ \nu = \tilde{\phi}^\nu \circ \nu_A$. Explicitement $\tilde{\phi}^\nu(\sum_{n \in N_1} a_n n) = \sum_{n \in N_1} \phi(a_n)\nu(n)$. Autrement dit l'application

$$\begin{array}{rccc} \tilde{(-)}^\nu : & \mathrm{Hom}_{Mono}(N_1, N_2) & \hookrightarrow & \mathrm{Hom}_A(A[N_1], B[N_2]) \\ & \nu : N_1 \to N_2 & \to & \tilde{\phi}^\nu : A[N_1] \to B[N_2] \end{array}$$

est injective.

2.3. **Sous-A-algèbre engendrée par une partie.** Soit $\phi : A \to B$ une A-algèbre. Une sous-A-algèbre de $\phi : A \to B$ est un sous-anneau $B' \subset B$ tel que $\mathrm{im}(\phi) \subset B'$ (noter que $Z(B) \cap B' \subset Z(B')$); le morphisme $\phi|^{B'} : A \to B'$ munit alors B' d'une structure de A-algèbre qui fait de l'inclusion $B' \subset B$ un morphisme de A-algèbres. Si $B_i \subset B$, $i \in I$ est une famille de sous-A-algèbres, $\cap_{i \in I} B_i \subset B$ est encore une sous-A-algèbre. Pour tout sous-ensemble $X \subset B$, il existe une unique sous-A-algèbre $\langle X \rangle_A \subset B$, contenant X et minimale pour $\subset$. On dit que $\langle X \rangle_A \subset B$ est la sous-A-algèbre de B engendrée par X. Explicitement $\langle X \rangle_A$ est l'intersection de tous les sous-A-algèbres de B contenant X. Si $B = \langle X \rangle_A$, on dit que X est un système de générateurs de B comme A-algèbre (ou que B est

engendré par X comme A-algèbre). Si on peut prendre X fini, on dit que B est une A-algèbre de type fini.

Lorsque les éléments de X commutent deux à deux, on note en général $A[X] := \langle X \rangle_A \subset B$ la sous-A-algèbre de B engendré par X (à ne pas confondre avec une A-algèbre de polynômes!!) et 2.2.5 nous donne un unique morphisme de A-algèbres - automatiquement surjectif - $ev_X^\phi : A[\mathbb{N}^{(X)}] \twoheadrightarrow A[X]$ tel que $ev_X^\phi(e_x) = x$ (où on note $e_x := (\delta_{x,x'})_{x' \in X} \in \mathbb{N}^X$), $x \in X$. Toute A-algèbre commutative est donc quotient d'une A-algèbre de polynômes. Si $X = \{x_1, \ldots, x_r\}$ est fini, on note plutôt $A[x_1, \ldots, x_r] := A[X]$ et 2.2.5 nous donne un unique morphisme de A-algèbres - automatiquement surjectif - $ev_{\underline{x}}^\phi : A[X_1, \cdots, X_r] \twoheadrightarrow A[x_1, \ldots, x_r]$ tel que $ev_{\underline{x}}^\phi(X_i) = x_i$, $i = 1, \ldots, r$. Toute A-algèbre commutative de type fini est donc quotient d'une A-algèbre de polynômes à n indéterminées avec $n \geq$ nombre minimal de générateurs comme A-algèbre.

Lorsque $A = \mathbb{Z}$, on parle plutôt de sous-anneau engendré par une partie.

** Dans la suite, sauf mention explicite du contraire, nous ne considérerons que des anneaux commutatifs **

3. Idéaux et quotients

3.1. **Définitions, premiers exemples.**

3.1.1. Soit A un anneau (commutatif, donc). Un idéal de A est un sous-ensemble $I \subset A$ qui est un sous-groupe de $(A, +)$ et tel que $A \cdot I \subset I$ *i.e.* tel que $a' - b' \in I$, $a', b' \in I$ et $aa' \in I$, $a \in A$, $a' \in I$. On notera $\mathcal{I}_A$ l'ensemble des idéaux de A; l'inclusion ensembliste $\subset$ munit $\mathcal{I}_A$ d'un ordre partiel. Pour un idéal $I \subset A$, on notera $V^{tot}(I) \subset \mathcal{I}_A$ le sous-ensemble des idéaux de A qui contiennent I

Exemples.
- Le singleton $\{0\}$ et A sont des idéaux de A.
- Si k est un corps commutatif, les seuls idéaux de k sont $\{0\}$ et k (et réciproquement un anneau A ne possédant que deux idéaux $\{0\}$ et A est un corps).
- Un idéal $I \subset A$ est en particulier un sous-groupe de $(A, +)$. Par exemple, les seuls candidats possibles pour les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \geq 0$ (division euclidienne). On vérifie immédiatement que les $n\mathbb{Z}$ sont bien des idéaux de $\mathbb{Z}$. Donc les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, $n \geq 1$. On notera que $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si $m|n$. La k-algèbre $k[X]$ des polynômes à une indéterminée sur un corps est également munie d'une division euclidienne et on verra que dans ce cas aussi, tous les idéaux de $k[X]$ sont de la forme $Pk[X]$, $P \in k[X]$.
- Pour tout $a \in A$, $Aa \subset A$ est un idéal. Les idéaux de cette forme sont appelés principaux. On dit qu'un anneau A principal si tous ses idéaux sont principaux et s'il est intègre. Les anneaux $\mathbb{Z}$ et $k[X]$ sont principaux. Par contre, $k[X, Y]$ n'est pas principal, par exemple l'ensemble $I := \{XP + YQ \mid P, Q \in k[X, Y]\} \subset k[X, Y]$ est un idéal qui n'est pas principal.
- Si A_i, $i \in I$ est une famille d'anneaux, et, pour chaque $i \in I$, $I_i \subset A_i$ est un idéal, $\prod_{i \in I} I_i \subset \prod_{i \in I} A_i$ est un idéal. Mais les idéaux de $\prod_{i \in I} A_i$ ne sont pas tous de cette forme. Par exemple, si I est infini, $A^{(I)} \subset A^I$ est un idéal de A^I qui n'est pas un produit d'idéaux.
- Si $I \subset A$ est un idéal, $I[X_1, \ldots, X_r] := \{\sum_{\underline{n} \in \mathbb{N}^r} a_{\underline{n}} \underline{X}^{\underline{n}} \mid a_{\underline{n}} \in I,\ \underline{n} \in \mathbb{N}^r\} \subset A[X_1, \ldots, X_r]$ est un idéal.

3.1.2. *Idéal engendré par une partie, sommes d'idéaux.* Soit $\mathcal{I} \subset \mathcal{I}_A$ une famille d'idéaux. On vérifie immédiatement que $\cap_{I \in \mathcal{I}} I \subset A$ est idéal. Pour tout sous-ensemble $X \subset A$, il existe un unique idéal $\langle\langle X \rangle\rangle_A \subset A$, contenant X et minimal pour $\subset$ *i.e.* tel que pour tout idéal $I \subset A$, $X \subset I$

implique $\langle\langle X\rangle\rangle_A \subset I$. On dit que $\langle\langle X\rangle\rangle_A \subset A$ est l'idéal engendré par X. Explicitement $\langle\langle X\rangle\rangle_A$ est l'intersection de tous les idéaux de A contenant X. On peut également décrire $\langle\langle X\rangle\rangle_A$ comme

$$\langle\langle X\rangle\rangle_A = \{\sum_{x\in X} a(x)x \mid a \in A^{(X)}\},$$

ce qui justifie la notation plus intuitive $\langle\langle X\rangle\rangle_A := \sum_{x\in X} Ax \subset A$. Si $\mathcal{I} \subset \mathcal{I}_A$ une famille d'idéaux, on note en particulier

$$\langle\langle \bigcup_{I\in\mathcal{I}} I \rangle\rangle_A := \sum_{I\in\mathcal{I}} I \subset A.$$

et on dit que $\sum_{I\in\mathcal{I}} I \subset A$ est la somme des I, $I \in \mathcal{I}$. Si $I = \sum_{x\in X} Ax$, on dit que X est un système de générateurs de I et si on peut prendre X fini, on dit que I est un idéal de type fini.

Exemples Les idéaux principaux d'un anneau A sont les idéaux engendrés par les singletons $\{a\}$, $a \in A$. En particulier, dans un anneau principal comme $\mathbb{Z}$ ou $k[X]$, tout idéal est de type fini. De façon plus surprenante, on verra que tous les idéaux de $k[X_1, \cdots, X_r]$ (et, partant, de toute k-algèbre de type fini) sont de type fini. Un anneau ayant cette propriété est dit noetherien. Par contre l'idéal $A^{(\mathbb{N})} \subset A^{\mathbb{N}}$ n'est pas de type fini (pourquoi?); en particulier, $A^{\mathbb{N}}$ n'est pas noetherien.

3.1.3. *Produits d'idéaux.* Si $I_1, \ldots, I_r \subset A$ est une famille finie d'idéaux, on note $I_1 \cdots I_r \subset A$ l'idéal *engendré* par les éléments de la forme $a_1 \cdots a_r$, $a_i \in I_i$, $i = 1, \ldots, r$. On a toujours

$$(*)\ \ I_1 \cdots I_r \subset \bigcap_{1\le i\le r} I_i \subset I_i \subset \sum_{1\le i\le r} I_i.$$

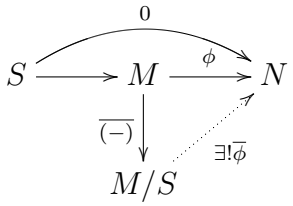
Exemple. Dans $\mathbb{Z}$, on a pour tout $m_1, \ldots, m_r \in \mathbb{Z}$, $m_1\mathbb{Z}\cdots m_r\mathbb{Z} = (m_1\cdots m_r)\mathbb{Z}$, $m_1\mathbb{Z} \cap \cdots \cap m_r\mathbb{Z} = ppcm(m_1, \ldots, m_r)\mathbb{Z}$, $m_1\mathbb{Z} + \cdots + m_r\mathbb{Z} = pgcd(m_1, \cdots, m_r)\mathbb{Z}$. Les inclusions $(*)$ ci-dessus correspondent aux relations de divisibilité

$$pgcd(m_1, \cdots, m_r) | m_i | ppcm(m_1, \cdots, m_r) | m_1 \cdots m_r.$$

3.1.4. Si $\phi : A \to B$ est un morphisme d'anneaux, et $J \subset B$ un idéal alors $\phi^{-1}(J) \subset A$ est un idéal. En particulier, $\ker(\phi) \subset A$ est un idéal. Si $\phi : A \twoheadrightarrow B$ est surjectif et $I \subset A$ est un idéal alors $\phi(I) \subset B$ est un idéal mais ce n'est plus vrai si on ne suppose pas $\phi : A \twoheadrightarrow B$ surjectif (*e.g.* si on considère l'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $\mathbb{Z}$ est tautologiquement un idéal de $\mathbb{Z}$ mais ce n'est pas un idéal de $\mathbb{Q}$).

3.2. **Quotient.**

3.2.1. *Groupes abéliens.* On rappelle que si $(M, +)$ est un groupe abélien et $S \subset M$ un sous-groupe, la relation $m \sim m' \iff m - m' \in S$ est une relation d'équivalence sur M et que, si on note $p_S : M \twoheadrightarrow M/S$ l'application qui à $m \in M$ associe sa classe d'équivalence $m + S$, l'application $M \times M \xrightarrow{-+-} M \xrightarrow{p_S} M/S$ se factorise en une application $+ : M/S \times M/S \to M/S$ (observer que si $m_1 - m_1' \in S$, $m_2 - m_2' \in S$ alors $(m_1+m_2)-(m_1'+m_2') = (m_1-m_1')+(m_2-m_2') \in S$ puisque $S \subset M$ est un sous-groupe) qui fait de $(M/S, +)$ un groupe de zéro la classe $0_M + S$ tel que la projection canonique $p_S : (M, +) \to (M/S, +)$ est un morphisme de groupes de noyau S. On rappelle qu'en outre $p_S : (M, +) \to (M/S, +)$ vérife la propriété universelle suivante: pour tout groupe abélien $(N, +)$ et pour tout morphisme de groupes $\phi : M \to N$ tel que $\ker(\phi) \subset S$ il existe un unique morphisme de groupes $\overline{\phi} : M/S \to N$ tel que $\overline{\phi} \circ p_S = \phi$. Ou encore, plus visuellement:



Ou encore que l'application canonique

$$\mathrm{Hom}_{Grp}(M/S,N)\to \ker(-|_S:\mathrm{Hom}_{Grp}(M,N)\to \mathrm{Hom}_{Grp}(S,N)),\ \ \overline{\phi}:M/S\to \overline{\phi}\circ p_S$$

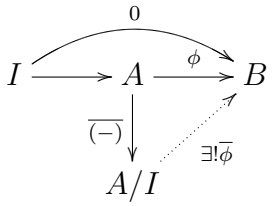
est bijective. Cette dernière réécriture fait apparaitre clairement que le foncteur représenté par $p_S:(M,+)\to(M/S,+)$ est le foncteur

$$\ker(-|_S:\mathrm{Hom}_{Grp}(M,-)\to \mathrm{Hom}_{Grp}(S,-)):Grp\to Ens.$$

3.2.2. *Anneaux.* Le noyau d'un morphisme d'anneaux $\phi:A\to B$ est un idéal. Réciproquement,

3.2.2.1 **Lemme.** (Propriété universelle du quotient) *Pour tout idéal $I\subset A$ il existe un morphisme d'anneaux $p:A\to Q$, unique à unique isomorphisme près, tel que pour tout morphisme d'anneaux $\phi:A\to B$ avec $I\subset\ker(\phi)$, il existe un unique morphisme d'anneaux $\overline{\phi}:Q\to B$ tel que $\phi=\overline{\phi}\circ p$.*

Visuellement:



Preuve. On procède en deux temps.

- Existence / construction. Comme un idéal $I\subset A$ est en particulier un sous-groupe de $(A,+)$. On dispose déjà du groupe quotient A/I, qui est un groupe abélien et de la projection canonique $p_I:=\overline{-}:A\twoheadrightarrow A/I$ qui est un morphisme surjectif de groupes, de noyau I. On peut de plus munir A/I d'une unique structure d'anneau telle que la projection canonique $p_I:=\overline{-}:A\twoheadrightarrow A/I$ est un morphisme d'anneaux. En effet, la condition que $p_I:=\overline{-}:A\twoheadrightarrow A/I$ soit un morphisme d'anneaux impose $\overline{ab}=\overline{a}\overline{b}$. Il faut donc vérifier que $\overline{ab}$ ne dépend pas du choix des représentants a, b de $\overline{a}$, $\overline{b}$. ou encore que l'application

$$\begin{array}{ccc} A\times A & \to & A/I \\ (a,b) & \to & \overline{ab}\end{array}$$

se factorise en

$$\begin{array}{ccc} A\times A & \xrightarrow{(a,b)\to\overline{ab}} & A/I\ . \\ {\scriptstyle \overline{-}\times\overline{-}}\downarrow & \nearrow_{(\overline{a},\overline{b})\to\overline{a}\cdot\overline{b}:=\overline{ab}} & \\ A/I\times A/I & & \end{array}$$

Cela résulte de la relation $(a+I)(b+I)=ab+aI+Ib+I^2\subset ab+I$, $a,b\in I$. On vérifie ensuite facilement que $(A/I,+,\cdot)$ ainsi défini vérifie bien les axiomes d'un anneau commutatif de zéro $\overline{0}$ et d'unité $\overline{1}$.

Vérifions que le morphisme d'anneaux $p_I=:\overline{-}:A\twoheadrightarrow A/I$ convient. Soit $\phi:A\to B$ un morphisme d'anneaux tel que $I\subset\ker(\phi)$. Si $\overline{\phi}:A/I\to B$ existe, la condition $\phi=\overline{\phi}\circ p$ force $\overline{\phi}(\overline{a})=\phi(a)$,

$a \in A$. Cela montre l'unicité de $\overline{\phi}$ sous réserve de son existence. Il reste à voir que $\overline{\phi} : A/I \to B$ est automatiquement un morphisme d'anneaux. On sait déjà que c'est un morphisme de groupes additifs, donc il suffit de vérifier la compatibilité au produit. Cela résulte des définitions:

$$\overline{\phi}(\overline{a}\overline{b}) \overset{(1)}{=} \overline{\phi}(\overline{ab}) \overset{(2)}{=} \phi(ab) \overset{(3)}{=} \phi(a)\phi(b) \overset{(4)}{=} \overline{\phi}(\overline{a})\overline{\phi}(\overline{b}),$$

où (1) est par construction du produit sur A/I, (2) et (4) est la relation $\phi = \overline{\phi} \circ \overline{-}$ et (3) est le fait que ϕ est un morphisme d'anneaux.

- Unicité. C'est le même argument formel que celui utilisé dans 2.1.1. □

Par construction $p_I : A \twoheadrightarrow A/I$ est surjectif de noyau I.

Remarque. On peut aussi réécrire 3.2.1 en disant que, pour tout anneau B l'application canonique

$$\mathrm{Hom}_{Anneau}(A/I, B) \to \ker(-|_I : \mathrm{Hom}_{Anneau}(A, B) \to \mathrm{Hom}_{Grp}(I, B)), \quad \overline{\phi} : A/I \to \overline{\phi} \circ p_I$$

est bijective. Cette dernière réécriture fait apparaitre clairement que le foncteur représenté par $p_I : A \to A/I$ est le foncteur

$$\ker(-|_I : \mathrm{Hom}_{Anneau}(A, -) \to \mathrm{Hom}_{Grp}(I, -)) : Anneaux \to Ens.$$

En particulier, tout morphisme d'anneaux $\phi : A \to B$ se décompose de façon canonique sous la forme

$$\begin{array}{ccccc} A & & \xrightarrow{\phi|^{\mathrm{im}(\phi)}} & & \mathrm{im}(\phi) \hookrightarrow B \\ \Big\downarrow{\scriptstyle =} & & \overset{\simeq}{\nearrow}_{\overline{\phi}} & & \\ A/\ker(\phi) & & & & \end{array}$$

Exemples. (Caractéristique d'un anneau) Le noyau du morphisme caractéristique $c_A : \mathbb{Z} \to A$ est un idéal de $\mathbb{Z}$ donc de la forme $\ker(c_A) = n\mathbb{Z}$ pour un unique entier $n \geq 0$, appelé la caractéristique de A.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0;
- $\mathbb{Z}/n$ est de caractéristique n, $n \geq 0$;
- Si $A' \subset A$ est un sous-anneau, A et A' ont même caractéristique. En particulier A, A^I, $A[X]$ ont même caractéristique. Si $\mathcal{P}$ est un ensemble infini de nombres premiers distincts, l'anneau produit $\prod_{p \in \mathcal{P}} \mathbb{Z}/p$ est de caractéristique 0.
- Si $\phi : A \to B$ est une A-algèbre, la caractéristique de B divise la caractéristique de A. Cela résulte de $\phi \circ c_A = c_B$.

3.2.2.2 **Lemme.** *Soit $I \subset A$ un idéal. La projection canonique $p_I : A \twoheadrightarrow A/I$ induit une bijection d'ensembles ordonnés $p_I : (V^{tot}(I), \subset) \tilde{\to} (\mathcal{I}_{A/I}, \subset)$, $J \to p_I(J) = J/I$ d'inverse l'application $p_I^{-1} : (\mathcal{I}_{A/I}, \subset) \tilde{\to} (V^{tot}(I), \subset)$, $\overline{J} \to p_I^{-1}(\overline{J})$.*

Informellement, les idéaux de A/I sont en bijection avec les idéaux de A contenant I.

Proof. Le fait que $p_I : V^{tot}(I) \to \mathcal{I}_{A/I}$ préserve l'inclusion est immédiat. Pour montrer que c'est une bijection, il suffit d'exhiber l'application inverse. Comme $\ker(p_I) = I$, $p_I^{-1} : \mathcal{I}_{A/I} \to \mathcal{I}_A$ est à valeur dans $V^{tot}(I)$ donc induit une application $p_I^{-1} : \mathcal{I}_{A/I} \to V^{tot}(I)$; vérifions que celle-ci convient. Comme $p_I : A \twoheadrightarrow A/I$ est surjective, on a toujours $p_I \circ p_I^{-1}(\overline{J}) = \overline{J}$, $\overline{J} \in \mathcal{I}_{A/I}$. Inversement, si $J \in \mathcal{I}_A$, on a $p_I^{-1} \circ p_I(J) = I + J$ donc, si on suppose de plus $I \subset J$, on a $p_I^{-1} \circ p_I(J) = I + J = J$. □

Soit $I_1, \dots, I_r \subset A$ des idéaux et considérons le produit des projections canoniques $p := \prod_{1\leq i\leq r} p_{I_i} : A \to \prod_{1\leq i\leq r} A/I_i$; c'est un morphisme d'anneaux de noyau $\cap_{1\leq i\leq r} I_i$. De plus

3.2.2.3 **Lemme.** (Restes chinois) *Si $I_i + I_j = A$, $1 \leq i \neq j \leq r$ alors $\cap_{1\leq i\leq r} I_i = I_1 \cdots I_r$ et $p : A \to \prod_{1\leq i\leq r} A/I_i$ est surjective. Inversement, si $p : A \to \prod_{1\leq i\leq r} A/I_i$ est surjective alors $I_i + I_j = A$, $1 \leq i \neq j \leq r$.*

Proof. Supposons d'abord que $I_i + I_j = A$, $1 \leq i \neq j \leq r$. On a toujours $\cap_{1\leq i\leq r} I_i \supset I_1 \cdots I_r$. Pour l'inclusion inverse et la surjectivité de $p := \prod_{1\leq i\leq r} p_{I_i} : A \to \prod_{1\leq i\leq r} A/I_i$, on procède par récurrence sur r. Si $r = 2$, il existe $a_i \in I_i$, $i = 1, 2$ tels que $1 = a_1 + a_2$. En particulier,
- Pour tout $x \in I_1 \cap I_2$, $x = x1 = x(a_1 + a_2) = xa_1 + xa_2 = a_1x + xa_2 \in I_1 \cdot I_2$.
- Soit $x_1, x_2 \in A$ arbitraires. En posant $x = a_1x_2 + a_2x_1$ on a bien $p_{I_1}(x) = p_{I_1}(a_2)p_{I_1}(x_1) = p_{I_1}(x_1)$ et $p_{I_2}(x) = p_{I_2}(a_1)p_{I_2}(x_2) = p_{I_2}(x_2)$.

Si $r \geq 3$, on a par hypothèse de récurrence $I_2 \cap \cdots \cap I_r = I_2 \cdots I_r$ et $A/(I_2 \cap \cdots \cap I_r) \twoheadrightarrow \prod_{2\leq i\leq r} A/I_i$. Il suffit de montrer que $I_1 + I_2 \cdots I_r = A$. En effet, le cas $r = 2$ (et l'hypothèse de récurrence) nous donnera alors
- $I_1 \cap (I_2 \cap \cdots \cap I_r) = I_1 \cap (I_1 \cdots I_r) = I_1 \cdot (I_2 \cdots I_r) = I_1 \cdots I_r$.
- $A \twoheadrightarrow A/I_1 \times A/(I_2 \cap \cdots \cap I_r) \twoheadrightarrow A/I_1 \times \prod_{2\leq i\leq r} A/I_i = \prod_{1\leq i\leq r} A/I_i$

Mais pour $i = 2, \dots, r$ il existe $a_i \in I_1$, $b_i \in I_i$ tels que $a_i + b_i = 1$. On a donc $1 = \prod_{2\leq i\leq r}(a_i + b_i) = \prod_{2\leq i\leq r} b_i + \cdots \in I_2 \cdots I_r + I_1$.
Inversement, si $p : A \to \prod_{1\leq i\leq r} A/I_i$ est surjective, pour tout $1 \leq i \leq r$, il existe $x_i \in A$ tel que $p(x_i) = (\delta_{i,k})_{1\leq k\leq r} \in \prod_{1\leq k\leq r} A/I_i$ *i.e.* $x_i \in 1 + I_i$ et, pour tout $A \leq k \neq i \leq r$, $x_i \in I_k$ donc $1 = (1 - x_i) + x_i \in I_i + I_k$. □

3.3. **Classification grossière des idéaux.**

3.3.1. *Corps et idéaux maximaux.* Le singleton $\{0\}$ et A sont des ideaux de A. En général, un anneau contient beaucoup d'idéaux. L'ensemble des idéaux et leur 'position' dans l'anneau mesure la complexité de celui-ci. En ce sens, les anneaux les plus simples sont les corps.

3.3.1.1 **Lemme.** *Les PSSE: (i) A est un corps;*
(ii) Les seuls idéaux de A sont $\{0\}$ et A.

Proof. Si A est un corps, tout idéal $\{0\} \subsetneq I \subset A$ contient un élément $a \neq 0$ donc inversible. Mais alors $1 = a^{-1}a \in AI = I$ donc $A = A1 \subset AI = I$. Inversement, si les seuls idéaux de A sont $\{0\}$ et A, pour tout $a \neq 0$, $\{0\} \subsetneq Aa \subset A$ est un idéal donc $Aa = A$. En particulier $1 \in Aa$ *i.e.* il existe $a^{-1} \in A$ tel que $1 = a^{-1}a$. □

3.3.1.2 **Lemme.** *Soit $I \subsetneq A$ un idéal. Les PSSE (i) A/I est un corps;*
(ii) I est maximal dans $(\mathcal{I}_A \setminus \{A\}, \subset)$.

Proof. Cela résulte de 3.2.2 et du fait que les propriétés équivalentes de 3.3.1.1 sont aussi équivalentes à $|\mathcal{I}_A| = 2$. □

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de 3.3.1.2 est *maximal*.

3.3.1.3 **Lemme.** [Utilise le Lemme de Zorn] *L'ensemble ordonné $(\mathcal{I}_A \setminus \{A\}, \subset)$ est (non-vide; il contient $\{0\}$) inductif. En particulier, tout idéal $I \subsetneq A$ est contenu dans un idéal maximal.*

Proof. Il suffit d'observer que si $I_1 \subset I_2 \subset \cdots \subsetneq A$ est une suite d'ideaux de A distincts de A et croissante pour $\subset$, $I := \cup_{n\geq 1} I_n \subsetneq A$ est encore un idéal de A distincts de A. En effet, pour tout $a, b \in I$ il existe n tel que $a, b \in I_n$ donc $a - b \in I_n \subset I$ et pour tout $\alpha \in A$, $\alpha a \in I_n \subset I$; cela montre

déjà que $I \subset A$ est un idéal. Dans ce cas, $I = A$ si et seulement si $1 \in I$. Mais si $1 \in I$, il existerait $n \geq 1$ tel que $1 \in I_n$, ce qui n'est pas possible puisque par hypothèse $I_n \subsetneq A$. □

En particulier, pour tout $a \in A$, $a \notin A^\times \Leftrightarrow Aa \subsetneq A \Leftrightarrow a$ est contenu dans au moins un idéal maximal de A.

On notera $spm(A)$ l'ensemble des idéaux maximaux de A et on dit que c'est le *spectre maximal* de A. Avec cette notation, $A^\times = \cap_{\mathfrak{m} \in spm(A)}(A \backslash \mathfrak{m})$. D'après 2.1.1, les projections canoniques $p_\mathfrak{m} : A \twoheadrightarrow A/\mathfrak{m}$, $\mathfrak{m} \in spm(A)$ induisent un morphisme d'anneaux canonique

$$p_{max} : A \to \prod_{\mathfrak{m} \in spm(A)} A/\mathfrak{m}$$

dont le noyau $\mathcal{J}_A := \ker(p_{max}) = \bigcap_{\mathfrak{m} \in spm(A)} \mathfrak{m} \subset A$ est un idéal appelé *radical de Jacobson* de A.

3.3.2. *Anneaux intègres et idéaux premiers.* On dit qu'un élément $t \in A$ est de torsion (ou est un diviseur de zéro) s'il existe $0 \neq a \in A$ tel que $at = 0$ ou, encore, si $\ker(L_a : A \to A) \supsetneq \{0\}$. On notera $A_{tors} \subset A$ l'ensemble des éléments de torsion de A et $A_{reg} := A \setminus A_{tors} \subset A$ l'ensemble des éléments réguliers de A. On dit qu'un anneau A est *intègre* si $0 \neq 1$ et $A_{tors} = \{0\}$.

Exemples.
- Les corps sont intègres, $\mathbb{Z}$ est intègre.
- Tout sous-anneau d'un anneau intègre est intègre. Si A est un anneau intègre, $A[X]$ est intègre. Par contre, le produit $A_1 \times A_2$ de deux anneaux non nuls n'est jamais intègre (pourquoi?).
- $\mathbb{Z}/n$ est intègre si et seulement si n est un nombre premier. En particulier, la caractérisque d'un anneau intègre est 0 ou un nombre premier.

Remarque. Pour tout $a \in A \setminus A_{tors}$ et pour tout $b, c \in A$ on a $ab = ac \Leftrightarrow a(b - c) = \Leftrightarrow b - c = 0$. Autrement dit, 'on peut simplifier par a'. En particulier, si A est intègre, on peut simplifier par tout élément $a \neq 0$.

3.3.2.1. **Lemme.** *Soit $I \subsetneq A$ un idéal. Les PSSE* *(i) A/I est intègre;* *(ii) Pour tout $a, b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.*

Proof. (i) ⇒ (ii): Si $ab \in I$ alors $\overline{a}\overline{b} = 0$ dans A/I. Par (i), on a forcément $\overline{a} = 0$ (*i.e.* $a \in I$) ou $\overline{b} = 0$ (*i.e.* $b \in I$) dans A/I. (ii) ⇒ (i): Pour tout $0 \neq \overline{a}, \overline{b} \in A/I$, choisissons $a, b \in A$ relevant $\overline{a}, \overline{b} \in A/I$. On a forcément $a, b \notin I$ donc, par (ii), $ab \notin I$ *i.e.* $\overline{a}\overline{b} = \overline{ab} \neq 0$ dans A/I. □

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de 3.3.1.2 est *premier*. On notera $spec(A)$ l'ensemble des idéaux premiers de A et on dit que c'est le *spectre* de A. D'après 2.1.1, les projections canoniques $p_\mathfrak{p} : A \twoheadrightarrow A/\mathfrak{p}$, $\mathfrak{p} \in spec(A)$ induisent un morphisme d'anneaux canonique

$$p_{prem} : A \to \prod_{\mathfrak{p} \in spec(A)} A/\mathfrak{p}$$

dont le noyau $\mathcal{R}_A := \ker(p_{prem}) = \bigcap_{\mathfrak{p} \in spec(A)} \mathfrak{p} \subset A$ est un idéal appelé *radical* de A.

On dit qu'un élément $a \in A$ est *nilpotent* s'il existe un entier $n \geq 1$ tel que $a^n = 0$ et, si $a \neq 0$, on dit que le plus petit entier $n \geq 1$ tel que $a^{n-1} \neq 0$ et $a^n = 0$ est l'indice de nilpotence de a (on dit parfois que 0 est d'indice de nilpotence 1). On note $\mathcal{N}_A \subset A$ l'ensemble des éléments nilpotents de

A. On a évidemment $\mathcal{N}_A \subset A_{tors}$ donc, en particulier, si A est un anneau intègre, $\mathcal{N}_A = \{0\}$.

3.3.2.2. **Proposition.** [Utilise le Lemme de Zorn] *$\mathcal{N}_A \subset A$ est un idéal et $\mathcal{N}_A = \mathcal{R}_A$.*

Proof. Vérifions d'abord que $\mathcal{N}_A \subset A$ est un idéal. Pour tout $a, b \in \mathcal{N}_A$, il existe des entiers $m, n \geq 1$ tel que $a^m = b^n = 0$. Donc, par la formule du binôme de Newton

$$(a-b)^{m+n-1} = \sum_{0 \leq k \leq m+n-1} \binom{k}{m+n-1} (-1)^{m+n-k-1} a^k b^{m+n-k} = 0$$

puisque, si $k < m$, $m+n-k-1 > n-1$ donc $m+n-k-1 \geq n$. On a aussi pour tout $\alpha \in A$ $(\alpha a)^m = \alpha^m a^m = 0$.

Pour tout morphime d'anneaux $\phi : A \to B$ on a $\phi(\mathcal{N}_A) \subset \mathcal{N}_B$. En particulier, si B est un anneau intègre, $\mathcal{N}_A \subset \ker(\phi)$. En appliquant cette observation aux projections canoniques $p_{\mathfrak{p}} : A \twoheadrightarrow A/\mathfrak{p}$, $\mathfrak{p} \in spec(A)$, on en déduit l'inclusion $\mathcal{N}_A \subset \mathcal{R}_A$. Inversement, soit $a \notin \mathcal{N}_A$; on veut montrer que $a \notin \mathcal{R}_A$ *i.e.* il existe $\mathfrak{p} \in spec(A)$ tel que $a \notin \mathfrak{p}$ (ce qui équivaut aussi à $a^n \notin \mathfrak{p}$ pour n'importe quel entier $n \geq 1$). Notons $X_a := \{a^n \mid n \in \mathbb{Z}_{\geq 1}\}$ l'ensemble des puissances de a. On a par hypothèse $0 \notin X_a$ donc l'ensemble $\Sigma_a \subset \mathcal{I}_A$ des idéaux $I \subset A$ tels que $X_a \cap I = \emptyset$ est non-vide puisqu'il contient $\{0\}$. On vérifie immédiatement que $(\Sigma_a, \subset)$ est ordonné inductif donc, par le Lemme de Zorn, possède un élément maximal $I \in \Sigma_a$. Puisque $a \notin I$, il suffit de montrer que I est premier *i.e.* que A/I est intègre. Notons $\overline{a}$ l'image de a dans A/I. Par définition de I, $0 \notin X_{\overline{a}}$ mais pour tout idéal $\{0\} \subsetneq \overline{J} \subset A/I$, $X_{\overline{a}} \cap \overline{J} \neq \emptyset$. En particulier, pour tout $0 \neq \overline{b} \in A/I$, il existe $n_b \geq 1$ tel que $\overline{a}^{n_b} \in (A/I)\overline{b}$ donc pour tout $0 \neq \overline{b}, \overline{b'} \in A/I$, $\overline{a}^{n_b+n_{b'}} \in (A/I)\overline{bb'}$ donc $\overline{bb'} \neq 0$. □

Remarque. Lorsqu'on aura vu la localisation, on pourra réécrire la preuve de cette proposition de façon complètement transparente.

3.3.3. *Anneaux réduits et idéaux radiciels.* On dit qu'un anneau A est *réduit* si $\mathcal{R}_A = \mathcal{N}_A = 0$.

Exemples. Les anneaux intègres sont réduits, l'anneau $\mathbb{Z} \times \mathbb{Z}$ est réduit non-intègre. Si p est un nombre premier l'anneau $\mathbb{Z}/p^n$ n'est pas réduit et contient un élément d'indice de nilpotence n, $n \geq 1$. Si on note p_n le nième nombre premier, l'anneau $\prod_{n \geq 1} \mathbb{Z}/p_n^n$ n'est pas réduit et contient un élément d'indice de nilpotence n pour tout $n \geq 1$.

Pour un idéal $I \subset A$, on note $\sqrt{I} := p_I^{-1}(\mathcal{N}_{A/I})$. Par définition,

$$I \subset \sqrt{I} = \bigcup_{n \geq 1} \{a \in A \mid a^n \in I\}.$$

On dit que $\sqrt{I}$ est la racine de I. Avec cette notation, $\mathcal{N}_A = \sqrt{\{0\}}$. Il résulte des définitions que pour un idéal $I \subsetneq A$ les PSSE (i) A/I est réduit;
(ii) $I = \sqrt{I}$.
On dit qu'un idéal $I \subsetneq A$ qui vérifie les propriétés (i), (ii) ci-dessus est *radiciel*. On notera $\mathcal{I}_A^{rad}$ l'ensemble des idéaux radiciels de A.

Si I est un idéal de A on note $V(I) \subset spec(A)$ l'ensemble des idéaux premiers de A qui contiennent I. Puisque $I \subset \sqrt{I}$ on a $V(\sqrt{I}) \subset V(I)$. Inversement, si $\mathfrak{p} \in V(I)$, pour tout $a \in \sqrt{I}$ il existe $n \geq 1$ tel que $a^n \in I \subset \mathfrak{p}$ donc, comme $\mathfrak{p}$ est premier, $a \in \mathfrak{p}$. Cela montre que $\sqrt{I} \subset \mathfrak{p}$ donc que $V(I) = V(\sqrt{I})$.

3.3.4. *Synthèse.*

3.3.4.1. En résumé on a

$$\text{Maximal} \Rightarrow \text{Premier} \Rightarrow \text{Radicieł; } \textit{i.e. } spm(A) \subset spec(A) \subset \mathcal{I}_A^{rad}$$

et

I	A/I
Maximal	Corps
Premier	Intègre
Radiciel	Réduit

Classification grossière des idéaux

3.3.4.2. Tout morphisme $\phi : A \to B$ d'anneaux commutatifs induit une application $\phi^{-1} : (\mathcal{I}_B, \subset) \to (\mathcal{I}_A, \subset)$ préservant $\subset$. De plus, si $I \in \mathcal{I}_B$, le noyau de $A \xrightarrow{\phi} B \xrightarrow{p_I} B/I$ est $\phi^{-1}(I)$, d'où un morphisme d'anneaux injectifs $A/\phi^{-1}(I) \hookrightarrow B/I$. Comme un sous-anneau d'un anneau intègre (resp. réduit) est intègre (resp. réduit), on en déduit que $\phi^{-1} : (\mathcal{I}_B, \subset) \to (\mathcal{I}_A, \subset)$ se restreint en des applications

$$\begin{array}{ccc} (\mathcal{I}_B, \subset) & \xrightarrow{\phi^{-1}} & (\mathcal{I}_A, \subset) \\ \bigcup & & \bigcup \\ (\mathcal{I}_B^{rad}, \subset) & \xrightarrow{\phi^{-1}} & (\mathcal{I}_A^{rad}, \subset) \\ \bigcup & & \bigcup \\ (spec(B), \subset) & \xrightarrow{\phi^{-1}} & (V(\ker(\phi)), \subset) \end{array}$$

Il n'est par contre pas vrai qu'un sous-anneau d'un corps est un corps (*e.g.* $\mathbb{Z} \subset \mathbb{Q}$) donc l'image inverse d'un idéal maximal par un morphisme d'anneau n'est, en général, pas maximal.

4. Anneaux noetheriens

4.1. Lemme. *Soit A un anneau. Les PSSE.*
(1) Tout idéal $I \subset A$ est de type fini.
(2) Toute suite d'idéaux de A croissante pour $\subset$ est stationnaire à partir d'un certain rang.
(3) Tout sous-ensemble non vide d'idéaux de A admet un élément maximal pour $\subset$.

Proof. (1) $\Rightarrow$ (2). Supposons que tous les idéaux de A sont de type fini. Soit $I_0 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots \subset A$ une suite croissante d'idéaux pour $\subset$. L'ensemble $I := \cup_{n \geq 0} I_n \subset A$ est un idéal; il existe donc un ensemble fini $X \subset A$ tels que $I = \sum_{x \in X} Ax$. Mais pour chaque $x \in X$, il existe $n_x \geq 0$ tel que $x \in I_{n_x}$. Donc avec $n := \max\{n_x \mid x \in X\}$, on a $X \subset I_n$ donc $I \subset I_n$.
(2) $\Rightarrow$ (3). Soit $\mathcal{I} \subset \mathcal{I}_A$ un sous-ensemble non-vide. Supposons que $\mathcal{I}$ n'admette pas d'élément maximal pour $\subset$. Soit $I_0 \in \mathcal{I}$. Puisque I_0 n'est pas maximal pour $\subset$, on peut trouver $I_1 \in \mathcal{I}$ tel que $I_0 \subsetneq I_1$. En réitérant l'argument on construit une suite strictement croissante $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \cdots$ d'élément de $\mathcal{I}$, ce qui contredit (2).
(3) $\Rightarrow$ (1). Soit $I \subset A$ un idéal. Notons $\mathcal{I} \subset \mathcal{I}_A$ le sous-ensemble des idéaux de type fini de A contenu dans I. $\mathcal{I}$ est non-vide puisqu'il contient $\{0\}$. Par (3), il admet donc un élément I° maximal pour $\subset$. Si $I^\circ \subsetneq I$, il existe $a \in I$ tel que $I^\circ \subsetneq I^\circ + Aa \subset I$. Par construction $I^\circ + Aa$ est de type fini, ce qui contredit la maximalité de I°. □

On dit qu'un anneau A qui vérifie les propriétés équivalente du Lemme 4.1 est *noetherien*.

4.2. Exemples.

(1) Les anneaux principaux (*e.g.* k, $\mathbb{Z}$, $k[X]$, où k est un corps commutatif) sont noetheriens.
(2) Si k est un corps commutatif, une k-algèbre $\phi : k \to A$ est toujours munie d'une structure de k-espace vectoriel: $k \times A \to A$, $(\lambda, a) \to \phi(\lambda)a$. Avec cette structure de k-espace vectoriel, les idéaux de A sont automatiquement des sous-k-espaces vectoriels. Si A est de dimension finie sur k, elle est donc noetherienne. Par exemple l'anneau $k[X]/Pk[X]$, où $0 \neq P \in k[X]$, est noetherien.
(3) Tout quotient d'un anneau noetherien est noetherien. En effet, soit A est un anneau noetherien et $I \subset A$ un idéal; notons $p_I : A \twoheadrightarrow A/I$ la projection canonique. Si $J \subset A/I$ est un idéal, $p_I^{-1}(J) \subset A$ est un idéal donc, en particulier, il est engendré par un nombre fini $a_1, \ldots, a_r$ d'éléments. Mais alors, $J = p_I p_I^{-1}(J)$ est engendré par les $p_I(a_1), \ldots, p_I(a_r)$.
(4) Par contre un sous-anneau d'un anneau noetherien n'est pas forcément noetherien. Par exemple, on va voir (4.3) que si k est un corps commutatif, l'anneau $k[X_1, X_2]$ est noetherien mais la sous-k-algèbre $A \subset k[X_1, X_2]$ engendrée par les $X_1 X_2^n$, $n \geq 0$ n'est pas un anneau noetherien. En effet en notant $I_n \subset A$ l'idéal de A engendré par $X_1 X_2, \ldots, X_1 X_2^n$ on a $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \cdots$. Sinon, il existerait $n \geq 1$ tel que $I_n = I_{n+1}$ donc $X_1 X_2^{n+1} = \sum_{1 \leq k \leq n} a_k X_1 X_2^k$ avec $a_1, \ldots, a_k \in A$. Par définition de A, les a_k s'écrivent dans $k[X_1, X_2]$ sous la forme $a_k = a_{k,0} + X_1 b_k$ avec $a_{k,0} \in k$ et $b_k \in k[X_1, X_2]$. Comme X_1 n'est pas de torsion, on a $X_2^{n+1} = \sum_{1 \leq k \leq n} a_k X_2^k$ donc $X_2^{n+1} - \sum_{1 \leq k \leq n} a_{k,0} X_2^k = X_1 \sum_{k \in I} b_k X_2^k$: contradiction.

La proposition suivante et son corollaire fournissent un très grand nombre d'exemples d'anneaux noetheriens.

4.3. Proposition. (Transfert de noetherianité) *A noetherien $\Rightarrow$ $A[X]$ noetherien.*

Proof. Soit $I \subset A[X]$ un idéal. Pour chaque $n \geq 0$ définissons $\mathfrak{I}_n \setminus \{0\} \subset A$ comme l'ensemble des $a \in A$ qui apparaissent comme coefficient dominant d'un polynôme de degré n dand I *i.e.* $a \in \mathfrak{I}_n$ si et seulement si il existe $a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + aX^n \in I$. Comme $I \subset A[X]$ est un idéal, les $\mathfrak{I}_n \subset A$ sont automatiquement des idéaux. De plus,

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + aX^n \in I \Rightarrow a_0 X + a_1 X^2 + \cdots + a_{n-1} X^n + aX^{n+1} \in I$$

donc on a

$$\mathfrak{I}_0 \subset \mathfrak{I}_1 \subset \cdots \subset \mathfrak{I}_n \subset \mathfrak{I}_{n+1} \subset \cdots$$

Comme A est noetherien, cette suite devient stationnaire à partir d'un certain rang, disons n. De plus, chaque $\mathfrak{I}_k$ est de type fini; notons $a_{k,1}, \ldots, a_{k,r_k} \in \mathfrak{I}_k$ un ensemble fini de générateurs de $\mathfrak{I}_k$. Enfin, pour $k = 0, \ldots, n$, $l = 1, \ldots, r_k$, fixons un polynôme $P_{k,l} \in I$ de degré k et de coefficient dominant $a_{k,l}$. Il suffit de montrer que I est engendré par les $P_{k,l}$, $l = 1, \ldots, r_k$, $k = 0, \ldots, n$. Notons donc $I^\circ := \sum A[X] P_{k,l} \subset I$ et montrons par induction sur le degré d de $P \in I$ que $P \in I^\circ$. Si $d = 0$, on a par définition $\mathfrak{I}_0 \subset I^\circ$. Supposons que I° contient tous les éléments de I de degré $\leq d$. Soit $P = a_0 + \cdots + a_d X^d + a_{d+1} X^{d+1} \in I$ de degré $d+1$. Si $d+1 \geq n$, on a $a_{d+1} \in \mathfrak{I}_{d+1} = \mathfrak{I}_n$ donc on peut écrire $a_{d+1} = \sum_{1 \leq i \leq r_n} \alpha_i a_{n,i}$ et $P - \sum_{1 \leq i \leq r_n} \alpha_i X^{d+1-n} P_{n,i}$ est encore dans I mais de degré $\leq d$ donc, par hypothèse de récurrence, dans I°. Si $d+1 \leq n$, $a_{d+1} \in \mathfrak{I}_{d+1}$ donc on peut écrire $a_{d+1} = \sum_{1 \leq i \leq r_{d+1}} \alpha_i a_{d+1,i}$ et $P - \sum_{1 \leq i \leq r_n} \alpha_i P_{d+1,i}$ est encore dans I mais de degré $\leq d$ donc, par hypothèse de récurrence, dans I°. □

4.4. Corollaire. *Si A est un anneau noetherien, toute A-algèbre de type fini est un anneau noetherien.*

Proof. Observons d'abord qu'en raisonnant par induction sur $n \geq 1$, l'isomorphisme

$$A[X_1, \ldots, X_n] \tilde{\to} A[X_1, \cdots, X_{n-1}][X_n]$$

et la Proposition 4.3 impliquent que $A[X_1, \ldots, X_n]$ est un anneau noetherien. On conclut par l'Exemple 4.2 (3) puisque toute A-algèbre de type fini est quotient d'une A-algèbre de la forme $A[X_1, \ldots, X_n]$. □

5. Anneaux principaux, euclidiens

5.1. On dit qu'un anneau commutatif *intègre* A est

- *euclidien* s'il est muni d'une application - appelée stathme euclidien - $\sigma : A \setminus \{0\} \to \mathbb{N}$ vérifiant la propriété suivante (division euclidienne): pour tout $0 \neq a, b \in A$ il existe $q, r \in A$ tels que

$$b = qa + r$$
$$r = 0 \text{ ou } r \neq 0 \text{ et } \sigma(r) < \sigma(a).$$

  Remarque: Parfois on prolonge$\sigma : A \setminus \{0\} \to \mathbb{N}$ en $\sigma : A \to \mathbb{N} \cup -\infty$ en posant $v(0) = -\infty$ de sorte que la condition "$r = 0$ ou $r \neq 0$ et $\sigma(r) < \sigma(a)$" se réécrit de façon plus compacte en $\sigma(r) < \sigma(a)$.
- *principal* si ce n'est pas un corps et si tout idéal est de la forme Aa, $a \in A$.

5.2. Exemples

(1) La valeur absolue usuelle $|-| : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ sur $\mathbb{Z}$ est un stathme euclidien. En effet, pour tout $0 \neq a, b \in \mathbb{Z}$ notons $R := \{b - qa \mid q \in \mathbb{Z}\}$. On a évidemment $R \cap \mathbb{N} \neq \emptyset$ donc on peut poser $r := \min R \cap \mathbb{N}$. Par définition de R, $b = qa + r$ et si $|a| \leq r$ on aurait $r - |a| \in R \cap \mathbb{N}$: contradiction.

Remarque: Les éléments q, r ne sont pas uniques - par exemple: $5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$ mais ils le sont si on impose de plus que $r \geq 0$.

(2) **Algèbres de polynômes sur un anneau intègre.** Soit A un anneau commutatif et $r \geq 1$ un entier. La A-algèbre $A[X_1, \ldots, X_r]$ n'est euclidienne que si A est un corps et $r = 1$ mais, lorsque A est intègre, elle se comporte presque comme un anneau euclidien.
- $r = 1$. On rappelle que tout $f \in A[X]$ s'écrit de façon unique sous la forme $f = \sum_{n \in \mathbb{N}} a_n X^n$ avec $\underline{a} : n \to a_n \in A^{(\mathbb{N})}$. Cela permet de définir l'application degré:

$$\begin{array}{rccl} deg: & A[X] \setminus \{0\} & \to & \mathbb{N} \\ & f = \sum_{n \in \mathbb{N}} a_n X^n & \to & \max\{n \in \mathbb{N} \mid a_n \neq 0\} \end{array}$$

  et une application 'coefficient dominant'

$$\begin{array}{rccl} CD: & A[X] \setminus \{0\} & \to & A \setminus \{0\} \\ & f = \sum_{n \in \mathbb{N}} a_n X^n & \to & a_{deg(f)} \end{array}$$

  La définition du produit dans $A[X]$ montre que $deg(fg) \leq deg(f) + deg(g)$ et que si l'un au moins de $CD(f), CD(g)$ n'est pas de torsion dans A, $deg(fg) = deg(f) + deg(g)$, $CD(fg) = CD(f)CD(g)$. On a aussi toujours $deg(f + g) \leq \max\{deg(f), deg(g)\}$.

  Lemme *Soit $0 \neq f, g \in A[X]$ et supposons que $CD(f) \in A^\times$. Alors il existe un unique couple $q, r \in A[X]$ tel que $g = qf + r$ et $r = 0$ ou $deg(r) < deg(f)$.*

  Proof. Montrons l'existence par récurrence sur $deg(g)$. Ecrivons $f = \sum_{0 \leq n \leq d_f} a_n X^n$, $g = \sum_{0 \leq n \leq d_g} b_n X^n$, où $d_f := deg(f)$, $d_g := deg(g)$. Si $d_g = 0$ et $d_f > 0$, $q = 0$ et $r = g$ conviennent. Si $d_g = d_f = 0$, $f = a_0 = a_{d_f} \in A^\times \subset A[X]^\times$ donc $q = f^{-1}g$ et $r = 0$ conviennent. Si $d_g \geq 1$

et $d_f > d_g$, $q = 0$ et $r = g$ conviennent. Supposons donc $d_f \leq d_g$. Comme $a_{d_f} \in A^\times$ on peut écrire

$$g = a_{d_g} a_{d_f}^{-1} X^{d_g - d_f} f + (g - a_{d_g} a_{d_f}^{-1} X^{d_g - d_f} f).$$

Par construction, $g_1 := (g - a_{d_g} a_{d_f}^{-1} X^{d_g - d_f} f)$ est de degré $\leq d_g - 1$. Par hypothèse de récurrence il existe donc $q_1, r_1 \in A[X]$ tels que $g_1 = q_1 f + r_1$ et $r_1 = 0$ ou $deg(r_1) < deg(f)$; $q := a_{d_g} a_{d_f}^{-1} X^{d_g - d_f} + q_1$, $r := r_1$ conviennent. Il reste à prouver l'unicité. Si $q', r' \in A[X]$ est un autre couple tel que $g = fq' + r'$ et $r' = 0$ ou $deg(r') < deg(f)$, on a $f(q - q') = r' - r$. Si $r - r' \neq 0$, en prenant le degré

$$deg(f) \leq deg(f) + deg(q - q') \overset{(1)}{=} deg(f(q - q')) = deg(r - r') < deg(f),$$

où (1) utilise encore que $CD(f) \in A^\times$. On a donc forcément $r = r'$ donc $f(q - q') = 0$ donc, toujours parce que $CD(f) \in A^\times$, $q = q'$.

□

En particulier, si $A = k$ est un corps, le degré $deg : k[X] \setminus \{0\} \to \mathbb{N}$ est un stathme euclidien sur $k[X]$.

- $r \geq 1$. En utilisant les isomorphismes canoniques

$$A[X_1, \ldots, X_r] \tilde{\to} A[X_1, \ldots, \hat{X}_i, \cdots, X_r][X_i], \quad i = 1, \ldots, r,$$

on peut encore appliquer le Lemme ci-dessus dans $A[X_1, \ldots, X_r]$: les polynômes par lesquels on peut diviser sont ceux de la forme $aX_i^d + \sum_{\underline{n} \in \mathbb{N}^r, \, | \, n_i < d} a_{\underline{n}} \underline{X}^{\underline{n}}$, avec

$$a \in A[X_1, \ldots, \hat{X}_i, \cdots, X_r]^\times = A^\times$$

(car A est intègre donc réduit).

(3) On peut montrer que le carré de la valeur absolue usuelle $| - |^2 : \mathbb{Z}[w] \to \mathbb{N}$ est un stathme euclidien sur certains sous-anneaux de $\mathbb{C}$ de la forme $\mathbb{Z}[w] \subset \mathbb{C}$; c'est par exemple le cas pour $w = \sqrt{-1}, \sqrt[3]{-1}, \sqrt{-2}$. En particulier, on notera que les éléments $q, r \in A$ donnés par la division euclidienne ne sont pas uniques. En effet, dans $\mathbb{Z}[i]$ on a $3 = (1-i)(1+i)+1 = (2-i)(1+i)-i$ avec $|1|^2 = |i|^2 = 1 < |1+i|^2 = 2$

5.3. Lemme. *Euclidien ⇒ Principal.*

Proof. Soit A un anneau euclidien et soit $I \subset A$ un idéal. Fixons $a \in I$ tel que $\sigma(a) = \min\sigma(I)$. Puisque $a \in I$, on a $Aa \subset I$. Réciproquement, pour tout $b \in I$, effectuons la division euclidienne de b par a: il existe $q, r \in A$ tels que $b = qa + r$ et $r = 0$ ou $\sigma(r) < \sigma(a)$. Mais comme $r = b - qa \in I$, on ne peut pas avoir $\sigma(r) < \sigma(a)$, donc $r = 0$.

□

(Contre-)Exemple. Les anneaux principaux ne sont pas tous euclidiens. Par exemple $A = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ est principal non euclidien. *Cf.* T.D. 2.

6. Anneaux factoriels

Soit A un anneau commutatif intègre. On note $Princ(A)$ l'ensemble des idéaux principaux de A. Comme A est intègre, le produit d'idéaux munit $Princ(A) \setminus \{0\}$ d'une structure de monoïde commutatif d'unité $A = A \cdot 1$ et telle que l'application surjective $A \setminus \{0\} \twoheadrightarrow Princ(A) \setminus \{0\}$, $a \mapsto Aa$ est un morphisme de monoïdes. En outre, pour tout $a, b \in A \setminus \{0\}$,

- $Aa \subset Ab$ ssi $b|a$ *i.e.* il existe $\alpha \in A$ tel que $a = \alpha b$.
- $Aa = Ab$ ssi $A^\times a = A^\times b$.
  En effet, on a toujours $A^\times a = A^\times b \Rightarrow Aa = Ab$. Inversement, si $Aa = Ab$ il existe $\alpha, \beta \in A$ tel que $a = \alpha b$, $b = \beta a$ donc $a = \alpha\beta a$ et comme A est intègre, $\alpha\beta = 1$.

En particulier, $A \setminus \{0\} \twoheadrightarrow Princ(A) \setminus \{0\}$ se factorise en un isomorphisme de monoïdes

$$\begin{array}{ccc} A \setminus \{0\} & \twoheadrightarrow & Princ(A) \setminus \{0\} \\ \downarrow & \nearrow_{\simeq}^{aA^\times \mapsto Aa} & \\ A \setminus \{0\}/A^\times & & \end{array}$$

qui, si on munit $A \setminus \{0\}/A^\times$ de la relation d'ordre partiel $a \leq b$ ssi $b|a$ devient un isomorphisme de monoïdes ordonnés

$$(A \setminus \{0\}/A^\times, \leq) \tilde{\to} (Princ(A) \setminus \{0\}, \subset), \quad aA^\times \mapsto Aa.$$

6.1. Eléments irréductibles, éléments premiers.

6.1.1. On dit que $0 \neq a \in A \setminus A^\times$ est
- irréductible s'il vérifie les conditions équivalentes suivantes:
  (1) Aa est maximal dans $(Princ(A) \setminus A, \subset)$;
  (2) pour tout $a_1, a_2 \in A$, $a = a_1 a_2$ implique $a_1 \in A^\times$ ou $a_2 \in A^\times$.

  (1) $\Rightarrow$ (2): Si $a = a_1 a_2$ on a, pour $i = 1, 2$, $Aa \subset Aa_i$ donc, par maximalité de Aa, $Aa = Aa_i$ ou $Aa_i = A$ *i.e.* $a_i \in A^\times$. Supposons $Aa = Aa_2$ donc $a = \alpha_2 a_2$ avec $\alpha_2 \in A^\times$. Mais alors $a = a_1 a_2 = \alpha_2 a_2$ implique, puisque A est intègre, $a_1 = \alpha_2 \in A^\times$.
  (2) $\Rightarrow$ (1): Pour tout $b \in A \setminus A^\times$ tel que $Aa \subset Ab$ il existe $\alpha \in A$ tel que $a = \alpha b$. Mais $b \notin A^\times$ par hypothèse donc (2) impose $\alpha \in A^\times$ et donc $Aa = Ab$.

- premier si $Aa \in spec(A)$.

Exemple. On a $\mathbb{Z}^\times = \{\pm 1\}$ et les irréductibles de $\mathbb{Z}$ sont les nombres premiers. Si l'on veut déterminer si un entier $n \in \mathbb{Z}_{\geq 1}$ est premier, on dispose d'un algorithme évident consistant à lister tous les premiers $\leq \sqrt{n}$ et vérifier s'ils divisent n mais cet algorithme devient très vite inutilisable sur machine. Les arithméticiens ont beaucoup étudié et étudient encore le problème de la construction et de la répartition des nombres premiers. L'une de leurs motivations est l'application des nombres premiers en cryptographie. Parmi les énoncés classiques les plus spectaculaires, on trouve par exemple le théorème des nombres premiers, qui dit que si on note $\pi(n)$ le nombre de nombre premiers $0 \leq p \leq n$, on a $\pi(n) \sim_{n \to +\infty} \ln(n)/n$ ou le théorème de la progression arithmétique, qui dit que pour tout entier $0 \neq m, n$ premiers entre eux l'ensemble $m + \mathbb{Z}n$ contient une infinité de nombres premiers. Ces énoncés se démontrent souvent par des méthodes analytiques.

6.1.2. Lemme. *Les éléments premiers sont irréductibles.*

Proof. Si $Ap \in spec(A)$, pour tout $a, b \in A$, $ab = p (\in Ap)$ implique $a \in Ap$ ou $b \in Ap$. Supposons $a \in Ap$ *i.e.* $a = \alpha p$. On a alors $p = ab = \alpha bp$ et, comme A est intègre, on peut simplifier par p ce qui donne $\alpha b = 1$ donc $b \in A^\times$. □

6.1.3. (Contre-)exemple. Dans $A = \mathbb{Z}[i\sqrt{5}]$, 2 est irréductible mais pas premier. En effet, introduisons la norme $N : A \to \mathbb{Z}_{\geq 0}$, $a + ib\sqrt{5} \to |a + ib\sqrt{5}|^2 = a^2 + 5b^2$. On vérifie immédiatement que $N(xy) = N(x)N(y)$, $N(x) = 0 \Leftrightarrow x = 0$ et que

$$x \in A^\times \Leftrightarrow N(x) = 1 \Leftrightarrow x = \pm 1.$$

Vérifions que 2 est irréductible. Si on écrit $2 = xy$ on doit avoir $4 = N(2) = N(xy) = N(x)N(y)$. En particulier, $N(x) = N(y) = 2$ ou $\{N(x), N(y)\} = \{1, 4\}$. Or $2 \notin N(A)$ donc nécessairement $N(x) = 1$ ou $N(y) = 1$ *i.e.* $x \in A^\times$ ou $y \in A^\times$. Par contre 2 n'est pas premier car en observant (division euclidienne) que $\mathbb{Z}[T]/(T^2 + 5) \tilde{\to} \mathbb{Z}[i\sqrt{5}]$ on a $\mathbb{Z}[i\sqrt{5}]/2 \tilde{\to} \mathbb{F}_2[T]/(T^2 + 5) = \mathbb{F}_2[T]/(T + 1)^2$, qui n'est pas intègre puisque la classe de $T + 1$ est nilpotente non nulle.

6.2. Anneaux factoriels.

6.2.1. Soit A un anneau commutatif intègre A. Fixons un système de représentants $\mathcal{P}_A$ des classes des éléments irréductibles dans $A \setminus \{0\}/A^\times$. On dispose alors de deux monoïdes commutatifs:
- $A \setminus \{0\}$
- $A^\times \times \mathbb{N}^{(\mathcal{P}_A)}$ (pour le produit $(u, \nu) \cdot (u', \nu') = (uu', \nu + \nu')$, où $(\nu + \nu')(p) = \nu(p) + \nu'(p)$)

et d'un morphisme canonique de monoïdes

$$\begin{array}{rccc} (6.2.1.1) & A^\times \times \mathbb{N}^{(\mathcal{P}_A)} & \to & A \setminus \{0\} \\ & (u, \nu) & \to & u \prod_{p \in \mathcal{P}_A} p^{\nu(p)} \end{array}$$

On dit que A est factoriel si (6.2.1.1) est un isomorphisme *i.e.* pour tout $0 \neq a \in A$ il existe une unique application $v_-(a) : \mathcal{P}_A \to \mathbb{N}$ à support fini et un unique $u_a \in A^\times$ tels que $a = u_a \prod_{p \in \mathcal{P}_A} p^{v_p(a)}$ (on parle de 'la' décomposition en produit d'irréductibles de a). On dit que $v_p(a)$ est la multiplicité ou l'ordre de a en p ou, encore, la valuation p-adique de a.

6.2.2. Soit A un anneau factoriel. On prolonge les applications $v_p : A \setminus \{0\} \to \mathbb{N}$ en $v_p : A \to \overline{\mathbb{N}} := \mathbb{N} \cup \{\infty\}$ par $v_p(0) = \infty$. Avec les conventions $n + \infty = \infty$ et $n \leq \infty$, $n \in \overline{\mathbb{N}}$, il résulte immédiatement de l'unicité dans la définition d'anneaux factoriel que les applications $v_p : A \to \overline{\mathbb{N}}$, $p \in \mathcal{P}_A$ vérifient les propriétés élémentaires suivantes.

(1) $v_p(ab) = v_p(a) + v_p(b)$, $a, b \in A$;

(2) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ et si $v_p(a) \neq v_p(b)$, $v_p(a+b) = \min\{v_p(a), v_p(b)\}$, $a, b \in A$, $a \neq p$.

En effet, écrivons $a = p^{v_p(a)}a'$, $b = p^{v_p(b)}b'$ avec $v_p(a') = v_p(b') = 0$. Si $v_p(a) > v_p(b)$, on a $a+b = p^{v_p(b)}(a'p^{v_p(a)-v_p(b)} + b')$ avec $v(a'p^{v_p(a)-v_p(b)} + b') = 0$ car $v_p(b') = 0$ et $v_p(a'p^{v_p(a)-v_p(b)}) = v_p(a) - v_p(b) > 0$. Si $v_p(a) = v_p(b) = v$, on a $v_p(a + b) = v + v_p(a' + b') \geq v$.

(3) $v_p^{-1}(0) = A \setminus Ap$, $v_p^{-1}(\overline{\mathbb{N}} \setminus \{0\}) = Ap$.

En particulier, (1) et (3) impliquent que $v_p : (A \setminus \{0\}, \cdot) \to (\mathbb{N}, +)$ est un morphisme de monoïdes.

6.2.3. Lemme. *Dans un anneau factoriel tout élément irréductible est premier.*

Proof. Soit A un anneau factoriel et $p \in A$ irréductible. Alors pour tout $a, b \in A$, on a $ab \in Ap \Leftrightarrow v_p(a) + v_p(b) = v_p(ab) \geq 1 \Leftrightarrow v_p(a) \geq 1$ ou $v_p(b) \geq 1 \Leftrightarrow a \in Ap$ ou $b \in Ap$.

□

On a également $A^\times = \{a \in A \mid v_p(a) = 0,\ p \in \mathcal{P}_A\}$.

6.2.4. Remarque. La propriété d'être factoriel et l'application[4] $v_{\_}(a) : \mathcal{P}_A \to \mathbb{N}$ ne dépendent pas du choix du systèmes de représentants $\mathcal{P}_A$ des classes éléments irréductibles dans $A \setminus \{0\}/A^\times$ par contre l'élément $u_a \in A^\times$ en dépend. En fait, le bon point de vue est de considérer le monoïde $A \setminus \{0\}/A^\times \tilde{\to} Princ(A) \setminus \{0\}$ plutôt que $A \setminus \{0\}$. Si on note $\mathcal{P}_A := spec(A) \cap Princ(A) \setminus \{0\}$, A est factoriel ssi le morphisme de monoïdes

$$\begin{array}{ccc} \mathbb{N}^{(\mathcal{P}_A)} & \to & Princ(A) \setminus \{0\} \\ \nu & \to & \prod_{\mathfrak{p} \in \mathcal{P}_A} \mathfrak{p}^{\nu(\mathfrak{p})} = \bigcap_{\mathfrak{p} \in \mathcal{P}_A} \mathfrak{p}^{\nu(\mathfrak{p})} \end{array}$$

est un isomorphisme. Sous cette forme, la décomposition d'un idéal principal en produit d'idéaux principaux premiers se généralise à des idéaux arbitraires (décomposition primaire - *cf.* [AM69, Chap. 4]).

6.3. Proposition.
(1) Principal ⇒ (Noetherien intègre + premier = irréductible) ⇒ factoriel.
(2) [Utilise le Lemme de Zorn] Factoriel + $spm(A) = spec(A) \setminus \{0\}$ ⇒ Principal.

6.3.1. Le lemme suivant montre que ce qui est 'profond' dans la définition d'anneau factoriel c'est surtout l'unicité de la décomposition en produit d'irréductibles. L'existence est vérifiée pour une classe d'anneaux beaucoup plus large.

Lemme. *Si A est un anneau notherien intègre, le morphisme de monoïde (6.2.1.1) est surjectif.*

Proof. Notons $\mathcal{F} \subset A \setminus \{0\}$ l'image de (6.2.1.1); en particulier $\mathcal{F} \subset A \setminus \{0\}$ est stable par produit et contient $\mathcal{P}_A$, $A^\times$. Si $a \notin \mathcal{F}$, $a \notin \mathcal{P}_A$ donc il existe $a_1, b_1 \notin A^\times$ tels que $a = a_1 b_1$. En particulier, $Aa \subsetneq Aa_1, Ab_1$. De plus, comme $\mathcal{F}$ est stable par produit, on a $a_1 \notin \mathcal{F}$ ou $b_1 \notin \mathcal{F}$. Supposons $a_1 \notin \mathcal{F}$. En itérant, $a_1 = a_2 b_2$ avec $a_2, b_2 \notin A^\times$ - donc $Aa_1 \subsetneq Aa_2, Ab_2$ - et $a_2 \notin \mathcal{F}$ *etc.* on construit ainsi une suite strictement croissante $Aa \subsetneq Aa_1 \subsetneq Aa_2 \subsetneq Aa_3 \subsetneq \cdots$ d'idéaux de A, ce qui contredit la noetherianité de A. □

6.3.2. Lemme. *Si A est un anneau principal $spm(A) = spec(A) \setminus \{0\}$.*

Proof. Soit A un anneau principal et $\mathfrak{p} = Ap \in spec(A) \setminus \{0\}$. Soit $I = Aa \subset A$ un idéal tel que $\mathfrak{p} \subset I$. On a donc $p = \alpha a$ pour un certain $\alpha \in A$. Or, puisque $\mathfrak{p}$ est premier, p est premier donc irréductible. Ce qui force $\alpha \in A^\times$ (*i.e* $Ap = Aa = I$) ou $a \in A^\times$ (*i.e* $I = Aa = A$). □

6.3.3. *Preuve de 6.3.*

(1) Principal ⇒ (Noetherien intègre + premier = irréductible).

Soit A un anneau principal. On sait déjà que A est intègre (par définition) et noetherien (puisque tous ses idéaux sont engendrés par un seul élément). De plus pour tout $p \in A \setminus A^\times$, p est irréductible ssi Ap est maximal dans $Princ(A) \setminus A$. Mais comme A est principal, $Princ(A) = \mathcal{I}_A$ donc on a les équivalences (la 3ème est le Lemme 6.3.2) p irréductible $\Leftrightarrow Ap \in spm(A) \Leftrightarrow Ap \in spec(A) \setminus \{0\} \Leftrightarrow p \in A$ premier.

(Noetherien intègre + premier = irréductible) ⇒ factoriel.

[4] Si on note $\mathfrak{p} := Ap$, on peut la définir intrinsèquement par $v_\mathfrak{p}(a) = \max\{n \in \mathbb{N} \mid a \in \mathfrak{p}^n\}$.

Par le Lemme 6.3.1, on sait déjà que l'application $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \to A\setminus\{0\}$ est surjective. Supposons que l'on ait

$$a := u\prod_{p\in\mathcal{P}_A} p^{\mu(p)} = v\prod_{p\in\mathcal{P}_A} p^{\nu(p)}$$

et que, $\nu(p) > \mu(p)$ pour un certain $p \in \mathcal{P}_A$. Comme A est intègre, on peut simplifier par $p^{\mu(p)}$; on peut donc supposer $\mu(p) = 0$ et $\nu(p) > 0$. Comme $\nu(p) > 0$, $\overline{a} = 0$ dans A/p. Comme p est premier, A/p est intègre et comme $\overline{u} \in (A/p)^\times$, il existe forcément $q \in \mathcal{P}_A$ tel que $\overline{q} = 0$ dans A/p *i.e.* $q \in Ap$, ce qui force $q = p$ puisque p, q sont irréductibles: contradiction.

(2) Supposons A factoriel et $spm(A) = spec(A) \setminus \{0\}$.

- Montrons d'abord que tout idéal premier est principal: si $\{0\} \subsetneq \mathfrak{p} \subsetneq A$ est premier, il contient un élément $0 \neq a \notin A^\times$. Comme A est factoriel, on peut écrire $a = u_a \prod_{p\in\mathcal{P}_A} p^{v_p(a)}$. Comme $A/\mathfrak{p}$ est intègre, il existe au moins un $p \in \mathcal{P}_A$ tel que $v_p(a) \geq 1$ et $\bar{p} = 0$ *i.e.* $p \in \mathfrak{p}$. En particulier $Ap \subset \mathfrak{p}$. Mais comme A est factoriel, $Ap \in spec(A)$ et comme $spm(A) = spec(A) \setminus \{0\}$ par hypothèse, $Ap = \mathfrak{p}$.

- Soit maintenant $\mathcal{E}$ l'ensemble des idéaux de A qui ne sont pas principaux. Supposons $\mathcal{E} \neq \emptyset$; comme $(\mathcal{E}, \subset)$ est un ensemble ordonné inductif, le Lemme de Zorn assure qu'il possède un élément $0 \subsetneq I \subsetneq A$ maximal pour $\subset$. Toujours par le Lemme de Zorn , I est contenu dans un idéal maximal $\mathfrak{m}$, dont on sait qu'il est principal $\mathfrak{m} = Ap$. Introduisons l'ensemble

$$J := \{a \in A \mid ap \in I\} = R_p^{-1}(I),$$

où $R_p : A \twoheadrightarrow Ap$, $a \mapsto ap$. Puisque I est un idéal, $I \subset J$ et J est un idéal de A. Comme $I \subset Ap$ et $R_p : A \twoheadrightarrow Ap$ est surjectif, $I = R_p(R_p^{-1}(I)) = pJ$. Si $I \subsetneq J$, par maximalité de I on aurait $J = Aa$ donc $I = Aap$, ce qui contredit $I \in \mathcal{E}$. Donc $I = J$, ce qui implique $I = Jp = Ip$. Cela contredit la factorialité de A. En effet, si $0 \neq a \in I$, on peut écrire $a = p^{v_p(a)}b$ avec $v_p(b) = 0$. Mais comme A est intègre, $p^{v_p(a)}b \in I = Ip \Rightarrow p^{v_p(a)-1}b \in I = Ip \Rightarrow p^{v_p(a)-2}b \in I = pI \Rightarrow ...$ $\Rightarrow b \in I = pI \Rightarrow v_p(b) \geq 1$.

Remarque. Si on suppose A noetherien dans (2), on n'a pas besoin d'invoquer le Lemme de Zorn.

6.3.2 **(Contre-)Exemples.** Les implications de 6.3 ne sont pas des équivalences. Par exemple,
- Anneau (noetherien + premier = irréductible) non principal: $k[X_1, X_2]$, où k est un corps commutatif;
- Anneau factoriel non noetherien: $k[X_1, \dots, X_n, \dots, X_{n+1}, \dots] = k[\mathbb{N}^{\mathbb{N}}]$, où k est un corps commutatif (observer que $k[\mathbb{N}^{\mathbb{N}}]$ peut s'écrire comme l'union croissante des sous-anneaux $k[\mathbb{N}^n] \subset k[\mathbb{N}^{n+1}] \subset \cdots \subset k[\mathbb{N}^{\mathbb{N}}]$).

6.4. Polynômes sur les anneaux factoriels.

6.4.1. Corps des fractions d'un anneau intègre. Nous allons d'abord construire le corps des fractions d'un anneau intègre. Il s'agit d'un cas particulier de localisation, construction que nous verrons en toute généralité un peu plus loin. L'objectif est de construire une A-algèbre dans laquelle tous les éléments non nuls de A sont inversibles et qui est universelle pour cette propriété.

Soit donc A un anneau intègre. On munit le produit ensembliste $A \setminus \{0\} \times A$ de la relation $\sim$ définie par: pour tout $(s, a), (s', a') \in A \setminus \{0\} \times A$, $(s, a) \sim (s', a')$ si $s'a - sa' = 0$.

On vérifie facilement que $\sim$ est une relation d'équivalence. On note $Frac(A) := A \setminus \{0\} \times A/\sim$ et

$$\begin{array}{rccc} -/-: & A\setminus\{0\}\times A & \to & Frac(A) \\ & (s,a) & \to & a/s =: s^{-1}a \end{array}$$

la projection canonique. Considérons les applications $+,\cdot : (A\setminus\{0\}\times A)\times(A\setminus\{0\}\times A) \to Frac(A)$ définies par

$$(s,a)+(t,b) = (ta+sb)/(st), \quad (s,a)\cdot(t,b) = (ab)/(st)$$

Si $(s,a)\sim(s',a')$, $(t,b)\sim(t',b')$ on a

$$s't'(ta+sb)-st(t'a'+s'b') = (s'a)(t't)+(ss')(t'b)-(sa')(tt')-(ss')(tb') = (s'a-sa')t't+(ss')(t'b-tb') = 0$$

$$(s't')(ab)-(st)(a'b') = (s'a)(t'b)-(sa')(tb') = 0$$

Cela montre que les applications $+,\cdot : (A\setminus\{0\}\times A)\times(A\setminus\{0\}\times A) \to Frac(A)$ se factorisent en

$$\begin{array}{ccc} (A\setminus\{0\}\times A)\times(A\setminus\{0\}\times A) & \xrightarrow{+,\cdot} & Frac(A) \\ {\scriptstyle -/-\times-/-}\downarrow & \nearrow_{+,\cdot} & \\ Frac(A)\times Frac(A) & & \end{array}$$

On laisse en exercice le soin de vérifier que $Frac(A)$ muni des lois $+,\cdot : Frac(A)\times Frac(A) \to Frac(A)$ ainsi définies vérifie bien les axiomes d'un anneau commutatif de zéro $0/1$ et d'unité $1/1$ et que, pour cette structure d'anneau, l'application canonique

$$\begin{array}{rccc} \iota_A: & A & \to & Frac(A) \\ & a & \to & a/1 \end{array}$$

est un morphisme d'anneaux injectif. De plus, tout élément non nul $a/b \in Frac(A)$ est inversible d'inverse b/a; $Frac(A)$ est donc un corps.

Lemme. (Propriété universelle du corps des fractions) *Pour tout anneau intègre A il existe un morphisme d'anneaux $\iota : A \to F$ tel que $\iota(A\setminus\{0\}) \subset F^\times$ et pour tout morphisme d'anneaux $\phi : A \to B$ tel que $\phi(A\setminus\{0\}) \subset B^\times$, il existe un unique morphisme d'anneaux $\tilde{\phi} : F \to B$ tel que $\phi = \tilde{\phi}\circ\iota$.*

Plus visuellement,

$$\begin{array}{ccc} A\setminus\{0\} & \xrightarrow{\phi} & B^\times \\ \downarrow & & \downarrow \\ A & \xrightarrow{\forall\phi} & B \\ {\scriptstyle \iota_A}\downarrow & \nearrow_{\exists!\tilde{\phi}} & \\ F & & \end{array}$$

Proof. Montrons que $Frac(A)$ muni de la structure d'anneau ci-dessus et le morphisme canonique $\iota_A : A \to Frac(A)$ conviennent. Soit $\phi : A \to B$ un morphisme d'anneaux tel que $\phi(A\setminus\{0\}) \subset B^\times$. Si $\tilde{\phi} : Frac(A) \to B$ existe la relation $\phi = \tilde{\phi}\circ\iota_A$ impose

$$\tilde{\phi}(a/s) = \tilde{\phi}((a/1)(1/s)) = \tilde{\phi}((a/1))\tilde{\phi}((s/1))^{-1} = \phi(a)\phi(s)^{-1}, \ (s,a) \in A\setminus\{0\}\times A,$$

d'où l'unicité sous réserve d'existence. Pour l'existence, considérons donc l'application

$$\begin{array}{rccc} \tilde{\phi}: & A\setminus\{0\}\times A & \to & B \\ & (s,a) & \to & \phi(s)^{-1}\phi(a). \end{array}$$

Si $(s,a) \sim (s,a)'$ on a $\phi(s')\phi(a) - \phi(s)\phi(a') = \phi((s'a - sa')) = \phi(0) = 0$. Mais comme $\phi(s), \phi(s') \in B^\times$, on peut réécrire cette égalité comme

$$\tilde{\phi}(s,a) = \phi(s)^{-1}\phi(a) = \phi(s')^{-1}\phi(a') = \tilde{\phi}(s',a').$$

Cela montre que l'application $\tilde{\phi} : A \setminus \{0\} \times A \to B$ se factorise en

$$\begin{array}{ccc} A \setminus \{0\} \times A & \xrightarrow{\tilde{\phi}} & B \\ {\scriptstyle -/-}\downarrow & \nearrow_{\tilde{\phi}} & \\ Frac(A) & & \end{array}$$

Par construction $\phi = \tilde{\phi} \circ \iota_A$ et on vérifie que $\tilde{\phi} : Frac(A) \to B$ est bien un morphisme d'anneaux. □

Comme d'habitude, le morphisme d'anneaux $\iota_A : A \to Frac(A)$ est unique à unique isomorphisme près; on dit que c'est le *corps des fractions* de A.

6.4.2. *Extension des valuations p-adiques.* Soit A un anneau factoriel (donc en particulier intègre) et $\iota_A : A \hookrightarrow K := Frac(A)$ son corps des fractions. Pour chaque $p \in \mathcal{P}_A$, l'application

$$\begin{array}{rccc} v_p : & A \setminus \{0\} \times A & \to & \overline{\mathbb{Z}} := \mathbb{Z} \cup \{\infty\} \\ & (s,a) & \to & v_p(a) - v_p(s) \end{array}$$

vérifie $(s,a) \sim (s',a') \Rightarrow v_p(a) - v_p(s) = v_p(a') - v_p(s')$ donc se factorise *via*

$$\begin{array}{ccc} A \setminus \{0\} \times A & \xrightarrow{v_p} & \overline{\mathbb{Z}} \\ {\scriptstyle -/-}\downarrow & \nearrow_{v_p} & \\ K & & \end{array}$$

qui vérifie encore

(1) $v_p(xy) = v_p(x) + v_p(y)$, $x, y \in K$;
(2) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$, $x, y \in K$;

De plus,

$$A^\times = \bigcap_{p \in \mathcal{P}_A} v_p^{-1}(0), \quad A = \bigcap_{p \in \mathcal{P}_A} v_p^{-1}(\overline{\mathbb{Z}}_{\geq 0}).$$

L'isomorphisme de monoïdes (6.1.2.1) s'étend également en un isomorphisme de groupes

$$\begin{array}{ccc} A^\times \times \mathbb{Z}^{(\mathcal{P}_A)} & \to & K \setminus \{0\} \\ (u, \nu) & \to & u \prod_{p \in \mathcal{P}_A} p^{\nu(p)} \end{array}$$

d'inverse

$$\begin{array}{ccc} K \setminus \{0\} & \to & A^\times \times \mathbb{Z}^{(\mathcal{P}_A)} \\ x & \to & (x \prod_{p \in \mathcal{P}_A} p^{-v_p(x)}, p \to v_p(x)) \end{array}$$

qui se prolongent en des isomorphismes $A^\times \times \overline{\mathbb{Z}}^{(\mathcal{P}_A)} \tilde{\to} K$, $K \tilde{\to} A^\times \times \overline{\mathbb{Z}}^{(\mathcal{P}_A)}$.

6.4.3. *Contenu.* Supposons toujours A factoriel. Pour tout $p \in \mathcal{P}_A$ on étend $v_p : K \to \overline{\mathbb{Z}}$ en $v_p : K[X] \to \overline{\mathbb{Z}}$ par

$$v_p(P) := \min\{v_p(a_n) \mid n \geq 0\}, \quad P = \sum_{n\geq 0} a_n X^n \in K[X]$$

On définit l'application contenu $C_A : K[X] \to K$ par

$$C_A(P) = \prod_{p\in\mathcal{P}_A} p^{v_p(P)}, \quad P \in K[X].$$

Noter que comme P n'a qu'un nombre fini de coefficients non nuls, les $v_p(P)$ sont nuls sauf pour un nombre fini de $p \in \mathcal{P}_A$. On a

- $C_A(P) = 0$ si et seulement si $P = 0$;
- $C_A(P) \in A$ si et seulement si $P \in A[X]$;
- Pour tout $a \in K$, $C_A(aP) = aC_A(P)$. En particulier, pour tout $P \in K[X]$, $P = C_A(P)P_1$ avec $C_A(P_1) = 1$.

Lemme. *Pour tout $P, Q \in K[X]$ on a $C_A(PQ) = C_A(P)C_A(Q)$.*

Proof. Si $P \in K$ ou $Q \in K$, c'est clair. Supposons donc $P, Q \in K[X]\setminus K$. En écrivant $P = C_A(P)P_1$, $Q = C_A(Q)Q_1$ on a $C_A(PQ) = C_A(P)C_A(Q)C_A(P_1Q_1)$. Il suffit donc de montrer que si $C_A(P) = C_A(Q) = 1$ alors $C_A(PQ) = 1$. Observons que pour $F \in K[X]$ on a $C_A(F) = 1$ si et seulement si

(1) $F \in A[X]$;
(2) Pour tout $p \in \mathcal{P}_A$, $\overline{F} \neq 0$ dans $A/pA[X]$,

où $\overline{F}$ est l'image de F par le morphisme canonique $A[X] \to A[X]/pA[X]\tilde{\to}(A/pA)[X]$. La propriété (1) est stable par produit puisque $A[X]$ est un anneau et la propriété (2) est stable par produit car $(A/pA)[X]$ est aussi un anneau intègre; ici on utilise que p est irréductible donc premier puisque A est factoriel. □

6.4.4. Proposition. (Transfert de factorialité) *A factoriel $\Rightarrow A[X]$ factoriel. De plus, les irréductible de $A[X]$ sont les irréductibles de A et les irréductible de $K[X]$ de contenu* 1.

Proof. L'idée est bien sûr d'exploiter que $K[X]$ est factoriel car euclidien. Fixons un système $\mathcal{P}_{K[X]}$ de représentants des classes des éléments irréductibles dans $K[X]\setminus\{0\}/K[X]^\times$ de contenu 1 (il suffit de remplacer un système de représentants $\mathcal{P}$ donné par les $P/C_A(P)$, $P \in \mathcal{P}$) et un système $\mathcal{P}_A$ de représentants des classes des éléments irréductibles dans $A\setminus\{0\}/A^\times$. Notons $\mathcal{P}_{A[X]}$ l'union de $\mathcal{P}_A$ et de $\mathcal{P}_{K[X]}$. Comme A est intègre, on sait déjà que $A[X]^\times = A^\times$. On procède en deux temps.

(1) Les éléments de $\mathcal{P}_{A[X]}$ sont irréductibles.

Il suffit de montrer que les éléments de $\mathcal{P}_{A[X]}$ sont premiers.

- Si $p \in \mathcal{P}_A$ comme A est factoriel et p est irréductible, p est premier donc A/pA est intègre. Cela implique que $(A/pA)[X]$ est intègre et on conclut par l'isomorphisme d'anneaux canoniques $A[X]/pA[X]\tilde{\to}(A/pA)[X]$.
- Si $P \in \mathcal{P}_{K[X]}$, considérons le morphisme canonique $\phi : A[X] \hookrightarrow K[X] \twoheadrightarrow K[X]/PK[X]$. Par construction $PA[X] \subset \ker(\phi)$. Inversement, si $F \in \ker(\phi)$ alors $F = PQ$ dans $K[X]$. Par le Lemme 6.4.3, $C_A(F) = C_A(P)C_A(Q) = C_A(Q)$ donc $C_A(Q) \in A$ *i.e.* $Q \in A[X]$. Donc $F \in PA[X]$ et le morphisme $\phi : A[X] \hookrightarrow K[X] \twoheadrightarrow K[X]/PK[X]$ se factorise en un morphisme d'anneaux injectif $A/PA[X] \hookrightarrow K[X]/PK[X]$. Comme $K[X]$ est factoriel et P est irréductible,

P est premier donc $K[X]/PK[X]$ est intègre. Comme un sous-anneau d'un anneau intègre est intègre, $A[X]/PA[X]$ est donc intègre.

(2) Pour tout $F \in A[X]$ il existe un unique $u \in A^\times$ et une unique application $\nu_F : \mathcal{P}_{A[X]} \to \mathbb{N}$ à support fini tels que

$$F = u \prod_{P \in \mathcal{P}_{A[X]}} P^{\nu_F(P)}.$$

Comme $K[X]$ est factoriel et que $K[X]^\times = K \setminus \{0\}$, il existe un unique $a \in K \setminus \{0\}$ et une unique application $v_-(F) : \mathcal{P}_{K[X]} \to \mathbb{N}$ à support fini tels que

$$F = a \prod_{P \in \mathcal{P}_{K[X]}} P^{v_P(F)}$$

Comme $C_A(a) = C_A(F) \in A$, $a \in A$ et comme A est factoriel, il existe un unique $u \in A^\times$ et une unique application $v_-(a) : \mathcal{P}_A \to \mathbb{N}$ à support fini tels que

$$a = u \prod_{p \in \mathcal{P}_A} P^{v_p(a)}.$$

On a donc

$$F = u \prod_{p \in \mathcal{P}_A} P^{v_p(a)} \prod_{P \in \mathcal{P}_{K[X]}} P^{v_P(F)}.$$

Cela montre l'existence de $u \in A^\times$ et $v_-(F) : \mathcal{P}_{A[X]} \to \mathbb{N}$. Supposons qu'on ait deux décompositions

$$F = u \prod_{p \in \mathcal{P}_A} p^{v_p(a)} \prod_{P \in \mathcal{P}_{K[X]}} P^{v_P(F)} = u' \prod_{p \in \mathcal{P}_A} p^{v'_p(a)} \prod_{P \in \mathcal{P}_{K[X]}} P^{v'_P(F)}.$$

En réécrivant

$$uu'^{-1} \prod_{p \in \mathcal{P}_A} p^{v_p(a))-v'_p(a)} = \prod_{P \in \mathcal{P}_{K[X]}} P^{v_P(F)-v'_P(F)} \in K \setminus \{0\},$$

la factorialité de $K[X]$ impose $v_P(F) = v'_P(F)$, $P \in \mathcal{P}_{K[X]}$. La factorialité de A impose alors $v_p(a) = v'_p(a)$, $p \in \mathcal{P}_A$.

Remarque. On a bien montré en passant que tout irréductible de $A[X]$ admet un représentant dans $\mathcal{P}_{A[X]}$: si $F \in A[X]$ est irréductible, il s'écrit de façon unique sous la forme

$$F = u \prod_{p \in \mathcal{P}_{A[X]}} p^{v_p(F)}$$

avec $u \in A^\times$ et comme F est par définition non inversible et ne peut s'écrire comme produit de deux éléments non-inversibles, on doit forcément avoir $v_p(F) = 1$ pour un certain $p \in \mathcal{P}_A \cup \mathcal{P}_{K[X]}$ et $v_q(F) = 0$, pour tout $p \neq q \in \mathcal{P}_A \cup \mathcal{P}_{K[X]}$ □

6.4.5. Corollaire. *Pour tout $n \geq 1$, A factoriel $\Rightarrow$ $A[X_1, \ldots, X_n]$ factoriel.*

Proof. Par induction sur n et en utilisant l'isomorphisme canonique

$$A[X_1, \ldots, X_n] \tilde{\to} A[X_1, \ldots, \ldots, X_{n-1}][X_n].$$

□

6.4.6. Exercice - critères d'irréductibilité pour les algèbres de polynômes sur les corps. Comme dans $\mathbb{Z}$, déterminer si un élément de $K[X]$ est irréductible est un problème délicat. Voici les deux critères d'irréductibilité les plus classiques pour les algèbres de polynômes. On renvoie au TD 2 pour les corrections.

(1) **(Critère d'Eisenstein)** Soit A un anneau factoriel de corps des fractions K et $P = \sum_{n\geq 0} a_n X^n \in A[X]$. S'il existe un irréductible p de A tel que $v_p(a_0) \leq 1$, $v_p(a_n) \geq 1$, $0 \leq n \leq deg(P) - 1$ et $v_p(a_{deg(P)}) = 0$ alors P est irréductible dans $K[X]$.
(2) **(Critère de réduction)** Soit A, B des anneaux intègres et L le corps des fractions de B. Soit $\phi : A \to B$ un morphisme d'anneaux. On note encore $\phi = A[X] \to B[X]$ l'unique morphisme de A-algèbres $A[X] \to B[X]$, $X \mapsto X$ (pro. univ. de $A[X]$); explicitement $\phi(\sum_{n\geq 0} a_n X^n) = \sum_{n\geq 0} \phi(a_n) X^n$). Soit $P \in A[X]$. Montrer que si $deg(\phi(P)) = deg(P)$ et $\phi(P)$ est irréductible dans $L[X]$ alors P ne peut s'écrire sous la forme $P = P_1 P_2$ avec $P_1, P_2 \in A[X]$ de degré ≥ 1.

Remarque. La terminologie 'critère de réduction' vient du fait qu'on applique en général ce critère avec les morphismes $p_I : A \twoheadrightarrow A/I$ de réduction modulo un idéal $I \subset A$. En général, on prend même $I = \mathfrak{m}$ maximal, ce qui permet de se ramener au cas de l'algèbre de polynôme $(A/\mathfrak{m})[X]$ qui est un anneau euclidien puisque $A/\mathfrak{m}$ est un corps. Typiquement, si $A = \mathbb{Z}$, on peut chercher un 'bon' nombre premier p tel que la réduction modulo p de $P \in \mathbb{Z}[X]$ soit irréductible dans $\mathbb{Z}/p[X]$.

6.5. Valuations et anneaux factoriels. Soit K un corps.

6.5.1. Une *valuation* (discrète de rang 1) sur K est une application surjective[5] $v : K \to \overline{\mathbb{Z}}$ qui vérifie
(1) $v(xy) = v(x) + v(b)$, $x, y \in K$;
(2) $v(x + y) \geq \min\{v(x), v(y)\}$, $x, y \in K$;
(3) $v(x) = \infty \Leftrightarrow x = 0$.

Remarque. La propriété (1) peut se réécrire en disant que $v : (K^\times, \cdot) \to (\mathbb{Z}, +)$ est un morphisme de groupes.

Notons $A_v := v^{-1}([0, \infty]) \subset K$. On dit qu'un anneau est *local* s'il possède un unique idéal maximal.

6.5.2. Lemme. *L'ensemble $Av \subset K$ est un sous-anneau de K, de corps des fractions K et tel que $A_v^\times = v^{-1}(0)$ et $\mathfrak{m}_v := A_v \setminus A_v^\times \subset A_v$ est un idéal. En particulier, A_v est local d'unique idéal maximal $\mathfrak{m}_v$. De plus les seuls idéaux de A_v sont les $\pi^n A_v$, $n \in \mathbb{Z}_{\geq 0}$, où $\pi \in A$ est tel que $v(\pi) = 1$.*

Proof. Montrons d'abord que $A_v \subset K$ est un sous-anneau. D'après la propriété (1) d'une valuation, $1 \in A$ (utiliser $1^2 = 1$) et $a, b \in A_v$ implique $ab \in A$. De plus, pour tout $x \in K^\times$ la relation $(-x)^2 = x^2$ et la propriété (1) d'une valuation montrent que $v(x) = v(-x)$ ce qui, combiné à la propriété (2) d'une valuation montre que $a, b \in A_v$ implique $a - b \in A_v$. Observons également que la propriété (1) d'une valuation implique

$$A_v^\times = \{x \in K^\times \mid x, x^{-1} \in A_v\} = v^{-1}(\{0\}).$$

Les propriétés (1) (respectivement (2)) assurent également que $\mathfrak{m}_v$ est stable par multiplication par les éléments de A (respectivement par différence) donc que $\mathfrak{m}_v \subset A_v$ est un idéal. C'est automatiquement l'unique idéal maximal de A_v puisque $A_v \setminus \mathfrak{m}_v = A_v^\times$. Soit $\pi \in A$ tel que $v(\pi) = 1$ (on utilise ici la surjectivité de v). Pour un id'eal $I \subset A_v$ arbitraire, notons $n := \min v(I)$. On a alors pour tout $a \in I$, $v(\pi^{-n} a) \geq 0$ donc $a \in A_v \pi^n$. Cela montre que $A \subset A\pi^n$. Inversement, soit $a \in I$ tel que $v(a) = n$. On a alors $v(\pi^{-n} a) = 0$ *i.e.* $A^\times a = A^\times \pi^n$ donc $A\pi^n = Aa \subset I$. Il reste à voir que K est le

[5]On fait cette hypothèse par commodité. Il suffit en fait de supposer que $v : K \to \overline{\mathbb{Z}}$ est non nulle; on peut alors se ramener au cas surjectif en utilisant que tout sou groupe non-nul de $\mathbb{Z}$ est isomorphe à $\mathbb{Z}$.

corps des fractions de A_v; cela résulte du fait que tout $x \in A$ s'écrit sous la forme $x = (x\pi^{-v(x)})\pi^{v(x)}$ avec $x\pi^{-v(x)} \in A_v^\times$. □

On dit qu'un anneau de la forme A_v est un *anneau de valuation discrète*. Ces anneaux jouent un rôle fondamental en géométrie arithmétique. Ils possèdent plusieurs caractérisations équivalentes. On en verra quelques unes en TD.

6.5.3. Si A est factoriel de corps des fractions $\iota_A : A \hookrightarrow K := Frac(A)$, les applications $v_p : K \to \overline{\mathbb{Z}}$, $p \in \mathcal{P}_A$ sont donc des valuations sur K. Et la famille de valuations

$$\mathcal{V} := \{v_p : Frac(A) \to \overline{\mathbb{Z}} \mid p \in \mathcal{P}_A\}$$

vérifie les propriétés suivantes:

- (6.5.1.1) Pour tout $0 \neq x \in K$,
$$|\{v \in \mathcal{V} \mid v(x) \neq 0\}| < +\infty;$$
- (6.5.1.2) Il existe une famille d'élements $(p_v)_{v\in\mathcal{V}} \in K$ telle que $v(p_w) = \delta_{v,w}$, $v, w \in \mathcal{V}$;
- (6.5.1.3) $A = \bigcap_{v\in\mathcal{V}} A_v$

Inversement, on a

6.5.4. Proposition. *Soit K un corps muni d'une famille $\mathcal{V}$ de valuation $v : K \to \overline{\mathbb{Z}}$ vérifiant les propriétés (6.5.1.1), (6.5.1.2). Alors*

$$A := \bigcap_{v\in\mathcal{V}} v^{-1}(\overline{\mathbb{N}}) \subset K$$

est un sous-anneau qui est factoriel et les p_v, $v \in \mathcal{V}$ forme un système de représentants des classes des éléments irréductibles dans $A \setminus \{0\}/A^\times$.

Proof. Observons d'abord que $A \subset K$ est un sous-anneau comme intersection de sous-anneaux (Lemme 6.5.2). La propriété (1) d'une valuation implique également que

$$A^\times = \{x \in K^\times \mid x, x^{-1} \in A\} = \bigcap_{v\in\mathcal{V}} v^{-1}(\{0\}).$$

Montrons ensuite que les p_v, $v \in \mathcal{A}$ sont irréductibles. Soit donc $v \in \mathcal{V}$. La condition $v(p_v) = 1$ assure déjà que $p \notin A^\times$. Ecrivons $p_v = ab$, $a, b \in A$. On doit avoir $v(p_v) = 1 = v(a) + v(b)$ et $w(p_v) = 0 = w(a) + w(b)$, $v \neq w \in \mathcal{V}$. Comme par définition de A, $w(a), w(b) \geq 0$, $w \in \mathcal{V}$, ces relations impliquent $v(a) = 1$ et $v(b) = 0$ ou $v(a) = 0$ et $v(b) = 1$ et $w(a) = w(b) = 0$, $v \neq w \in \mathcal{V}$. Donc $a \in A^\times$ ou $b \in A^\times$.

Soit maintenant $0 \neq a \in A$. Par (6.5.1.1), on peut définir

$$u_a := a \prod_{v\in\mathcal{V}} p_v^{-v(a)} \in K^\times,$$

qui vérifie par construction et la propriété (1) d'une valuation $v(u_a) = 0$, $v \in \mathcal{V}$ *i.e.* $u_a \in A^\times$. L'écriture $a = u_a \prod_{v\in\mathcal{V}} p_v^{v(a)}$ montre déjà que les p_v, $v \in \mathcal{V}$ forment un système de représentants des classes d'irrréductibles de A. De plus, l'écriture $a = u_a \prod_{v\in\mathcal{V}} p_v^{v(a)}$ est unique. Si on a une écriture $a = u \prod_{v\in\mathcal{V}} p_v^{v'(a)}$ avec $u' \in A^\times$, $v'\_(a) : \mathcal{V} \to \mathbb{N} \in \mathbb{N}^{(\mathcal{V})}$, l'égalité

$$u'^{-1} u_a = \prod_{v\in\mathcal{V}} p_v^{v'(a)-v(a)} \in A^\times$$

implique, par évaluation en chacune des $v \in \mathcal{V}$ et en utilisant (6.5.1.2) que $v'(a) = v(a)$, $v \in \mathcal{V}$ et donc $u' = u_a$. □

6.5.5. Exercice. (ppcm, pgcd) Soit A un anneau factoriel.

(1) Montrer que $Aa \cap Ab$ est un idéal principal engendré par

$$ppcm(a,b) := \prod_{p \in \mathcal{P}_A} p^{\max\{v_p(a), v_p(b)\}}.$$

On dit que les éléments de $A^\times ppcm(a,b)$ sont les plus petits communs multiples de a et b.

(2) Montrer que l'ensemble des idéaux principaux de A qui contiennent $Aa + Ab$ admet un plus petit élément, engendré par

$$pgcd(a,b) := \prod_{p \in \mathcal{P}_A} p^{\min\{v_p(a), v_p(b)\}}.$$

On dit que les éléments de $A^\times pgcd(a,b)$ sont les plus grands communs diviseurs de a et b. Montrer sur un exemple qu'en général l'inclusion $Aa + Ab \subsetneq Apgcd(a,b)$ est stricte.

(3) Généraliser (1) et (2) à un nombre fini $a_1, \ldots, a_r$ d'éléments de A.

(4) (Bézout) Supposons A principal. Montrer que $pgcd(a_1, \ldots, a_r)A^\times = A^\times$ si et seulement si il existe $u_1, \ldots, u_r \in A$ tels que $u_1a_1 + \cdots + u_ra_r = 1$.

7. Localisation, anneaux de fractions.

Soit A un anneau commutatif.

7.1. Une *partie multiplicative* de A est un sous-ensemble $S \subset A \setminus \{0\}$ stable par multiplication et contenant 1.

7.1.1. Exemples.

7.1.1.1 $S := A \setminus A_{tors}$; en particulier, si A est intègre, $S := A \setminus \{0\}$;

7.1.1.2 Pour $a \in A \setminus \sqrt{\{0\}}$, $S_a := \{a^n \mid n \in \mathbb{N}\}$;

7.1.1.3 Pour $\mathfrak{p} \in spec(A)$, $S_\mathfrak{p} := A \setminus \mathfrak{p}$.

7.1.2. Soit $S \subset A \setminus \{0\}$ une partie multiplicative. On munit le produit ensembliste $S \times A$ de la relation $\sim$ définie par: pour tout $(s,a),(s',a') \in S \times A$, $(s,a) \sim (s',a')$ s'il existe $s'' \in S$ tel que $s''(s'a - sa') = 0$.

On vérifie que $\sim$ est une relation d'équivalence. On remarquera que si A est intègre, on peut, dans la définition de $\sim$, simplifier par s'' et la relation $\sim$ devient simplement $(s,a),(s',a') \in S \times A$, $(s,a) \sim (s',a')$ si $s'a - sa' = 0$. Mais on prendra garde que si A n'est pas intègre, la relation $(s,a) \sim (s',a')$ si $s'a - sa' = 0$ n'est pas transitive donc ne définit pas une relation d'équivalence.

On note $S^{-1}A := S \times A/\sim$ et

$$\begin{array}{rccc} -/-: & S \times A & \to & S^{-1}A \\ & (s,a) & \to & a/s \end{array}$$

la projection canonique.

Considérons les applications

$$\begin{array}{rccc} + & : (S\times A)\times(S\times A) & \to & S^{-1}A \\ & ((s,a),(t,b)) & \to & (ta+sb)/(st) \end{array} \quad , \quad \begin{array}{rccc} \cdot & : (S\times A)\times(S\times A) & \to & S^{-1}A \\ & ((s,a),(t,b)) & \to & (ab)/(st) \end{array}$$

Si $(s,a)\sim(s',a')$, $(t,b)\sim(t',b')$ *i.e.* il existe $s'',t''\in S$ tels que $s''(s'a-sa')=0$, $t''(t'b-tb')=0$. Comme $s''t''\in S$ par multiplicativité, on a

$$s''t''(s't'(ta+sb)-st(t'a'+s'b')) = s''s'a'tt't''-t'bss's''-s''t''st(t'a'+s'b') = s''sa''tt't''-tb'ss's''-s''t''st(t'a'+s'b')$$

et

$$s''t''(s't'ab-sta'b') = s''s'at''t'b-s''sa't''tb' = s''sa't''t'b-s''sa't''tb' = s''sa't''(t'b-tb') = 0.$$

Cela montre que les applications $+,\cdot:(S\times A)\times(S\times A)\to S^{-1}A$ se factorisent en

$$\begin{array}{ccc} (S\times A)\times(S\times A) & \xrightarrow{+,\cdot} & S^{-1}A \\ {\scriptstyle -/-\times-/-}\downarrow & \nearrow_{+,\cdot} & \\ S^{-1}A\times S^{-1}A & & \end{array}$$

On laisse en exercice le soin de vérifier que $S^{-1}A$ muni des lois $+,\cdot:S^{-1}A\times S^{-1}A\to S^{-1}A$ ainsi définies vérifie bien les axiomes d'un anneau commutatif de zéro $0/1$ et d'unité $1/1$ et que, pour cette structure d'anneau, l'application canonique

$$\begin{array}{rccc} \iota_S: & A & \to & S^{-1}A \\ & a & \to & a/1 \end{array}$$

est un morphisme d'anneaux de noyau $\ker(\iota_S)=\{a\in A\mid \exists s\in S,\ sa=0\}=\cup_{s\in S}\ker(s\cdot:A\to A,\ a\mapsto sa)$. En particulier, si A est intègre (ou plus généralement si S ne contient pas d'éléments de torsion), $\iota_S:A\to S^{-1}A$ est injectif. De plus, $\iota_S(S)\subset(S^{-1}A)^\times$ puisque $s/1\cdot 1/s=s/s=1/1$.

7.1.3. Lemme. (Propriété universelle de la localisation) *Pour toute partie multiplicative $S\subset A\backslash\{0\}$ il existe un morphisme d'anneaux $\iota_S:A\to F$, unique à unique isomorphisme près, tel que $\iota(S)\subset F^\times$ et pour tout morphisme d'anneaux $\phi:A\to B$ tel que $\phi(S)\subset B^\times$, il existe un unique morphisme d'anneaux $\tilde\phi:F\to B$ tel que $\phi=\tilde\phi\circ\iota_S$.*

Proof. Montrons que $S^{-1}A$ muni de la structure d'anneau ci-dessus et le morphisme canonique $\iota_S:A\to S^{-1}A$ conviennent. Soit $\phi:A\to B$ un morphisme d'anneaux tel que $\phi(S)\subset B^\times$. Si $\tilde\phi:S^{-1}A\to B$ existe la relation $\phi=\tilde\phi\circ\iota_S$ impose que $\tilde\phi:S^{-1}A\to B$ est unique puisqu'on doit nécessairement avoir

$$\tilde\phi(A/s)=\tilde\phi((a/1)(1/s))=\tilde\phi((a/1))\tilde\phi((s/1))^{-1}=\phi(a)\phi(s)^{-1},\ (s,a)\in S\times A.$$

Considérons donc l'application $\begin{array}{rccc}\tilde\phi: & S\times A & \to & B \\ & (a,s) & \to & \phi(s)^{-1}\phi(a).\end{array}$ Si $(s,a)\sim(s',a')$ *i.e.* il existe $s''\in S$ tels que $s''(s'a-sa')=0$, on a $\phi(s'')(\phi(s')\phi(a)-\phi(s)\phi(a'))=\phi(s''(s'a-sa'))=\phi(0)=0$. Mais comme $\phi(s),\phi(s'),\phi(s'')\in B^\times$, on peut réécrire cette égalité comme

$$\tilde\phi(s,a)=\phi(s)^{-1}\phi(a)=\phi(s')^{-1}\phi(a')=\tilde\phi(s',a').$$

Cela montre que l'application $\tilde{\phi} : S \times A \to B$ se factorise en

$$\begin{array}{ccc} S \times A & \xrightarrow{\tilde{\phi}} & B \\ {\scriptstyle -/-}\downarrow & \nearrow_{\tilde{\phi}} & \\ S^{-1}A & & \end{array}$$

Par construction $\phi = \tilde{\phi} \circ \iota_S$ et on vérifie que $\tilde{\phi} : S^{-1}A \to B$ est bien un morphisme d'anneaux. Comme d'habitude, l'unicité à unique isomorphisme près de $\iota_S : A \to S^{-1}A$ résulte formellement de (l'existence et de) l'unicité de $\tilde{\phi} : F \to B$ dans la propriété universelle. □

On dit que $\iota_S : A \to S^{-1}A$ est 'la' localisation de A en S. Localiser A en S revient donc à inverser formellement les éléments de S.

7.1.4. Exemples.

7.1.4.1 On dit que $(A \setminus A_{tors})^{-1}A$ est l'anneau des fractions de A. Si A est un anneau intègre, on retrouve le corps des fractions de A. Si A n'est pas intègre, $(A \setminus A_{tors})^{-1}A$ n'est pas un corps (le vérifier sur un exemple).

7.1.4.2 Pour $a \in A \setminus \sqrt{\{0\}}$ on note $A_a := S_a^{-1}A$;

7.1.4.3 Pour $\mathfrak{p} \in spec(A)$, on note $A_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}A$. Noter que si A est intègre $\{0\} \in spec(A)$ et, dans ce cas, $A_{\{0\}} = Frac(A)$.

7.1.5. Soit $\phi : A \to B$ un morphisme d'anneaux et $S \subset A$, $T \subset B$ des parties multiplicatives telles que $\phi(S) \subset T$. On a en particulier $\iota_T \circ \phi(S) \subset \iota_T(T) \subset (T^{-1}B)^\times$ donc par propriété universelle de $\iota_S : A \to S^{-1}A$ il existe un unique morphisme d'anneaux $\phi_{S,T} : S^{-1}A \to T^{-1}B$ tel que $\iota_T \circ \phi = \phi_{S,T} \circ \iota_S$; explicitement $\phi_{S,T}(a/s) = \phi(a)/\phi(s)$ dans $T^{-1}B$. Si $\phi : A \to B$, $\psi : B \to C$ sont des morphismes d'anneaux et $S \subset A$, $T \subset B$, $U \subset C$ des parties multiplicatives telles que $\phi(S) \subset T$, $\psi(T) \subset U$, on a $(\psi \circ \phi)_{S,U} = \phi_{S,T} \circ \psi_{T,U}$.

Exemple.

(1) Soit $\phi : A \to B$ un morphisme d'anneaux et $\mathfrak{q} \subset spec(B)$. On a alors $\mathfrak{p} := \phi^{-1}(\mathfrak{q}) \in spec(A)$ et $\phi(A \setminus \mathfrak{p}) \subset B \setminus \mathfrak{q}$ donc $\phi : A \to B$ induit un morphisme d'anneaux canonique $\phi_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{q}}$.
(2) Si A est intègre, $\{0\} \in spec(A)$ et pour toute partie multiplicative $S \subset A \setminus \{0\}$, en appliquant ce qui précède à $\phi = Id : A \to A$, $S = S$, $T = A \setminus \{0\}$, on obtient un morphisme canonique $\phi : S^{-1}A \to A_{\{0\}} = Frac(A)$ dont on vérifie immédiatement qu'il est injectif.

7.2. Idéaux. Soit $S \subset A$ une partie multiplicative. Pour un sous-ensemble $X \subset A$, notons

$$S^{-1}X := \{a/s \mid a \in X,\ s \in S\} \subset S^{-1}A.$$

On vérifie immédiatement que si $I \subset A$ est un idéal alors $S^{-1}I \subset S^{-1}A$ est aussi un idéal (c'est l'idéal engendré par $\iota_S(I)$ dans $S^{-1}A$). On a donc une application bien définie et croissante pour $\subset$

$$S^{-1} : (\mathcal{I}_A, \subset) \to (\mathcal{I}_{S^{-1}A}, \subset).$$

Dans l'autre direction on a l'application

$$\iota_S^{-1} : (\mathcal{I}_{S^{-1}A}, \subset) \to (\mathcal{I}_A, \subset)$$

induite par le morphisme de localisation $\iota_S : A \to S^{-1}A$.
- Pour $I \subset A$ un idéal, on a

$$\iota_S^{-1}S^{-1}I = \{a \in A \mid a/1 \in S^{-1}I\} = \{a \in A \mid Sa \cap I \neq \emptyset\} = \bigcup_{s\in S}(s\cdot)^{-1}I.$$

En particulier, $S^{-1}I = S^{-1}A$ (si et seulement si $\iota_S^{-1}S^{-1}I = A$) si et seulement si $S \cap I \neq \emptyset$.

- Pour $I \subset S^{-1}A$ un idéal, on a

$$S^{-1}\iota_S^{-1}I = \{a/s \in S^{-1}I \mid a \in \iota_S^{-1}I\} \supset I$$

et comme pour tout $a/s \in I$ on a $a/1 = (s/1)^{-1}(a/s) \in I$ donc $a \in \iota_S^{-1}I$, on a en fait $S^{-1}\iota_S^{-1}I = I$.

On a donc montré:

7.2.1. Lemme. *L'application $S^{-1} : (\mathcal{I}_A, \subset) \to (\mathcal{I}_{S^{-1}A}, \subset)$ est surjective, croissante pour $\subset$ et se restreint en une surjection*

$$S^{-1} : \{I \in \mathcal{I}_A \mid I \cap S = \emptyset\} \twoheadrightarrow \mathcal{I}_{S^{-1}A} \setminus \{S^{-1}A\}.$$

L'application $\iota_S^{-1} : (\mathcal{I}_{S^{-1}A}, \subset) \to (\mathcal{I}_A, \subset)$ est injective, croissante pour $\subset$ et induit une bijection

$$\iota_S^{-1} : \mathcal{I}_{S^{-1}A} \tilde{\to} \{I \in \mathcal{I}_A \mid I = \bigcup_{s\in S}(s\cdot)^{-1}I\}.$$

En particulier, le localisé d'un anneau noetherien (resp. artinien) est encore noetherien (resp. artinien).

7.2.2. Lemme. *Les applications $S^{-1} : \mathcal{I}_A \to \mathcal{I}_{S^{-1}A}$ et $\iota_S^{-1} : \mathcal{I}_{S^{-1}A} \to \mathcal{I}_A$ se restreignent en des bijections inverses l'une de l'autres*

$$spec(S^{-1}A) \underset{S^{-1}}{\overset{\iota_S^{-1}}{\rightleftarrows}} \{\mathfrak{p} \in spec(A) \mid \mathfrak{p} \cap S = \emptyset\}$$

Proof. Si $\mathfrak{p} \in spec(A)$ est tel que $S \cap \mathfrak{p} = \emptyset$ alors $\mathfrak{p} = \bigcup_{s\in S}(s\cdot)^{-1}\mathfrak{p}$ (si $s \in S$, $a \in \mathfrak{p}$, $sa \in \mathfrak{p}$ implique $a \in \mathfrak{p}$) donc $\iota_S^{-1}S^{-1}\mathfrak{p} = \mathfrak{p}$. Comme on a toujours $S^{-1}\iota_S^{-1} = Id$, et $\iota_S^{-1}spec(S^{-1}A) \subset spec(A)$, il reste seulement à montrer que si $\mathfrak{p} \in spec(A)$ est tel que $S \cap \mathfrak{p} = \emptyset$ alors $S^{-1}\mathfrak{p} \in spec(S^{-1}A)$. Soit donc $\mathfrak{p} \in spec(A)$ et $a/s, b/t \in S^{-1}A$ tels que $(ab)/(st) \in S^{-1}\mathfrak{p}$ *i.e.* il existe $p \in \mathfrak{p}$ et $u, v \in S$ tels que $v(uab - stp) = 0$ ou encore $vuab = vstp \in \mathfrak{p}$. Mais comme $\mathfrak{p} \in spec(A)$ et $vu \notin \mathfrak{p}$, on a $ab \in \mathfrak{p}$ donc $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. □

Exemple.

(1) Pour $\mathfrak{p} \in spec(A)$, , $spec(A_\mathfrak{p}) \tilde{\to} \{\mathfrak{q} \in spec(A) \mid \mathfrak{q} \subset \mathfrak{p}\}$. En particulier, $A_\mathfrak{p}$ est local d'unique idéal maximal $\mathfrak{p}A_\mathfrak{p}$. Le corps $\kappa(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est appelé le corps résiduel de $spec(A)$ en $\mathfrak{p}$. Si on reprend les notations de l'Exemple 7.1.5, le morphisme $\phi : A_\mathfrak{p} \to B_\mathfrak{q}$ envoie $\mathfrak{p}$ dans $\mathfrak{q}$ donc induit par passage au quotient un morphisme de corps - nécessairement injectif $\kappa(\mathfrak{p}) \hookrightarrow \kappa(\mathfrak{q})$.
(2) Pour tout $a \in A \setminus A_{tors}$, $spec(A_a) \tilde{\to} \{\mathfrak{p} \in spec(A) \mid a \notin \mathfrak{p}\}$.

La philosophie générale à retenir est que passer au quotient par un idéal premier (resp. maximal), permet de ramener certains problèmes au cas où l'anneau de base est intègre (resp. un corps) et que localiser en idéal premier permet de ramener certains problèmes au cas où l'anneau de base est local.

Part 2. Modules sur un anneau

On rappelle que sauf mention explicite du contraire tous les anneaux sont commutatifs.

8. Premières définitions et constructions

8.1. Définitions.

8.1.1. Soit A un anneau, un A-module (à gauche) est un couple $((M,+),\cdot)$ formé d'un groupe abélien $(M,+)$ (on notera 0 son élément neutre et $-m$ l'inverse d'un élément $m \in M$) et d'une application $\cdot : A \times M \to A$ - appelées la multiplication extérieure - vérifiant les axiomes suivants:

(1) $a \cdot (m+n) = a \cdot m + a \cdot n$, $a \in A$, $m, n \in M$;
(2) $(a+b) \cdot m = a \cdot m + b \cdot m$, $a, b \in A$, $m \in M$;
(3) $(a \cdot b) \cdot m = a \cdot (b \cdot m)$, $a, b \in A$, $m \in M$;
(4) $1 \cdot m = m$, $m \in M$.

De façon équivalente, l'application $A \to End_{Grp}(M)$ est un morphisme d'anneaux.

Etant donnés deux A-modules M, N, un morphisme de A-modules est un morphisme de groupes $f : (M,+) \to (N,+)$ A-linéaire *i.e* qui vérifie:

$$f(a \cdot m) = a \cdot f(m),\ a \in A,\ m \in M.$$

On remarquera que l'application identité $Id : M \to M$ est un morphisme de A-modules et que si $f : M \to N$ et $g : N \to P$ sont des morphismes de A-modules alors $g \circ f : M \to P$ est un morphisme de A-modules. On notera $Hom_A(M,N)$ l'ensemble des morphismes de A-modules $\phi : M \to N$ et, si $M = N$, $End_A(M) := Hom_A(M,M)$.

On dit qu'un morphisme de A-modules $f : M \to N$ est injectif, (resp. surjectif, resp. un isomorphisme) si l'application d'ensemble sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $f : M \to N$ est un isomorphisme de A-modules l'application inverse $f^{-1} : N \to M$ est automatiquement un morphisme de A-modules.

8.1.2. *Exemples.*
- Si $A = \mathbb{Z}$, les $\mathbb{Z}$-modules sont les groupes abéliens.
- Si $A = k$ est un corps commutatif, les k-modules sont les k-espaces vectoriels.
- On peut toujours voir un anneau A comme un A-module sur lui-même en prenant pour multiplication extérieure le produit $\cdot : A \times A \to A$. Cet exemple qui semble tautologique est en fait fondamental! On va s'en rendre compte rapidement. Plus généralement, tout idéal $I \subset A$ muni de $\cdot : A \times I \to I$ induite par le produit de A est un A-module.
- Si M est un A-modules et X un ensemble, l'ensemble $Hom_{Ens}(X,M)$ des applications ensemblistes de X dans M et le sous-ensemble $Hom^{sf}_{Ens}(X,M) \subset Hom_{Ens}(X,M)$ de celles à support fini sont naturellement munis d'une structure de A-module pour les lois $(f+g)(x) = f(x)+g(x)$, $(a \cdot f)(x) = a \cdot (f(x))$.
- Si M, N sont deux A-modules, $Hom_A(M,N)$ est naturellement muni d'une structure de A-module pour les lois $(f+g)(m) = f(m)+g(m)$, $(a \cdot f)(m) = a \cdot (f(m))$.
- Si $\phi : A \to B$ est un morphisme d'anneaux tout B-module M est naturellement un A-module pour la multiplication extérieure $A \times M \to M$, $(a,n) \to \phi(a) \cdot n$. On notera $\phi^* M$ ou $M|_A$ lorsqu'il n'y a pas d'ambiguité sur $\phi : A \to B$ le A-module ainsi obtenu à partir du B-module N. On notera que tout morphisme de B-modules $f : M \to N$ est automatiquement un morphisme de A-modules $f|_A = f : M|_A \to N_A$. En particulier, une structure de A-algèbre $\phi : A \to B$ sur un anneau

B détermine une structure de A-module ϕ^*B sur B. Inversement, une structure de A-module $\cdot : A \times B \to B$ sur le groupe abélien sous-jacent $(B, +)$ d'un anneau B détermine une structure de A-algèbre $\phi : A \to B$ sur B en posant $\phi(a) = a \cdot 1_B$. En particulier, si M est un A-module, $End(M)$ est naturellement muni d'une structure de A-algèbre.

- Soit A un anneau commutatif. Par la propriété universelle de $\iota_A : A \to A[X_1, \ldots, X_n]$, la donnée d'un $A[X_1, \ldots, X_1]$-module est équivalente à la donnée d'un couple $(M, \underline{\phi})$, où M est un A-module et $\underline{\phi} := (\phi_1, \ldots, \phi_n)$ est un n-uplet d'endomorphismes A-linéaires de M qui commutent deux à deux. Par exemple, si V est un k-espace vectoriel de dimension finie, et $u \in \mathrm{End}_k(V)$, on peut munir V de la structure V_u de $k[X]$-module définie par $P(X) \cdot v = P(u)(v)$. Si $u, u' \in \mathrm{End}_k(V)$, on a
$$\mathrm{Hom}_{k[X]}(V_u, V_{u'}) = \{\varphi : V \to V \mid \varphi \circ u = u' \circ \varphi\}.$$
Un certain nombre de résultats d'algèbre linŕaire s'interprètent (et deviennent bien plus naturels!) en termes de $k[X]$-modules.

8.1.3. Si M est un A-module, un *sous A-module* de M est un sous-ensemble $M' \subset M$ tel que $aM' \subset M'$, $a \in A$.

Exemple.
- Les sous-A-modules du A-module régulier A sont les idéaux de A.
- Si $f : M \to N$ est un morphisme de A-module et $M' \subset M$ (resp. $N' \subset N$) est un sous-A-module alors $f(M') \subset N$ (resp. $f^{-1}(N') \subset M$) est un sous-A-module. En particulier, $\mathrm{im}(f) \subset N$ et $\ker(f) \subset M$ sont des sous-A-modules.
- Si M est un A-modules et X un ensemble, $Hom^{sf}_{Ens}(X, M) \subset Hom_{Ens}(X, M)$ est un sous-A-module. Si M, N sont deux A-modules, $Hom_A(M, N) \subset Hom_{Ens}(M, N)$ est un sous-A-module.
- Si $I \subset A$ est un idéal et M un A-module, $IM := \{\sum_{m \in M} a_m m \mid a_- : M \to I \in I^{(M)}\} \subset M$ est un sous-A-module.

8.2. Produits et sommes directes. Soit M_i, $i \in I$ une famille de A-modules.

On munit le groupe abélien produit $\prod_{i \in I} M_i$ de la structure de A-module
$$\begin{array}{ccc} A \times \prod_{i \in I} M_i & \to & \prod_{i \in I} M_i \\ (a, \underline{m} = (m_i)_{i \in I}) & \to & a \cdot \underline{m} = (a \cdot m_i)_{i \in I}. \end{array}$$
Avec cette structure de A-module, les projections canoniques $p_j : \prod_{i \in I} M_i \to M_j$, $j \in I$ deviennent des morphismes de A-modules.

On note $\bigoplus_{i \in I} M_i \subset \prod_{i \in I} M_i$ le sous A-module des $\underline{m} = (m_i)_{i \in I}$ tels que
$$|supp(\underline{m}) = \{i \in I \mid m_i \neq 0\}| < +\infty.$$
Les injections canoniques $\iota_j : M_j \hookrightarrow \bigoplus_{i \in I} M_i$, $j \in I$ sont des morphismes de A-modules. Si I est fini, on a tautologiquement $\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i$.

Lemme. (Propriété universelle du produit et de la somme directe) *Pour toute famille M_i, $i \in I$ de A-modules, il existe des morphismes de A-modules $p_i : \Pi \to M_i$, $i \in I$ et $\iota_i : M_i \to \Sigma$, $i \in I$ tels que*

(1) Pour toute famille de morphismes de A-modules $f_i : M \to M_i$, $i \in I$ il existe un unique morphisme de A-modules $f : M \to \Pi$ tel que $p_i \circ f = f_i$, $i \in I$.

(2) Pour toute famille de morphismes de A-modules $f_i : M_i \to M$, $i \in I$ il existe un unique morphisme de A-modules $f : \Sigma \to M$ tel que $f \circ \iota_i = f_i$, $i \in I$.

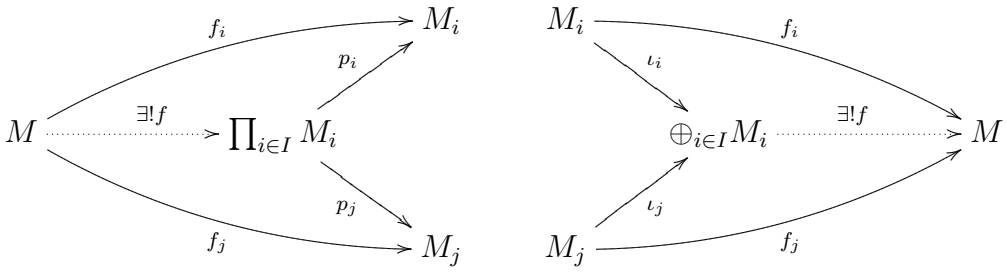
Proof. On vérifie comme d'habitude que les morphismes de A-modules $p_j : \prod_{i\in I} M_i \to M_j$, $j \in I$ et $\iota_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$, $j \in I$ construits ci-dessus conviennent. □

On peut aussi réécrire le lemme en disant que, pour tout A-module M les morphismes canoniques

$$\mathrm{Hom}_A(M, \prod_{i\in I} M_i) \to \prod_{i\in I} \mathrm{Hom}_A(M, M_i),\ f \to (p_i \circ f)_{i\in I}$$

$$\mathrm{Hom}_A(\oplus_{i\in I} M_i, M) \to \prod_{i\in I} \mathrm{Hom}_A(, M_i M),\ f \to (f \circ \iota_i)_{i\in I}$$

sont des isomorphismes ou encore, plus visuellement:



$f(m) = (f_i(m))_{i\in I}$ $\qquad$ $f(\underline{m}) = \sum_{i\in I} f_i(m_i)$

On remarquera que l'expression $f(\underline{m}) = \sum_{i\in I} f_i(m_i)$ ne fait sens que si $|supp(\underline{m})| < +\infty$.

Comme d'habitude, le produit $p_j : \prod_{i\in I} M_i \to M_j$, $j \in I$ et la somme directe $\iota_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$, $j \in I$ sont uniques à unique isomorphisme près.

Si $M_i = M$ pour tout $i \in I$, on notera $M^I := \prod_{i\in I} M_i$ et $M^{(I)} := \oplus_{i\in I} M_i$. Par construction, on a des isomorphismes canoniques

$$\mathrm{Hom}_A(A^{(I)}, -) \simeq \prod_{i\in I} \mathrm{Hom}_A(A, -) \simeq (-)^I$$

et on dit que $A^{(I)}$ est le *A-module libre de base I*.

Soit $f_i : M_i \to N_i$, $i \in I$ une famille de morphismes de A-modules. En appliquant la propriété universelle des $p_j : \prod_{i\in I} N_i \to N_j$, $j \in I$ à la famille de morphismes de A-modules

$$\prod_{i\in I} M_i \xrightarrow{p_j} M_j \xrightarrow{f_j} N_j,\ j \in I$$

on obtient un unique morphisme de A-modules $f := \prod_{i\in I} f_i : \prod_{i\in I} M_i \to \prod_{i\in I} N_i$ tel que $p_i \circ f = f \circ p_i$, $i \in I$. De même, en appliquant la propriété universelle des $\iota_j : M_j \to \oplus_{i\in I} M_i$, $j \in I$ à la famille de morphismes de A-modules

$$M_j \xrightarrow{f_j} N_j \xrightarrow{\iota_j} \oplus_{i\in I} M_i,\ j \in I$$

on obtient un unique morphisme de A-modules $f := \oplus_{i\in I} f_i : \oplus_{i\in I} M_i \to \oplus_{i\in I} N_i$ tel que $f \circ \iota_i = \iota_i \circ f$, $i \in I$.

Remarque. On notera les similitudes suivantes au niveau des propriétés universelles.

	A-modules	A-algèbres
Objets libres de rang fini	$A^{\oplus n}$	$A[X_1, \ldots, X_n]$
Coproduits finis	$\oplus_{1\leq i\leq n} M_i$	$A_1 \otimes_A \cdots \otimes_A A_n$
Produit	$\prod_{i\in I} M_i$	$\prod_{i\in I} A_i$

8.3. Sous-module engendré par une partie, sommes Si $M_i \subset M$, $i \in I$ est une famille de sous A-modules de M, on vérifie immédiatement que l'intersection

$$\bigcap_{i\in I} M_i \subset M$$

est encore un sous-A-module de M.

Si $X \subset M$ est un sous-ensemble, on note $\langle X\rangle$ l'intersection de tous les sous A-modules $M' \subset M$ contenant X. D'après ce qui précède, c'est encore un sous A-module de M et, par construction, c'est le plus petit sous A-module de M contenant X. On dit que $\langle X\rangle$ est le *sous A-module* engendré par X et on vérifie qu'il coincide avec l'ensemble des éléments de la forme $\sum_{x\in X} a(x)x$, où $a : X \to A$ est une application à support fini. La propriété universelle de $\iota_x : A \hookrightarrow A^{(X)}$, $x \in X$ appliquée aux morphismes de A-modules $- \cdot x : A \to M$, $a \to ax$, $x \in X$ nous donne un unique morphisme de A-modules $p_X : A^{(X)} \to M$ tel que $p_X \circ \iota_x(a) = ax$, $x \in X$. On vérifie immédiatement que les propriétés suivantes sont équivalentes:

(1) $M = \langle X\rangle$;
(2) Le morphsime de A-modules $p : A^{(X)} \to M$ est surjectif.

On dit alors que X est un système de générateurs de M comme A-modules (ou que M est engendré par X comme A-module). Si on peut prendre X fini, on dit que M est un A-module *de type fini*.

Si $M_i \subset M$, $i \in I$ est une famille de sous A-modules de M, on note

$$\sum_{i\in I} M_i = \langle \bigcup_{i\in I} M_i\rangle \subset M.$$

Là encore la propriété universelle de $\iota_i : M_i \hookrightarrow \oplus_{i\in I} M_i$, $i \in I$ appliquée aux morphismes de A-modules $M_i \subset \sum_{i\in I} M_i$ (inclusion), $i \in I$ nous donne un unique morphisme de A-modules - automatiquement surjectif - $p : \oplus_{i\in I} M_i \twoheadrightarrow \sum_{i\in I} M_i (\subset M)$ tel que $p \circ \iota_i(m_i) = m_i$, $m_i \in M_i$, $i \in I$.

8.4. Quotients. Soit $M' \subset M$ un sous A-module. C'est en particulier un sous groupe abélien et on dispose donc du quotient $p_{M'} := \overline{(-)} : M \to M/M'$ comme groupe abélien. On peut munir M/M' d'une structure de A-module comme suit. Pour tout $a \in A$, l'application

$$\begin{array}{rccc} \mu_a\colon & M & \to & M/M' \\ & m & \to & \overline{a\cdot m} \end{array}$$

est un morphisme de groupes abéliens tel que $M' \subset \ker(\mu_a)$; il se factorise donc en

$$\begin{array}{ccc} M & \xrightarrow{\mu_a} & M/M' \\ {\scriptstyle \overline{(-)}}\downarrow & \nearrow_{\overline{\mu}_a} & \\ M/M' & & \end{array}$$

On pose alors

$$\begin{array}{rcl} A \times M/M' & \to & M/M' \\ (a, \overline{m}) & \to & a\cdot\overline{m} := \overline{\mu}_a(m)(= \overline{a\cdot m}). \end{array}$$

On vérifie immédiatement que cela définit bien une structure de A-module sur M/M' et que c'est l'unique structure de A-module sur M/M' qui fait de $\overline{(-)} : M \to M/M'$ un morphisme de A-modules. De plus,

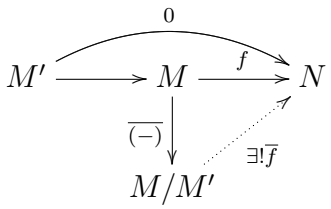
Lemme. (Propriété universelle du quotient) *Pour tout sous-A-module $M' \subset M$ il existe un morphisme de A-modules $p : M \to Q$ tel que pour tout morphisme de A-modules $f : M \to N$ tels que $M' \subset \ker(f)$, il existe unique morphisme de A-modules $\overline{f} : Q \to N'$ tel que $\overline{f} \circ p = f$.*

Proof. On vérifie comme d'habitude que le morphisme de A-modules $p_{M'} = \overline{(-)} : M \twoheadrightarrow M/M'$ construit ci-dessus convient. □

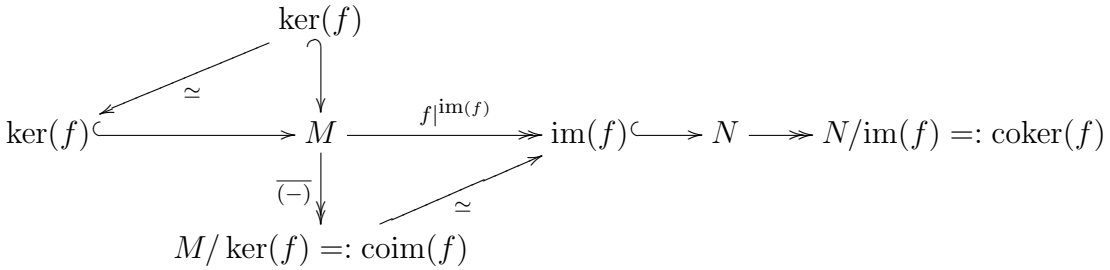
On peut aussi réécrire le lemme en disant que, pour tout A-module N le morphisme canonique

$$\mathrm{Hom}_A(M/M', N) \to \{M \xrightarrow{f} N \mid M' \subset \ker(f)\},\ \overline{f} \to \overline{f} \circ \overline{(-)}$$

est un isomorphisme ou encore, plus visuellement:



On observera que $M' = \ker(\overline{(-)})$ et $M/M' = \mathrm{im}(\overline{(-)})$. Inversement, si $f : M \to N$ est un morphisme de A-modules, on a un diagramme commutatif canonique de morphismes de A-modules



On a donc une correspondance bijective entre sous A-modules et noyaux de morphismes de A-modules d'une part et A-modules quotients et images de morphismes de A-modules d'autre part. Même si les A-modules $\mathrm{im}(f)$ et $M/\ker(f)$ sont isomorphes, on notera parfois $\mathrm{coim}(f) := M/\ker(f)$ (coimage). On note $\mathrm{coker}(f) := N/\mathrm{im}(f)$ (conoyau).

8.5. Suites exactes, lemme du serpent et lemme des cinq. On dit qu'une suite de morphismes de A-modules

$$M_0 \xrightarrow{u_0} M_1 \xrightarrow{u_1} M_2 \xrightarrow{u_2} \cdots \xrightarrow{u_n} M_{n+1}$$

est exacte si $\mathrm{im}(u_i) = \ker(u_{i+1})$ pour tout $0 \leq i \leq n-1$. Une suite exacte courte est une suite exacte de la forme:

$$0 \to M' \to M \to M'' \to 0.$$

La notion de suite exacte est au coeur de l'étude de la structure des A-module. La raison première est que c'est l'outil qui permet de 'dévisser' un A-module compliqué (M) en deux A-modules plus simples (M' et M'').

8.5.1. Lemme. *Soit*

$$0 \to M' \stackrel{u}{\to} M \stackrel{v}{\to} M'' \to 0$$

une suite exacte courte de A-modules. Les propriétés suivantes sont équivalentes:
(1) il existe un morphisme de A-modules $s : M'' \to M$ tel que $v \circ s = Id_{M''}$;
(2) il existe un morphisme de A-modules $r : M' \to M'$ tel que $r \circ u = Id_{M'}$;
(3) il existe un isomorphisme de A modules $f : M \tilde{\to} M' \oplus M''$ tel que $\iota_{M'} = f \circ u$ et $p_{M''} \circ f = v$.

On dit qu'une suite exacte courte vérifiant les conditions équivalentes ci-dessus est *scindée*.

Proof. On peut par exemple montrer (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2): Si $s : M'' \to M$ est un morphisme de A-modules tel que $vs = Id_{M''}$ on vérifie que le morphisme de A-modules $Id - sv : M \to M$ a son image contenue dans $\ker(v) = u(M')$ et que $t := (u|^{u(M')})^{-1} \circ (Id - sv) : M \to M'$ vérifie bien $tu = Id_{M'}$.

(2) $\Rightarrow$ (3): Si $s : M \to M'$ est un morphisme de A-modules tel que $su = Id_{M'}$, on peut considérer $f := s \oplus v : M \to M' \oplus M''$. Par construction, $p_{M''} \circ f = v$ et $f \circ u(s(m)) = s(m) = \iota_{M'}(s(m))$ donc, comme $s : M \to M'$ est surjective, $f \circ u = \iota_{M'}$. Enfin, $f : M \to M' \oplus M''$ est un isomorphisme. Il est injectif car si $f(m) = 0$ alors $v(m) = 0$ *i.e.* $m \in \ker(v) = u(M')$ donc $m = u(m')$ et $m' = su(m') = 0$. Donc, en fait $m = 0$. Il est surjectif car pour tout $m' \in M'$, $m'' \in M''$, on peut écrire $m'' = v(m) = v(m - us(m) + u(m'))$ et $m' = su(m') = s(m - us(m) + u(m'))$.

(3) $\Rightarrow$ (1): Si $f : M \tilde{\to} M' \oplus M''$ est un isomorphisme de A-modules tel que $p_{M''} \circ f = v$ et $f \circ u = \iota_{M'}$, on peut considérer $s := f^{-1} \circ \iota_{M''} : M'' \to M$. Par construction $vs(m) = vf^{-1}\iota_{M''} = p_{M''}\iota_{M''} = Id_{M''}$. □

8.5.2. Exemple (*cf.* TD 4 pour la correction).
(1) Si $n \geq 2$ est un entier, montrer que la suite de $\mathbb{Z}$-modules $0 \to \mathbb{Z} \stackrel{n\cdot}{\to} \mathbb{Z} \to \mathbb{Z}/n \to 0$ n'est pas scindée.
(2) On considère les structure de $\mathbb{Z}[X]$-modules suivantes sur $\mathbb{Z}^2$
   (a) $X \cdot (a, b) = (a + b, b)$;
   (b) $X \cdot (a, b) = (b, a)$.
   Dans le cas (a), la suite exacte courte de $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z} \stackrel{a \to (a,0)}{\to} \mathbb{Z}^2 \to \mathbb{Z} \to 0$$

   est-elle scindée? Même question avec la suite exacte courte de $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z} \stackrel{a \to (a,a)}{\to} \mathbb{Z}^2 \to \mathbb{Z} \to 0$$

   dans le cas (b). Que se passe-t-il si on remplace $\mathbb{Z}$ par $\mathbb{Q}$?

8.5.3. Lemme du serpent Soit

$$\begin{array}{ccc} M' & \xrightarrow{u'} & M \\ {\scriptstyle \alpha'}\downarrow & & \downarrow{\scriptstyle \alpha} \\ N' & \xrightarrow[v']{} & N \end{array}$$

un diagramme commutatif de morphismes de A-modules. La commutativité assure que $u' : M' \to M$ se restreint en un morphisme $\ker(\alpha') \to \ker(\alpha)$ et que $v'(im(\alpha')) \subset im(\alpha)$ donc que $v' : N' \to N$

induit un morphisme canonique $\operatorname{coker}(\alpha') \to \operatorname{coker}(\alpha)$.
Soit

$$\begin{array}{ccccccc} & & M' & \xrightarrow{u'} & M & \xrightarrow{u} & M'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} \\ 0 & \longrightarrow & N' & \xrightarrow[v']{} & N & \xrightarrow[v]{} & N'' \end{array}$$

un diagramme commutatif de morphismes de A-modules dont les lignes horizontales sont exactes.

Lemme. (du serpent) *Il existe un morphisme 'naturel' $\delta : \ker(\alpha'') \to \operatorname{coker}(\alpha')$ tel que la suite de morphismes*

$$\ker(\alpha') \to \ker(\alpha) \to \ker(\alpha'') \xrightarrow{\delta} \operatorname{coker}(\alpha') \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\alpha'')$$

est exacte. En particulier,
- *si α', α'' sont injectives (resp. surjectives) alors α est injective (resp. surjective).*
- *On suppose de plus que $u' : M' \to M$ est injective et $v : N \to N''$ est surjective. Montrer que si deux des trois morphismes α, α', α'' sont des isomorphismes alors le troisième l'est aussi.*

Proof. Considérons la restriction de α à ${u'}^{-1}(\ker(\alpha''))$. Si $m \in {u'}^{-1}(\ker(\alpha''))$ on a $v' \circ \alpha(m) = \alpha'' \circ u'(m) = 0$ donc $\alpha({u'}^{-1}(\ker(\alpha''))) \subset \ker(v') = im(v)$. Mais comme v est injectif, il induit un isomorphisme sur son image. On peut donc considérer le morphisme composé:

$$\widetilde{\delta} : {u'}^{-1}(\ker(\alpha'')) \xrightarrow{\alpha} im(v) \xrightarrow{(v|^{im(v)})^{-1}} N' \xrightarrow{p_{im(\alpha')}} Coker(\alpha').$$

On a de plus, pour tout $m = u(m') \in \ker(u') = im(u)$, $v^{-1}\alpha u(m') = v^{-1}v\alpha'(m') = \alpha'(m') \in im(\alpha')$ donc $\ker(u') \subset \ker(\widetilde{\delta})$, ce qui montre que $\widetilde{\delta} : {u'}^{-1}(\ker(\alpha'')) \to Coker(\alpha')$ se factorise en $\delta : \ker(\alpha'') \simeq {u'}^{-1}(\ker(\alpha''))/\ker(u) \to Coker(\alpha')$. Cela donne la construction de $\delta : \ker(\alpha'') \to \operatorname{coker}(\alpha')$. On laisse le soin au lecteur de vérifier que la suite longue de l'énoncé est bien exacte. □

8.5.4. Soit

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

un diagramme commutatif de morphismes de A-modules dont les lignes horizontales sont exactes.

Corollaire. (lemme des cinq)
(1) Si α_1 est surjectf et α_2, α_4 sont injectifs, α_3 est injective.
(2) Si α_5 est injectif et α_2, α_4 sont surjectifs,

Proof. cf. T.D.4. □

9. Conditions de finitude

Soit A un anneau commutatif.

9.1. Lemme. *Soit M un A-module. Les conditions suivantes sont équivalentes.*
(1) Toute suite croissante de sous A-modules

$$M_0 \subset M_1 \subset \cdots \subset M_n \subset M_{n+1} \subset \cdots \subset M$$

est stationnaire à partir d'un certain rang;
(2) Tout ensemble non vide de sous A-modules de M possède un élément maximal pour l'inclusion;

(3) Tout sous A-module de M est de type fini.

Un A-module M vérifiant les conditions équivalentes du Lemme 9.1 est dit *noetherien*.

Proof. (1) $\Rightarrow$ (2): Si (2) n'était pas vrai, il existerait un ensemble non vide $\mathcal{E}$ de sous A-modules de M ne contenant aucun élément maximal pour l'inclusion. Soit $M_0 \in \mathcal{E}$. Comme M_0 n'est pas maximal pour l'inclusion, il existe $M_1 \in \mathcal{E}$ tel que $M_0 \subsetneq M_1$. On itère l'argument avec M_1 et on construit ainsi une suite strictement croissante infinie de sous A-modules de M, ce qui contredit (1).
(2) $\Rightarrow$ (3): Soit $M' \subset M$ un sous A-module et $\mathcal{E}$ l'ensemble des sous A-modules de type fini de M'. Comme le module trivial $\{0\}$ est dans $\mathcal{E}$, $\mathcal{E}$ est non-vide donc admet un élément M'' maximal pour l'inclusion. Pour tout $m \in M'$, le A-module $M'' + Am$ est dans $\mathcal{E}$ et contient M''. Par maximalité de M'', on a $M'' + Am = M''$ donc $m \in M''$.
(3) $\Rightarrow$ (1): Soit

$$M_0 \subset M_1 \subset \cdots \subset M_n \subset M_{n+1} \subset \cdots \subset M$$

une suite croissante de sous A-modules. La réunion

$$U := \bigcup_{n \geq 0} M_n \subset M$$

est un sous A-module. Soit $m_1, \ldots, m_r$ une famille de générateurs de U. Chaque m_i est dans M_{n_i} pour un certain $n_i \geq 0$. Avec

$$N := \max\{n_i \mid i = 1, \ldots, r\}$$

on a $M_n = M_N$, $n \geq N$. □

Remarque. Un anneau A est en particulier noetherien au sens de 4 s'il l'est comme A-module sur lui-même.

9.2. Lemme. *Soit M un A-module. Les conditions suivantes sont équivalentes.*

(1) Toute suite décroissante de sous A-modules

$$M \supset \cdots \supset M_0 \supset M_1 \supset \cdots \supset M_n \supset M_{n+1} \supset \ldots$$

est stationnaire à partir d'un certain rang;

(2) Tout ensemble non vide de sous A-modules de M possède un élément minimal pour l'inclusion.

Un A-module M vérifiant les conditions équivalentes du Lemme 9.2 est dit *artinien*. On laisse en exercice la preuve du Lemme 9.2, qui est exactement similaire à celle du Lemme 9.1

9.3. Exemple.

(1) Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est ni noetherien ni artinien.
(2) Le $\mathbb{Z}$-module régulier est noetherien mais pas artinien.
(3) Le $\mathbb{Z}$-module $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ est artinien mais pas noetherien. En effet, les sous $\mathbb{Z}$-modules de $M = \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ sont M et les $M_n = (\mathbb{Z}\frac{1}{p^n} + \mathbb{Z})/\mathbb{Z}$, $n \geq 0$. Les sous-$\mathbb{Z}$-modules de M sont en bijection avec les sous-$\mathbb{Z}$-modules de $\mathbb{Z}[\frac{1}{p}]$ qui contiennent $\mathbb{Z}$. Soit $M' \subset \mathbb{Z}[\frac{1}{p}]$ un tel sous-$\mathbb{Z}$-module. Observons que si $\frac{a}{p^n} \in M'$ avec $p \not| a$ et $n \geq 0$ alors $\frac{1}{p^n} \in M'$. En effet, par Bézout, on peut écrire $ua + vp^n = 1$ donc $\frac{1}{p^n} = v + u\frac{a}{p^n} \in M'$. Soit maintenant $-N := inf v_p(N)$. Si $N = +\infty$ cela veut dire que pour tout $n \geq 0$ il existe $N_n \geq n$ et un élément de la forme $\frac{a}{p^{N_n}} \in M'$ avec $p \not| a$ donc $\frac{1}{p^{N_n}} \in M'$ donc $\frac{1}{p^n} = p^{N_n - n}\frac{1}{p^{N_n}} \in M'$ donc $M' = \mathbb{Z}[\frac{1}{p}]$. Si $N < +\infty$, on a $N \subset \mathbb{Z}\frac{1}{p^N}$ et M' contient un élément de la forme $\frac{a}{p^N}$ avec $p \not| a$ donc $\frac{1}{p^N} \in M'$ donc $\mathbb{Z}\frac{1}{p^N} \subset M'$. *In fine*, l'ensemble des sous $\mathbb{Z}$-modules de M est totalement ordonné en une suite strictement croissante

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n \subsetneq M_{n+1} \subsetneq \cdots \subsetneq M$$

(4) Tout $\mathbb{Z}$-module fini est à la fois noetherien et artinien. Si A est une algèbre sur un corps k, tout A-module de k-dimension finie est à la fois noetherien et artinien.

9.4. Lemme.
(1) Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de A-modules. Alors M est noetherien (resp. artinien) si et seulement si M' et M'' sont noetheriens (resp. artininens).
(2) Une somme directe finie de A-modules noetheriens (resp. artiniens) est encore noetherien (resp. artinien).
(3) Tout module de type fini sur un anneau noethérien (resp. artinien) est noetherien (resp. artinien).

Proof. (1) Supposons M noetherien (resp. artinien). Toute suite croissante (resp. décroissante) de sous-A modules de M' est une suite de sous-A modules de M donc stationne à partir d'un certain rang. De même, l'image inverse dans M de toute suite croissante (resp. décroissante) de sous-A modules de M'' est une suite de sous-A modules de M donc stationne à partir d'un certain rang. Supposons M' et M'' noetheriens (resp. artiniens). Soit $M_1 \subset \cdots \subset M_n \subset M_{n+1} \subset \ldots M$ une suite croissante de sous-A modules de M. Il existe un entier N tel que $M_N \cap M' = M_n \cap M'$ et $(M_N + M')/M' = (M_n + M')/M'$n $n \geq N$. La conclusion résulte du lemme du serpent appliqué à

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_N \cap M' & \longrightarrow & M_N & \longrightarrow & (M_N + M')/M' & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & M_n \cap M' & \longrightarrow & M_n & \longrightarrow & (M_n + M')/M' & \longrightarrow & 0 \end{array}$$

L'assertion pour 'artinien' se montre de la même façon.
(2) On procède par induction sur n en utilisant 1.3.4 (1) et la suite exacte courte de A-modules

$$0 \to \oplus_{1 \leq i \leq n} M_i \to \oplus_{1 \leq i \leq n+1} M_i \to M_{n+1} \to 0.$$

(3) D'après 1.3.4 (2) $A^{\oplus n}$ est noetherien (resp. artinien) et, par définition, tout A-module de type fini est quotient d'un A-module de la forme $A^{\oplus n}$. Donc la conclusion résulte de 1.3.4 (1).

□

La propriété d'être noetherien et artinien est la bonne généralisation de la notion de dimension finie lorsque $A = k$ est un corps. Les points (1) et (2) du lemme suivant, par exemple, servent de substitut au Lemme du rang.

9.5. Lemme. (Fitting) *Soit $f : M \to M$ un endomorphisme de A-module.*
(1) Si M est noetherien et f surjectif alors f est un isomorphisme.
(2) Si M est artinien et f injectif alors f est un isomorphisme.
(3) (Lemme de 'Fitting') Si M est artinien et noetherien alors il existe une décomposition $M = f^\infty(M) \oplus f^{-\infty}(0)$ en somme directe de deux sous A-modules f-stables tels que la restriction de f à $f^\infty(M)$ soit un automorphisme et la restriction de f à $f^{-\infty}(0)$ soit nilpotente.

Proof. (1) Il existe un entier $N \geq 1$ tel que $\ker(f^N) = \ker(f^n)$, $n \geq N$ et on applique le lemme du serpent à

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f^N) & \longrightarrow & M & \xrightarrow{f^N} & M & \longrightarrow & 0 \\ & & \downarrow \simeq & & \simeq \downarrow Id & & \downarrow f & & \\ 0 & \longrightarrow & \ker(f^{N+1}) & \longrightarrow & M & \xrightarrow[f^{N+1}]{} & M & \longrightarrow & 0 \end{array}$$

(2) Il existe un entier $N \geq 1$ tel que $\mathrm{im}(f^N) = \mathrm{im}(f^n)$, $n \geq N$ et on applique le lemme du serpent à

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{f^{N+1}} & M & \longrightarrow & M/\mathrm{im}(f^{N+1}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle Id} & & \downarrow{\scriptstyle \simeq} & & \\ 0 & \longrightarrow & M & \xrightarrow[f^N]{} & M & \longrightarrow & M/\mathrm{im}(f^N) & \longrightarrow & 0 \end{array}$$

(3) (3) Comme Mest artinien et noetherien, il existe un entier $N \geq 1$ tel que

$$f^\infty(M) := \bigcap_{n\geq 0} \mathrm{im}(f^n) = \mathrm{im}(f^N), \quad f^{-\infty}(M) := \bigcup_{n\geq 0} \ker(f^n) = \ker(f^N).$$

On vérifie que $f^\infty(M)$, $f^{-\infty}(M)$ ainsi définis conviennent. Le seul point un peu astucieux est $M = f^\infty(M) + f^{-\infty}(M)$. On a envie d'écrire $m = f^N(\mu) + m - f^N(\mu)$ pour un certain $\mu \in M$. Mais il faut pouvoir choisir μ de sorte que $f^N(m - f^N(\mu)) = 0$ *i.e.* $f^N(m) = f^{2N}(\mu)$. Or comme $\mathrm{im}(f^N) = \mathrm{im}(f^{2N})$ un tel $\mu \in M$ existe effectivement.

□

10. Modules indécomposables, Krull-schmidt

10.1. Modules indécomposables. Un A-module M est dit *indécomposable* s'il est non nul et ne peut s'écrire sous la forme $M = M' \oplus M''$ avec $M', M'' \subset M$ deux sous A-modules non nuls. Un A-module M est dit *totalement décomposable* s'il peut s'écrire sous la forme $M = M_1 \oplus \cdots \oplus M_r$ avec $M_1, \ldots, M_r \subset M$ des sous A-modules indécomposables.

Un anneau E (non nécessairement commutatif ici!) est dit *local* si $E \setminus E^\times$ est un idéal; auquel cas, $E \setminus E^\times$ est l'unique idéal bilatère maximal de E.

10.2. Lemme. *Soit M un A-module. Si $E := \mathrm{End}_A(M)$ est local, M est indécomposable. Réciproquement, si M est artinien, noetherien et indécomposable, E est local.*

Proof. Supposons E local et qu'on puisse écrire $M = M' \oplus M''$ avec $M', M'' \subset M$ deux sous A-modules non nuls. Notons $e := \iota_{M'} \circ p_{M'} \in E$ la projection de M sur M' parallèlement à M''. On a $e, 1-e \in E \setminus E^\times$. Mais si E est local, $E \setminus E^\times$ est un idéal donc $1 = e + (1-e) \in E \setminus E^\times$: contradiction. Supposons maintenant que M est un A-module artinien et noetherien indécomposable, d'après le Lemme 9.5 (3), tout élément non nul de E est soit inversible soit nilpotent. En particulier $J := E \setminus E^\times$ est l'ensemble des éléments nilpotents de E. Il suffit de montrer que J est un idéal bilatère. Soit donc $j \in J$ et $e \in E$. Comme j est nilpotent on a $\ker(j) \neq 0$ et $\mathrm{im}(j) \neq M$ (Lemme 9.5 (1), (2)). Donc aussi $\ker(ej) \neq 0$ et $\mathrm{im}(je) \neq M$, ce qui montre que $ej, je \in E \setminus E^\times = J$. Donc $EJ = JE = J$. Il reste à voir que J est stable par addition. Soit $j, j' \in J$, si $j + j' \in E^\times$ il existerait $e \in E$ tel que $ej = 1 - ej'$. Comme $ej' \in J$, on a forcément $1 - ej' \in E^\times$ (d'inverse $\sum_{n\geq 0}(ej')^n$), ce qui contredit le fait que $j \in J$. □

10.3. Théorème de Krull-Schmidt. Notons $Ind(A)$ un système de représentants de l'ensemble des classes d'isomorphismes de A-modules indécomposables.

10.3.1. Théorème. (Krull-Schmidt) *Soit M un A-module artinien ou noetherien. Alors il existe une application à support finie $\kappa : Ind(A) \to \mathbb{Z}_{\geq 0}$ telle que*

$$M = \bigoplus_{N \in Ind(A)} N^{\oplus \kappa(N)}.$$

Si M est à la fois artinien et noetherien alors $\kappa : Ind(A) \to \mathbb{Z}_{\geq 0}$ est unique; on la notera $\kappa_M : Ind(A) \to \mathbb{Z}_{\geq 0}$.

Proof. Commençons par montrer l'existence de la décomposition. Raisonnons par l'absurde. Si M n'est pas totalement décomposable, M n'est en particulier pas indécomposable donc

$$M = M_1^{(0)} \oplus M_2^{(0)}$$

avec $0 \neq M_1^{(0)}, M_2^{(0)} \subset M$ deux sous A-modules dont l'un au moins des deux - disons $M_1^{(0)}$ n'est pas totalement décomposable. On itère l'argument pour obtenir une suite de décompositions en sommes directes de sous A-modules non nuls

$$M = M_1^{(1)} \oplus M_2^{(1)} \oplus M_2^{(0)}$$

$$\cdots$$

$$M = M_1^{(n+1)} \oplus M_2^{(n+1)} \oplus M_2^{(n)} \oplus M_2^{(n-1)} \oplus \cdots \oplus M_2^{(1)} \oplus M_2^{(0)}$$

avec, à chaque fois, $M_1^{(n)}$ qui n'est pas totalement décomposable. On obtient en particulier une suite strictement croissante de sous A-modules

$$\{0\} \subset M_2^{(0)} \subset M_2^{(1)} \oplus M_2^{(0)} \subset \cdots \subset M_2^{(n)} \oplus \cdots M_2^{(1)} \oplus M_2^{(0)} \subset \cdots$$

et une suite strictement décroissante de sous A-modules

$$M \supset M_1^{(0)} \supset M_1^{(0)} \supset \cdots \supset M_1^{(n)} \supset M_1^{(n+1)} \supset \cdots$$

Supposons maintenant que M est artinien et noetherien et montrons l'unicité de la décomposition. D'après le Lemme 10.2 et par récurrence, il suffit de montrer que si on a un isomorphisme de A-modules noetherien et artinien

$$M \oplus M' \simeq N_1 \oplus \cdots \oplus N_s =: N$$

avec $E := \mathrm{End}_A(M)$ local et les $N_1, \ldots, N_s$ indécomposables alors il existe $1 \leq i \leq s$ tel que $M \simeq N_i$ et $M' \simeq \oplus_{j \neq i} N_j$. Soit $\Phi = (\phi \ \phi') : M \oplus M' \tilde{\to} N$ ($\phi = \Phi \circ \iota_M$, $\phi' = \Phi \circ \iota_{M'}$) un isomorphisme de A-modules d'inverse

$$\Psi = \begin{pmatrix} \psi \\ \psi' \end{pmatrix} : N \tilde{\to} M \oplus M' \ \ (\psi = p_M \circ \Psi, \ \psi' = p_{M'} \circ \Psi).$$

Par le lemme 10.2, $E \setminus E^\times$ est un idéal bilatère et l'égalité

$$Id_M = p_M \circ Id_{M \oplus M'} \circ \iota_M = (p_M \circ \Psi) \circ (\Phi \circ \iota_M) = \psi \circ \phi = \psi \circ Id_N \circ \phi = \psi \circ (\sum_{1 \leq i \leq n} \iota_i \circ p_i) \circ \phi = \sum_{1 \leq i \leq s} \psi \circ \iota_i \circ p_i \circ \phi$$

(où on a écrit $\iota_i := \iota_{N_i}$ et $p_i := p_{N_i}$ pour simplifier) implique que $\chi_i := \psi \circ \iota_i \circ p_i \circ \phi \in E^\times$ pour au moins un $i = 1, \ldots, s$. On a alors $p_i \circ \phi : M \hookrightarrow N_i$ injectif, $\psi \circ \iota_i : N_i \twoheadrightarrow M$ surjectif et

$$0 \longrightarrow \ker(\psi \circ \iota_i) \longrightarrow N_i \underset{p_i \circ \phi \circ \chi_i^{-1}}{\overset{\psi \circ \iota_i}{\longrightarrow}} \mathrm{im}(\psi \circ \iota_i) \longrightarrow 0$$

donc

$$N_i = \ker(\psi \circ \iota_i) \oplus \mathrm{im}(p_i \circ \phi).$$

Comme par hypothèse N_i est indécomposable on a forcément $\ker(\psi \circ \iota_i) = 0$ et $\mathrm{im}(p_i \circ \phi) = N_i$. Donc $p_i \circ \phi : M \tilde{\to} N_i$ et $\psi \circ \iota_i : N_i \tilde{\to} M$ sont des isomorphismes. Il reste à voir que $M' \simeq \oplus_{j \neq i} N_j$. Pour cela, considérons les suites exactes courtes de A-modules:

$$0 \to M \overset{\iota}{\to} M \oplus M' \overset{p}{\to} M' \to 0$$

$$0 \to \bigoplus_{i \neq j} N_j \overset{\Psi \circ \iota_i'}{\to} M \oplus M' \overset{p_i \circ \Phi}{\to} N_i \to 0.$$

On sait que $p_i \circ \Phi \circ \iota = p_i \circ \phi : M \tilde{\to} N_i$ est un isomorphisme et on voudrait montrer que $p \circ \Psi \circ \iota'_i : \bigoplus_{i \neq j} N_j \to M'$ en est un aussi. Cela découle du petit lemme suivant, dont on laisse la preuve en exercice au lecteur. □

10.3.2. Lemme.

(1) Soit $0 \to K \xrightarrow{\alpha} M \xrightarrow{\beta} Q$ et $0 \to K' \xrightarrow{\alpha'} M \xrightarrow{\beta'} Q'$ deux suites exactes de A-modules. Alors $\beta'\alpha$ est injectif si et seulement si $\beta\alpha'$ est injectif.

(2) Soit $K \xrightarrow{\alpha} M \xrightarrow{\beta} Q \to 0$ et $K' \xrightarrow{\alpha'} M \xrightarrow{\beta'} Q' \to 0$ deux suites exactes de A-modules. Alors $\beta'\alpha$ est surjectif si et seulement si $\beta\alpha'$ est surjectif.

11. Modules de type fini sur les anneaux principaux

11.1. Soit M un A-module. Un élément $m \in M$ est dit *de torsion* s'il existe $a \in A \setminus A_{tors}$ tel que $am = 0$. On note $T_M \subset M$ l'ensemble des éléments de torsion de M. On vérifie immédiatement que c'est un sous A-module et que le A-module M/T_M est sans torsion. Le A-module M s'insère donc dans la suite exacte courte

$$(*) \quad 0 \to T_M \to M \to M/T_M \to 0,$$

où T_M est de torsion et M/T_M est sans torsion. Cela indique la voie pour classifier les A-modules de type fini: montrer que la suite exacte courte $(*)$ se scinde, ce qui par le Lemme 8.5.1 impliquera automatiquement que

$$M \tilde{\to} T_M \oplus M/T_M$$

et réduit donc le problème de la classification des A-modules de type fini à

- la classification des A-modules de type fini sans torsion;
- la classification des A-modules de type fini de torsion.

En fait, on va plutôt procéder dans l'ordre suivant. Notons que si A est noetherien (*e.g.* principal...) et M de type fini, M est noetherien. Donc T_M et M/T_M sont aussi noetheriens donc de type fini.

(1) La raison pour laquelle on se restreint aux A-modules de type fini provient du lemme suivant.

11.1.1 **Lemme.** *Si A est un anneau principal tout A-module de type fini et de torsion est noetherien et artinien.*

Proof. Soit M un A-module de type fini et de torsion. Soit $m_1, \ldots, m_r \in M$ un système de générateurs. Pour chaque $i = 1, \ldots, r$ on peut trouver un élément $0 \neq a_i \in A$ tel que $a_i m_i = 0$. On a donc une factorisation

$$\begin{array}{ccc} A^{\oplus r} & \xrightarrow{(m_1,\ldots,m_r)} & M \\ \downarrow & \nearrow & \\ A/Aa_1 \oplus \cdots \oplus A/Aa_r & & \end{array}$$

D'après le Lemme 9.4, il suffit donc de montrer que les A-module de la forme A/Aa avec $0 \neq a \in A$ sont artiniens et noetheriens. Cela résulte du fait que A/Aa n'a qu'un nombre fini de sous-A-modules. En effet, observons qu'un sous-A-module $M \subset A/Aa$ est automatiquement un sous-A/Aa-module (car $aM = 0$). Or si on note $\pi : A \to A/Aa$ la projection canonique, o l'application $\mathcal{I}_{A/Aa} \to \mathcal{I}_A$, $M \mapsto \pi^{-1}(M)$ induit une bijection croissante pour $\subset$ de $\mathcal{I}_{A/Aa}$ sur les idéaux de $I \subset A$ tels que $Aa \subset I$. Mais comme A est principal, les idéaux I de cette forme sont les Ab avec $b|a$. Or comme principal $\Rightarrow$ factoriel, a n'a qu'un nombre fini de diviseurs (modulo $A^\times$). □

(2) On va ensuite montrer que tout A-modules libre (sur un anneau intègre) est classifié par son rang et qu'un A-module de type fini sans torsion sur un anneau principal est libre de rang fini. Cela permettra aussi d'appliquer l'observation suivante.

11.1.2 **Lemme.** *Si M'' est un A-module libre alors toute suite exacte courte de A-modules $0 \to M' \stackrel{u}{\to} M \stackrel{v}{\to} M'' \to 0$ est scindée.*

Proof. On construit une section en utilisant la propriété universelle de la somme directe. Plus précisément, quitte à composer v par un isomorphisme, on peut supposer que $M'' = A^{(I)}$. Pour chaque $i \in I$ notons $e_i = (\delta_{i,j})_{j\in I} \in A^{(I)}$ et choisissons $m_i \in M$ tel que $v(m_i) = e_i$. Le choix de m_i définit un morphisme de A-module $s_i : Ae_i \stackrel{e_i \to m_i}{\to} Am_i \hookrightarrow M$. Par propriété universelle des $\iota_i : Ae_i \to A^{(I)}$, $i \in I$, on en déduit un unique morphisme $s : A^{(I)} \to M$ tel que $s \circ \iota_i = s_i$, $i \in I$. Par construction $v \circ s = Id$. □

(3) D'après le Lemme 11.1.1 et le Théorème de Krull-Schmidt 10.3.1, T_M est totalement décomposable et sa décomposition en somme directe de A-modules indécomposables est unique; le point sera donc de classifier les modules indécomposables de torsion sur un anneau principal A. On montrera que ce sont exactement les A-modules de la forme $A/\mathfrak{p}^n$, où $\mathfrak{p}$ est un idéal premier (=maximal) de A et $n \geq 0$.

11.2. Classification des A-modules de type fini sans torsion. Supposons d'abord que A est seulement un anneau commutatif intègre.

11.2.1. Lemme. *Un A-module de type fini sans torsion est isomorphe à un sous A-module d'un A-module libre de type fini.*

Proof. Soit $m_1, \dots m_r \in M$ un système de générateurs. L'ensemble

$$\mathcal{S} := \{I \subset \{1, \dots, r\} \mid A^I \stackrel{(m_i)_{i\in I}}{\hookrightarrow} M\}$$

est non vide (puisque M est sans torsion) donc contient un élément $I \subset \{1, \dots, r\}$ maximal pour l'inclusion. Notons

$$N := \sum_{i\in I} Am_i \simeq A^{(I)}.$$

Par maximalité de I, pour chaque $j \in I^c := \{1, \dots, r\} \setminus I$ il existe $0 \neq a_j \in A$ tel que $a_j m_j \in N$. Notons $a := \prod_{j\in I^c} a_j \in A$; c'est un élément non nul de A puisque A est intègre. On en déduit que le morphisme de A-module

$$\begin{array}{ccc} M & \to & N \\ m & \to & am \end{array}$$

est injectif, puisque M est sans torsion. □

11.2.2. Lemme. (Classification des A-modules libres de type fini par le rang)

(1) Le A-module libre $A^{(I)}$ est de type fini si et seulement si $|I| < +\infty$.

(2) Soit I, J deux ensembles finis. Alors $A^{(I)}$ et $A^{(J)}$ sont isomorphes comme A-modules si et seulement si $|I| = |J|$.

Proof. Le sens réciproque ("si") des assertions est immédiat. Prouvons le sens direct. L'idée est de se ramener au cas des espaces vectoriels sur un corps pour lesquels le lemme est connu. Soit donc M un A-module libre de type fini et I un ensemble pour lequel on a un isomorphisme de A-modules

$$f : A^{(I)} \tilde{\to} M.$$

Posons $m_i := f(e_i)$, où e_i est le 'i-ème vecteur de la base canonique', $i \in I$. Fixons un idéal maximal $\mathfrak{m} \subset A$ et considérons le $k := A/\mathfrak{m}$ espace vectoriel $M/\mathfrak{m}M$. On va montrer que les images $\overline{m}_i$, $i \in I$ des m_i, $i \in I$ dans $M/\mathfrak{m}M$ forment une k-base de $M/\mathfrak{m}M$. Cela assurera dans (2), que I est en bijection avec une k-base de $M/\mathfrak{m}M$, donc de cardinal indépendant de I. Cela impliquera également (1) puisque si $A^{(I)}$ est de type fini, $M/\mathfrak{m}M$ est un k-espace vectoriel de type fini donc de dimension finie. En particulier $|I| = dim_k(M/\mathfrak{m}M) < +\infty$.
On sait déjà que les $\overline{m}_i$, $i \in I$ forment une famille génératrice de $M/\mathfrak{m}M$ comme k-espace vectoriel. Montrons qu'elle est libre. Soit $a : I \to A$ à support fini telle que

$$\sum_{i \in I} a(i) m_i \in \mathfrak{m}M.$$

Comme $M = \oplus_{i \in I} Am_i$ et $A \tilde{\to} Am_i$, $a \to am_i$, $i \in I$, cela implique $a(i) \in \mathfrak{m}$ donc $\overline{a}_i = 0$, $i \in I$. □

Le Lemme 11.2.2 montre en particulier que si M est un A-module libre de type fini il existe un unique entier $r \geq 1$ tel que $M \simeq A^{\oplus r}$. On appelle cet entier le *rang* du A-module libre M. C'est également la dimension du $A/\mathfrak{m}$-espace vectoriel $M/\mathfrak{m}M$, pour $\mathfrak{m}$ un idéal maximal de A.

Supposons maintenant que A *est principal*.

11.2.3. Lemme. *Un sous A-module d'un A-module libre de rang fini r est un A-module libre de rang $\leq r$.*

Proof. On procède par récurrence sur r. Si $r = 1$, cela résulte du fait que A est principal. Supposons que l'énoncé du Lemme 11.2.3 est vérifié pour tout A-module libre de rang $\leq r$. Soit $M \subset A^{\oplus(r+1)}$ un sous A-module. Notons $p_{r+1} : A^{\oplus(r+1)} \twoheadrightarrow A$ la $r+1$-ième projection canonique. Comme $\ker(p_{r+1}) \simeq A^{\oplus r} \subset A^{\oplus(r+1)}$ est un A-module libre de rang r, par hypothèse de récurrence, le sous A-module $M \cap \ker(p_{r+1}) \subset \ker(p_{r+1})$ est un A-module libre de rang $s \leq r$. Comme $p_{r+1}(M) \subset A$ est un idéal et que A est principal, il existe $d_0 \in A$ tel que $p_{r+1}(M) = Ad_0 \overset{\cdot d_0}{\tilde{\leftarrow}} A$ et on conclut par le Lemme 11.1.2. □

On vient donc de montrer

11.2.4. Corollaire. *Un A-module de type fini sans torsion est libre de rang fini. Plus précisément, l'application $\mathbb{Z}_{\geq 0} \to \mathrm{Mod}_{/A}$, $r \to A^{\oplus r}$ induit une bijection de $\mathbb{Z}_{\geq 0}$ sur l'ensemble des classes d'isomorphismes de A-modules de type fini sans torsion.*

En particulier, M/T_M est un A-module libre de rang fini - disons r - donc, par le Lemme 11.1.2 on a

$$M \simeq T_M \oplus M/T_M \simeq T_M \oplus A^{\oplus r}.$$

Il reste à classifier les A-modules de type fini qui sont de torsion.

11.3. Classification des A-modules de type fini de torsion. Soit A un anneau principal.

11.3.1. Théorème. *Les A-modules de type fini de torsion qui sont indécomposables sont exactement les A-modules de la forme $A/\mathfrak{p}^n$, où $\mathfrak{p} \subset A$ est un idéal premier non nul et $n \in \mathbb{Z}_{\geq 0}$.*

Proof. Vérifions d'abord qu'un A-module de la forme $A/\mathfrak{p}^n$ est indécomposable. Observons que

$$\mathrm{End}_A(A/\mathfrak{p}^n) \simeq \mathrm{End}_{A/\mathfrak{p}^n}(A/\mathfrak{p}^n) \simeq A/\mathfrak{p}^n$$

a un unique idéal maximal (c'est par exemple la factorialité de A) - $\mathfrak{p}/\mathfrak{p}^n$, donc est local (ici $A/\mathfrak{p}^n$ est commutatif). Le fait que $A/\mathfrak{p}^n$ est indécomposable résulte alors du lemme 10.2.

Montrons maintenant que tout A-module indécomposable est de cette forme. Soit donc M un A-module. Pour $m \in M$, on note

$$Ann_A(m) := \{a \in A \mid am = 0\} \subset A$$

l'idéal annulateur de m et on se fixe un générateur $a_m \in Ann_A(m)$. On note également

$$Ann_A(M) := \bigcap_{m \in M} Ann_A(m) \subset A$$

l'idéal annulateur de M. Observons que l'énoncé est vrai, alors tout A-module indécomposable M est de la forme Am pour un certain $m \in M$ ($\overline{1} \in A/\mathfrak{p}^n$) tel que $Ann_A(M) = Ann_A(m) := \ker(A \to Am,\ a \mapsto am) = \mathfrak{p}^n$. Tout le jeu consiste donc à reconstruire $m \in M$ avec cette propriété à partir de la seule hypothèse que M est indécomposable.

11.3.1.1 **Lemme.** *Il existe $m \in M$ tel que $Ann_A(m) = Ann_A(M)$.*

Notons $B := A/Ann_A(m) = A/Ann_A(M)$ et considérons la suite exacte courte

$$0 \to B \xrightarrow{\cdot m} M \to M/Am \to 0.$$

On notera que comme $Ann_A(M)$ annnule M, cette suite est également une suite de B-modules.

11.3.1.2 **Lemme.** *La suite exacte courte de B-modules*

$$0 \to B \xrightarrow{\cdot m} M \to M/Am \to 0$$

est scindée.

Elle est donc *a fortiori* scindée comme suite exacte courte de A-modules *i.e.*

$$M \simeq A/Ann_A(M) \oplus M/Am$$

comme A-module. Mais comme M est indécomposable (et non nul), on en déduit $M = Am \simeq A/Ann_A(M) = A/Aa_m$. On conclut par la factorialité de A, le Lemme des restes Chinois et l'indécomposabilité de M. □

Preuve du lemme 11.3.1.1. Soit $m_1, \ldots, m_r$ un système de générateurs de M comme A-module. On a

$$Ann_A(M) = \cap_{1 \leq i \leq r} Ann_A(m_i).$$

Il suffit donc de montrer que pour tout $m_1, m_2 \in M$ il existe $m_3 \in M$ tel que

$$Ann_A(m_1) \cap Ann_A(m_2) = Ann_A(m_3).$$

Ecrivons $Ann_A(m_i) = Aa_i$, $i = 1, 2$. Comme A est factoriel, en utilisant la décomposition en produit de facteurs irréductibles de a_1 et a_2, on peut écrire $a_1 = \alpha_1\beta_1$ et $a_2 = \alpha_2\beta_2$ avec α_1, α_2 premier entre eux de produit 'le' plus petit commun multiple de a_1 et a_2 de sorte que $Aa_1 \cap Aa_2 = A(a_1 \vee a_2) = A\alpha_1\alpha_2 = A\alpha_1 \cap A\alpha_2$. Comme $A\alpha_1 = Ann_A(\beta_1 m_1)$, $A\alpha_2 = Ann_A(\beta_2 m_2)$, quitte à remplacer m_1, m_2 par $\beta_1 m_1$, $\beta_2 m_2$ on peut donc supposer que $a_1 \wedge a_2 = 1$. Posons $m_3 := m_1 + m_2$ et vérifions que m_3

convient. On a clairement $Ann_A(m_1) \cap Ann_A(m_2) \subset Ann_A(m_3)$. Pour l'inclusion réciproque, soit $a \in Ann_A(m_3)$. On a $am_1 = -am_2$. Par Bézout, il existe $u, v \in A$ tels que $ua_1 + va_2 = 1$. On a donc

$$am_1 = (ua_1 + va_2)am_1 = au\underbrace{a_1m_1}_{=0} + va_2am_1 = -av\underbrace{a_2m_2}_{=0} = 0.$$

Donc $a \in Ann_A(m_1)$. De même, $a \in Ann_A(m_2)$. □

Preuve du Lemme 11.3.1.2. Introduisons l'ensemble $\mathcal{E}$ des couples (u, N) où $m \in N \subset M$ est un sous-B-module et $u : N \to B$ un morphisme de B-modules tel que $u(m) = 1$. On munit $\mathcal{E}$ de la relation d'ordre $\leq$ définie par $(u_1, N_1) \leq (u_2, N_2)$ si $N_1 \subset N_2$ et $u_2|_{N_1} = u_1$. $\mathcal{E}$ est non-vide: par définition $B = A/Ann_A(m)$ donc on a un isomorphisme $v = - \cdot m : B \tilde{\to} Bm$ et $(Am, v^{-1}) \in \mathcal{E}$. Comme M est noetherien, $\mathcal{E}$ admet un élément maximal (u, N). Montrons que $N = M$. Sinon, soit $\mu \in M \setminus N$ et montrons qu'on peut étendre $u : N \to B$ en $u_1 : N + B\mu \to B$. Pour cela, il faut 'deviner' la bonne valeur de $u_1(\mu)$. Introduisons l'idéal

$$\mathfrak{i} := \{b \in B \mid b\mu \in N\} \subset B.$$

Ecrivons $Ann_A(M) = Aa$. Comme B est quotient de l'anneau principal A, $\mathfrak{i} = Ab/Aa$ avec $Aa \subset Ab$ *i.e.* $a = \alpha b$ pour un certain $\alpha \in A$. Notons $u(b\mu) = \overline{c}$ (on note $\overline{-}$ les classes modulo Aa). On a $u(a\mu) = 0 = \alpha\overline{c}$ donc $\alpha c = qa = q\alpha b$ dans A. Mais comme A est intègre $c = qb$. On a donc envie de poser $u_1(\mu) = \overline{q}$. Définissons $u_0 : N \oplus B \to B$ par $u_0(n \oplus \lambda) = u(n) + \lambda\overline{q}$. On a

$$\ker(N \oplus B \twoheadrightarrow N + B\mu, n \oplus \lambda \to n + \lambda\mu) = \{\beta b\mu \oplus -\beta b \mid \beta \in B\} \subset \ker(u_0)$$

En effet, $u_0(\beta b\mu \oplus -\beta b) = u(\beta b\mu) - \beta b\overline{q} = \beta u(b\mu) - \beta b\overline{q} = \beta\overline{c} - \beta b\overline{q} = 0$. Donc $u_0 : N \oplus B \to B$ passe au quotient en $u_1 : N + B\mu \to B$ avec $u_1|_N = u$. Cela contredit la maximalité de (u, N). □

11.3.2. Corollaire. *Soit M un A-module de type fini de torsion. Il existe une unique suite décroissante d'idéaux*

$$A \supsetneq I_1 \supset I_2 \supset \cdots \supset I_r \supsetneq 0$$

telle que

$$M \simeq A/I_1 \oplus \cdots \oplus A/I_r.$$

Proof. Comme M est artinien et noetherien, d'après le Théorème de Krull-Schmidt 10.3.1, M se décompose de façon unique comme somme directe de modules indécomposables. D'après le Théorème 11.3.1, cette décomposition s'écrit

$$M \simeq \bigoplus_{\mathfrak{p}} \bigoplus_{n \geq 0} A/\mathfrak{p}^{\alpha_{M,\mathfrak{p}}(n)},$$

où la première somme est indexée par l'ensemble $\mathrm{spec}(A)$ des idéaux premiers non nuls de A et

$$\alpha_{M,-} : \mathrm{spec}(A) \to \mathbb{Z}_{\geq 0}^{(\mathbb{Z}_{\geq 0})}$$

est une application à support fini telle que $\alpha_{M,\mathfrak{p}} = (\alpha_{M,\mathfrak{p}}(n))_{n \geq 0}$ est une suite décroissante dont les termes sont nuls pour $n \gg 0$. Pour chaque $\mathfrak{p} \in \mathrm{spec}(A)$ choisissons un générateur p de $\mathfrak{p}$ comme A-module. Soit $n \geq 0$ le plus grand des entiers tels qu'il existe $\mathfrak{p} \in \mathrm{spec}(A)$ pour lequel $\alpha_{M,\mathfrak{p}}(n) \neq 0$ et posons

$$a_{n+1-j} := \prod_{\mathfrak{p}} p^{\alpha_{M,\mathfrak{p}}(j)},\ j = 1, \ldots, n.$$

La suite d'idéaux $I_i := Aa_j$, $j = 1, \ldots, n$ vérifie alors la propriété de l'énoncé. Leur unicité résulte de l'unicité dans le théorème de Krull-Schmidt. □

On dit que la suite $A \supsetneq I_1 \supset I_2 \supset \cdots \supset I_r \supsetneq 0$ est la *suite des invariants* du A-module M.

11.4. Applications.

11.4.1. *Classification des groupes abéliens de type fini.* On peut appliquer la classification des A-modules de type fini sur un anneau principal à l'anneau $\mathbb{Z}$ pour obtenir le classique théorème de classification des groupes finis.

11.4.1.1. Corollaire. *Soit M un groupe abélien de type fini. Il existe un unique $r \in \mathbb{Z}_{\geq 0}$ et une unique suite d'entiers positifs $d_1|d_2|\ldots|d_s$ tels que*

$$M \simeq \mathbb{Z}^r \oplus (\oplus_{1\leq i\leq s}\mathbb{Z}/d_i).$$

11.4.1.2. Exercice. Donner la liste des groupes abéliens d'ordre 6, 18, 24 et 36.

11.4.2. Algèbre linéaire On peut également appliquer la classification à l'anneau $k[T]$ des polynômes à une indéterminée sur le corps k pour obtenir la classification des classes de conjugaison des endomorphisme d'un k-espace vectoriel de dimension finie par les invariants de similitude. Plus précisément, si V est un k-espace vectoriel de dimension finie tout endomorphisme $u : V \to V$ définit une structure de $k[T]$ module V_u sur V par $P(T)v = P(u)(v)$, $P \in k[T]$, $v \in V$. Le $k[T]$-module V_u est évidemment de type fini et de torsion. Il existe donc une unique suite de polynômes $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ telle que

$$V_u \simeq k[T]/P_{u,1} \oplus \cdots \oplus k[T]/P_{u,r_u}.$$

On dit que la suite $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ est la suite des *invariants de similitude* de l'endomorphisme u.

11.4.2.1. Exercice. (Classification des classes de conjugaison par les invariants de similitude)

(1) Soit $u, u' : V \to V$ deux endomorphismes. Montrer qu'il existe $\phi \in \mathrm{Aut}_k(V)$ tel que $u = \phi \circ u' \circ \phi^{-1}$ si et seulement si u et u' ont mêmes invariants de similitude.
(2) Calculer le polynôme minimal et le polynôme caractéristique de u en fonction de sa suite d'invariants de similitude. Montrer plus précisément qu'il existe une base du k-espace vectoriel V dans laquelle u a pour matrice la matrice diagonale par blocs dont les blocs diagonaux sont les matrices compagnons des $P_{u,i}$.
(3) Calculer le nombre de classes de conjugaison (sous $\mathrm{GL}_n(\mathbb{F}_q)$) dans $M_n(\mathbb{F}_q)$, dans $\mathrm{GL}_n(\mathbb{F}_q)$.

Au lieu d'appliquer le Corollaire 11.3.2 sous la forme énoncée, on peut l'appliquer avec la décomposition donnée par Krull-Schmidt (*cf.* preuve) *i.e.* il existe une unique famille de polynômes irréductibles $P_1, \ldots, P_s$ et des familles d'entiers $n_{i,1} \geq \cdots \geq n_{i,r_i} > 0$, $i = 1, \ldots, s$ tels que

$$V_u \simeq \bigoplus_{1\leq i\leq s} \bigoplus_{1\leq j\leq r_i} k[T]/P_i^{n_j}.$$

On retrouve alors la décomposition de Jordan en concaténant les bases $X^k P_i^l$, $0 \leq k \leq d_i - 1$, $0 \leq l \leq n_i - 1$ de $k[T]/P_i^{n_j}$, $i = 1, \ldots, s$. Dans cette base, la matrice de u est diagonale par blocs avec s blocs $D_1, \ldots, D_s$ et chaque bloc D_i est lui-même diagonale par bloc avec r_i blocs $D_{i,j}$, $j = 1, \ldots, r_j$ et chaque bloc $D_{i,j}$ de la forme

$$\begin{pmatrix} C(P_i) & 0 & \cdots & 0 & 0 \\ U & C(P_i) & & 0 & 0 \\ 0 & & \cdots & & \\ 0 & & & U & C(P_i) \end{pmatrix},$$

où U est ma matrice carrée de taille $d_i \times d_i$ avec $u_{1,d_i} = 1$ et $u_{i,j} = 0$ sinon et où on a n_j blocs $C(P_i)$.

11.4.3. Base adaptée La forme suivante du théorème de structure est aussi très utile en pratique.

11.4.3.1. Théorème. (Base adaptée) *Soit A un anneau principal, M un A-module libre de rang r et $N \subset M$ un sous-A-module. Il existe un unique entier $0 \leq s \leq r$, une unique suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ d'idéaux de A et $m_1, \ldots, m_r \in M$ tels que*

$$N = \bigoplus_{1 \leq i \leq s} Ad_i m_i \subset \bigoplus_{1 \leq i \leq r} Am_i = M.$$

Proof. L'unicité de s et de la suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ résulte du Corollaire 11.3.2 car $r - s$ est le rang de la partie libre de M/N et $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ est la suite des invariants de la partie de torsion de M/N. L'existence est un peu plus délicate. On procède par reccurence sur r. Si $r = 1$, c'est la traduction du fait que A est principal. Si $r \geq 1$, l'idée est de construire d_1, m_1 à partir de l'inclusion $N \hookrightarrow M$. Pour cela, on introduit l'ensemble $\mathcal{E}$ des idéaux de la forme $f(N) \subset A$, où $f : M \to A$ est un morphisme de A-module. Comme A est noetherien, $\mathcal{E}$ contient au moins un élément maximal $f(N) = Ad = Af(n)$.

(1) En fait, pour tout $g : M \to A$ on a $g(n) \in f(N) = Ad$. En effet, si δ est le pgcd de d et $g(n)$ il existe $u, v \in A$ tels que $ud + vg(n) = \delta$. Donc

$$f(N) = Ad \subset A\delta = A(uf + vg)(n) \subset (uf + vg)(N)$$

Par maximalité de $f(N)$, cela implique $f(N) = Ad = A\delta = (uf + vg)(N)$. En particulier, $d = \delta$ divise $g(n)$ comme annoncé.

(2) Il existe $\mu \in M$ tel que $d\mu = n$. Choisissons une A-base quelconque $m_1, \ldots, m_r$ de M et notons $p_i : M \twoheadrightarrow Am_i \simeq A$ la projection correspondante sur la i-ème coordonnée. On a, dans cette base, $n = \sum_{a \leq i \leq r} a_i m_i$ et en appliquant (1) aux p_i, on obtient que d divise a_i, $i = 1, \ldots, r$. Donc en écrivant $a_i = db_i$ pour un certain $b_i \in A$, $i = a, \ldots, r$, on peut prendre $\mu = \sum_{1 \leq i \leq r} b_i m_i$.

(3) De $d\mu = n$, on déduit $f(d\mu) = df(\mu) = f(n) = d$ donc comme A est intègre, $f(\mu) = 1$. Cela donne une décomposition $M \simeq \ker(f) \oplus A\mu$ ($m = (m - f(m)\mu) + f(m)\mu$ telle que $N = \ker(f) \cap N \oplus Ad\mu$. On peut donc appliquer l'hypothèse de recurrence à $\ker(f) \cap N \subset \ker(f)$ puisqu'on sait que $\ker(f)$ est un A-module libre de rang r pour obtenir une suite $A \supsetneq Ad_2 \supset \cdots \supset Ad_s \supsetneq 0$ d'idéaux de A et $m_2, \ldots, m_r \in \ker(f)$ tels que

$$\ker(f) \cap N = \bigoplus_{2 \leq i \leq s} Ad_i m_i \subset \bigoplus_{2 \leq i \leq r} Am_i = \ker(f).$$

Il reste à voir que $Ad_1 \supset Ad_2$. Ecrivons $Ad_1 + Ad_2 = Ad$ et fixons $u_1, u_2 \in A$ tels que $u_1 a_1 + u_2 a_2 = d$. Avec $g := u_1 pr_1 + u_2 pr_2 : M \to A$ et $\nu := d_1 m_1 + d_2 m_2 \in N$ on a $g(\nu) = c$ donc $f(N) = Ad_1 \subset Ac = Ag(\nu) \subset g(N)$. Par maximalité de $f(N)$ dans $\mathcal{E}$ on en déduit $Ad_1 = Ac$ *i.e.* $Ad_1 \supset Ad_2$.

□

11.4.3.2. Corollaire. (Classes d'équivalence) *On considère l'action de* $\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ *sur* $M_{n,m}(A)$ *donnée par* $(P, Q) \cdot M = PMQ^{-1}$. *L'application*

$$\begin{array}{rcl} \{Ad_1 \supset \cdots \supset Ad_n\} & \to & M_{n,m}(A) \\ Ad_1 \supset \cdots \supset Ad_n & \mapsto & D(d_1, \ldots, d_n) \end{array}$$

(cf. preuve pour la notation $D(d_1, \ldots, d_n)$) induit une bijection

$$\{Ad_1 \supset \cdots \supset Ad_n\} \tilde{\to} M_{n,m}(A)/\mathrm{GL}_n(A) \times \mathrm{GL}_m(A).$$

Proof. On suppose $m \geq n$. Notons $M := A^m$, $N := A^n$ et soit $f : M \to N \in \mathrm{Hom}_A(M, N)$. Par le théorème de la base adaptée pour $f(M) \subset N$ il existe un unique $0 \leq r \leq n$, une unique suite d'idéaux $A \supsetneq Ad_1 \supset Ad_2 \supset \cdots \supset Ad_r$ et des éléments $\nu_1, \ldots, \nu_n \in N$ tels que

$$f(M) = \oplus_{1 \leq i \leq r} Ad_i\nu_i \subset \oplus_{1 \leq i \leq n} A\nu_i = N.$$

Comme $f(M)$ est un A-module libre, la suite exacte courte

$$0 \to \ker(f) \to M \xrightarrow{f} f(M) \to 0$$

est scindée. Notons $s : f(M) \to M$ un scindage. On a alors $M \simeq \ker(f) \oplus s(f(N))$. Comme A est principal et M est un A-module libre, $\ker(f) \subset M$ est encore un A-module libre. En concaténant une A-base de $\ker(f)$ et la A-base $s(\nu_1), \ldots, s(\nu_n)$ de $f(N)$, on obtient une A-base $\mu_1, \ldots, \mu_n$ de M. La matrice de f dans les bases $\mu_1, \ldots, \mu_m$ et $\nu_1, \ldots, \nu_n$ est de la forme

$$D(d_1, \ldots, d_n) := \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 \\ 0 & d_2 & & 0 & 0 \\ 0 & & \cdots & & \\ 0 & & & d_n & 0 \end{pmatrix}.$$

On a donc montré que si $f, g : M \to N$ sont des morphismes de A-modules tels que $N/f(M) \simeq N/g(M)$ alors f, g sont équivalents. La réciproque est presque immédiate car s'il existe des automorphismes $\phi \in Aut_A(M)$, $\psi \in Aut_A(N)$ tels que $f \circ \phi = \psi \circ g$ alors $\psi : N \tilde{\to} N$ se restreint en un isomorphisme de A-modules $\psi : g(M) \tilde{\to} f(\phi(M)) = f(M)$ donc induit un isomorphisme de A-modules $\overline{\psi} : N/g(M) \tilde{\to} N/f(M)$. □

Remarque. Dans le cas où $A = k$ est un corps commutatif, on retrouve le théorème de classification des classes d'équivalence par le rang de la matrice.

12. Produit tensoriel

12.1. Définition. Soit $M_1, \ldots, M_r$ et M des A-modules. Notons

$$L_{r,A}(M_1 \times \cdots \times M_r, M)$$

l'ensemble des applications $f : M_1 \times \cdots \times M_r \to M$ qui sont r-A-linéaires *i.e.* telles que $f \circ \iota_i : M_i \to M$ est un morphisme de A-modules (où l'on a noté $\iota_i : M_i \hookrightarrow M_1 \oplus \cdots \oplus M_r \tilde{\to} M_1 \times \cdots \times M_r$ l'injection canonique), $i = 1, \ldots, r$.

12.1.1. Lemme. (Propriété universelle du produit tensoriel) *Pour toute famille $M_1, \ldots, M_r$ de A-modules, il existe un A-module T et une application r-A-linéaire $p : M_1 \times \cdots \times M_r \to T$, uniques à unique isomorphisme près et tels que pour tout A-module M et pour toute application r-A-linéaire $f : M_1 \times \cdots \times M_r \to M$ il existe un unique morphisme de A-modules $\widetilde{f} : T \to M$ tel que $\widetilde{f} \circ p = f$.*

Proof. Comme d'habitude, l'unicité à unique isomorphisme près résulte tautologiquement de l'unicité de $\widetilde{f} : T \to M$ dans la propriété universelle. Pour l'existence de $p : M_1 \times \cdots \times M_r \to T$,

- Construction: Notons $\Sigma := A^{(M_1 \times \cdots \times M_r)}$ le A-module libre engendré par $M_1 \times \cdots \times M_r$, $e_{\underline{m}} \in \Sigma$ l'élément correspondant au terme avec des 0 partout sauf en l'indice $\underline{m} := (m_1, \ldots, m_r)$ et $R \subset \Sigma$ le sous A-module engendré par les éléments de la forme

$$e_{(m_1, \ldots, a_i m_i + a_i' m_i', \ldots, m_r)} - a_i e_{(m_1, \ldots, m_i, \ldots, m_r)} - a_i' e_{(m_1, \ldots, m_i', \ldots, m_r)}.$$

  En posant $M_1 \otimes_A \cdots \otimes_A M_r := \Sigma/R$ et

$$\begin{array}{rccccc} p : & M_1 \times \cdots \times M_r & \to & A^{(M_1 \times \cdots \times M_r)} & \to & M_1 \otimes_A \cdots \otimes_A M_r \\ & \underline{m} & \to & e_{\underline{m}} & \to & e_{\underline{m}} \mathrm{mod} R =: m_1 \otimes \cdots \otimes m_r \end{array}$$

  on vérifie facilement que $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ est une application A-r-linéaire.

- Vérification de la propriété universelle: Soit M un A-module et $f : M_1 \times \cdots \times M_r \to M$ une application r-A-linéaire. Si $\widetilde{f} : M_1 \otimes \cdots \otimes M_r \to M$ existe, la condition $p \circ \widetilde{f} = f$ impose $\widetilde{f}(m_1 \otimes \cdots \otimes m_r) = f(m_1, \ldots, m_r)$. Comme $M_1 \otimes_A \cdots \otimes_A M_r$ est engendré, comme A-module, par les éléments de la forme $m_1 \otimes \cdots \otimes m_r$, cela montre l'unicité de $\widetilde{f}$ sous réserve de son existence. Par propriété universelle des $\iota_{\underline{m}} : A \hookrightarrow A^{(M_1 \times \cdots \times M_r)}$, $\underline{m} = (m_1, \ldots, m_r) \in M_1 \times \cdots \times M_r$, il existe un unique morphisme de A-modules $F : \Sigma = A^{(M_1 \times \cdots \times M_r)} \to M$ tel que $F \circ \iota_{\underline{m}} : A \to M$ est le morphisme qui envoie 1 sur $f(m_1, \ldots, m_r)$. Comme $f : M_1 \times \cdots \times M_r \to M$ est r-A-linéaire, $R \subset \ker(F)$ donc $F : \Sigma \to M$ se factorise en un morphisme de A-modules $\widetilde{f} : M_1 \otimes_A \cdots \otimes_A M_r \to M$ tel que $p \circ \widetilde{f} = F$; en particulier

$$p \circ \widetilde{f}(m_1 \otimes \cdots \otimes m_r) = F(m_1, \ldots, m_r) = f(m_1, \ldots, m_r),\ (m_1, \ldots, m_r) \in M_1 \times \cdots \times M_r.$$

□

Rem. On prendra garde que $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ n'est pas surjective en général mais que, $M_1 \otimes_A \cdots \otimes_A M_r$ est engendré comme A-module par les éléments de la forme $m_1 \otimes \cdots \otimes m_r$.

On peut aussi réécrire 12.1.1 en disant que pour tout A-module M l'application canonique

$$\mathrm{Hom}_A(M_1 \otimes_A \cdots \otimes_A M_r, M) \to L_{r,A}(M_1 \times \cdots \times M_r, M),\ f \to f \circ p$$

est bijective ou encore, plus visuellement,

$$\begin{array}{ccc} M_1 \times \cdots \times M_r & \xrightarrow{\forall f} & M \\ {\scriptstyle p}\downarrow & \nearrow_{\exists ! \widetilde{f}} & \\ M_1 \otimes_A \cdots \otimes_A M_r & & \end{array}$$

12.1.2. Si $f_i : M_i \to N_i$, $i = 1, \ldots, r$ sont r morphismes de A-modules, l'application

$$\begin{array}{cccc} (f_1, \ldots, f_r) & M_1 \times \cdots \times M_r & \to & N_1 \otimes_A \cdots \otimes_A N_r \\ & (m_1, \ldots, m_r) & \to & f_1(m_1) \otimes \cdots \otimes f_r(m_r) \end{array}$$

est r-A-linéaire donc se factorise en un morphisme de A-modules $f_1 \otimes_A \cdots \otimes_A f_r : M_1 \otimes_A \cdots \otimes_A M_r \to N_1 \otimes_A \cdots \otimes_A N_r$ tel que $f_1 \otimes_A \cdots \otimes_A f_r(m_1 \otimes \ldots m_r) = (f_1, \ldots, f_r)(m_1, \ldots, m_r) = f_1(m_1) \otimes \cdots \otimes f_r(m_r)$.

12.2. Propriétés élémentaires.

12.2.1. Lemme. (Le produit tensoriel 'commute' aux sommes directes) *Soit M_i, $i \in I$ et M des A-modules. On a un isomorphisme canonique*

$$\begin{array}{ccc} M \otimes_A (\bigoplus_{i \in I} M_i) & \tilde{\to} & \bigoplus_{i \in I} (M \otimes_A M_i) \\ m \otimes (m_i)_{i \in I} & \to & (m \otimes m_i)_{i \in I} \end{array}$$

Proof. Vérifions d'abord que $\phi : M \otimes_A (\bigoplus_{i \in I} M_i) \to \bigoplus_{i \in I} (M \otimes_A M_i)$ est bien défini. L'application $\Phi : M \times \bigoplus_{i \in I} M_i \to \bigoplus_{i \in I} (M \otimes_A M_i)$, $(m, (m_i)_{i \in I}) \to (m \otimes m_i)_{i \in I}$ est 2-A-linéaire donc par propriété universelle de $p : M \times (\bigoplus_{i \in I} M_i) \to M \otimes_A (\bigoplus_{i \in I} M_i)$ se factorise effectivement en un morphisme de A-modules $\phi : M \otimes_A (\bigoplus_{i \in I} M_i) \to \bigoplus_{i \in I} (M \otimes_A M_i)$ tel que $p \circ \phi = \Phi$. Inversement, pour tout $i \in I$ l'application $\Psi_i : M \times M_i \to M \otimes_A (\bigoplus_{i \in I} M_i)$, $(m, m_i) \to m \otimes \iota_i(m_i)$ est 2-A-linéaire donc par propriété universelle de $p : M \times M_i \to M \otimes_A M_i$ se factorise en un morphisme de A-modules $\psi_i : M \otimes_A M_i \to M \otimes_A (\bigoplus_{i \in I} M_i)$ tel que $p \circ \psi_i = \Psi_i$. Puis, par propriété universelle de $\iota_i : M \otimes_A M_i \to \bigoplus_{i \in I} (M \otimes_A M_i)$, $i \in I$ on obtient un unique morphisme de A-module $\psi : \bigoplus_{i \in I} (M \otimes_A M_i) \to M \otimes_A (\bigoplus_{i \in I} M_i)$ tel que $\psi \circ \iota_i = \Psi_i$, $i \in I$. On vérifie sur les constructions que ϕ, ψ sont inverses l'un de l'autre. □

Les preuves des lemmes suivant sont du même acabit *i.e.* purement formelles et laissées en exercice au lecteur.

12.2.2. Lemme. (Commutativité et associativité) *Soit L, M, N des A-modules. On a des isomorphismes (de A-modules) canoniques*

$$\begin{array}{ccccc} L \otimes_A (M \otimes_A N) & \tilde{\to} & (L \otimes_A M) \otimes_A N & \tilde{\to} & L \otimes_A M \otimes_A N \\ l \otimes (m \otimes n) & \to & (l \otimes m) \otimes n & \to & l \otimes m \otimes n \end{array}$$

$$\begin{array}{ccc} M \otimes_A N & \tilde{\to} & N \otimes_A M \\ m \otimes n & \to & n \otimes m \end{array}$$

12.2.3. Lemme. *Soit M un A-module. On a un isomorphisme canonique*

$$\begin{array}{ccc} A \otimes_A M & \tilde{\to} & M \\ a \otimes m & \to & am \end{array}$$

12.2.4. Soit I un ensemble. Pour $i \in I$ on rappelle qu'on note $e_i := (\delta_{i,j})_{j \in I} \in A^{(I)}$ le i-ème élément de la base canonique de $A^{(I)}$.

Lemme. *Soit $I_1, \ldots, I_r$ des ensembles. On a un isomorphisme de A-modules canonique*

$$A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_r)} \tilde{\to} A^{(I_1 \times \cdots \times I_r)}$$

qui envoie $e_{i_1} \otimes \cdots \otimes e_{i_r}$ sur $e_{(i_1,\ldots,i_r)}$, $(i_1, \ldots, i_r) \in I_1 \times \cdots \times I_r$. *Preuve.* Cela se déduit formellement, par induction sur r, des Lemmes 12.2.1, 12.2.2, 12.2.3:

$$\begin{aligned} A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_r)} &\tilde{\to} (A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_{r-1})}) \otimes_A A^{(I_r)} \\ &\tilde{\to} A^{(I_1 \times \cdots \times I_{r-1})} \otimes_A A^{(I_r)} \\ &\tilde{\to} \oplus_{i_r \in I_r} (A^{(I_1 \times \cdots \times I_{r-1})} \otimes_A A) \\ &\tilde{\to} \oplus_{i_r \in I_r} A^{(I_1 \times \cdots \times I_{r-1})} \\ &\tilde{\to} \oplus_{i_r \in I_r} \oplus_{(i_1,\ldots,i_{r-1}) \in I_1 \times \cdots \times I_{r-1}} A \tilde{\to} A^{(I_1 \times \cdots \times I_r)}. \ \square \end{aligned}$$

En particulier, si M_i est un A-module libre de rang fini d_i, $i = 1, \ldots, r$, $M_1 \otimes_A \cdots \otimes_A M_r$ est un A-module libre de rang $d_1 \ldots d_r$.

12.2.5. Lemme. *Soit M, N des A-modules. On a des morphismes de A-modules canoniques*

$$\begin{array}{ccccc} M^\vee \otimes_A N & \to & \mathrm{Hom}_A(M, N)\ , & M^\vee \otimes_A N^\vee & \to & (M \otimes_A N)^\vee \\ f \otimes n & \to & f(-)n; & f \otimes g & \to & m \otimes n \to f(m)g(n). \end{array}$$

et

$$\begin{array}{ccc} \mathrm{End}_A(M) \otimes_A \mathrm{End}_A(N) & \to & \mathrm{End}_A(M \otimes_A N) \\ f \otimes g & \to & m \otimes n \to f(m) \otimes g(n); \end{array}$$

Si de plus M et N sont libres de rang fini, ces trois morphismes sont des isomorphismes.

Proof. Les morphismes se construisent en utilisant la propriété universelle du produit tensoriel. En général, il n'y a par contre pas de façon canonique de construire des inverses de ces morphismes[6]. Mais si M et N sont libres de rang fini, on peut vérifier que ces trois morphismes envoient à chaque fois une base sur une base. $\square$

12.3. Adjonctions.

[6]Et d'ailleurs, ce ne sont pas toujours des isomorphismes, comme on le voit par exemple en considérant les $\mathbb{Z}$-modules $M = N = \mathbb{Z}/n$ puisque $(\mathbb{Z}/n)^\vee = 0$ donc $(\mathbb{Z}/n)^\vee \otimes \mathbb{Z}/n = 0$ alors que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/n) = \mathbb{Z}/n \neq 0$.

12.3.1. $- \otimes_A M$ **versus** $\mathrm{Hom}_A(M, -)$

Lemme. (Adjonction-1) *Soit L, M, N des A-modules. On a des isomorphismes (de A-modules) canoniques*

$$\begin{array}{ccccc} \mathrm{Hom}_A(L, \mathrm{Hom}_A(M,N)) & \tilde{\to} & L_{r,A}(L \times M, N) & \tilde{\to} & \mathrm{Hom}_A(L \otimes_A M, N) \\ f & \to & (l,m) \to f(l)(m) & & \\ l \to \beta(l,-) & \leftarrow & \beta & & \end{array}$$

(Le deuxième isomorphisme est simplement la propriété universelle du produit tensoriel).

Exercice Soit M un A-module. Montrer que pour toute suite exacte courte de A-modules

$$0 \to N' \overset{u}{\to} N \overset{v}{\to} N'' \to 0$$

(1) La suite

$$0 \to \mathrm{Hom}_A(M, N') \overset{u\circ}{\to} \mathrm{Hom}_A(M, N) \overset{v\circ}{\to} \mathrm{Hom}_A(M, N'')$$

est exacte. (On dit que $Hom_A(M, -)$ est un foncteur exact à gauche).

(2) La suite

$$M \otimes_A N' \overset{Id\otimes u}{\to} M \otimes_A N \overset{Id\otimes v}{\to} M \otimes_A N'' \to 0$$

est exacte. (On dit que $M \otimes_A -$ est un foncteur exact à droite).

On renvoie au TD 5 pour la correction.

12.3.2. Extension/Restriction des scalaires. Soit $\phi : A \to B$ une A-algèbre. A tout B-module M on peut associer un A-module noté $M|_A$ (ou $\phi_* M$) dont le groupe abélien sous-jacent est encore M et dont la structure de A-module est définie par $a \cdot m = \phi(a)m$, $a \in A$, $m \in M$. Tout morphisme de B-modules $f : M \to N$ induit alors tautologiquement un morphisme de A-modules $\phi_*(f) = f|_A : M|_A \to N|_A$. On notera aussi que $\phi_*(Id) = Id$ et que si $M' \overset{f}{\to} M \overset{g}{\to} M''$ est une suite de morphismes de B-modules, $\phi_*(g \circ f) = \phi_*(g) \circ \phi_*(f)$.

On voudrait, inversement, associer à tout A-module M un B-module $\phi^* M$ et à tout morphisme de A-modules $f : M \to N$ un morphisme de B-modules $\phi^* f : \phi^* M \to \phi^* N$.

Soit M un B-module et N un A-module. Pour tout $b_0 \in B$, l'application

$$\begin{array}{ccc} M \times N & \to & M \otimes_A N (:= (M|_A) \otimes_A N) \\ (m,n) & \to & (b_0 m) \otimes n \end{array}$$

est 2-A-linéaire donc se factorise en un morphisme de A-module $b_0 \cdot : M \otimes_A N \to M \otimes_A N$, $m \otimes n \to b_0 \cdot (m \otimes n) := (b_0 m) \otimes n$. On vérifie que cela définit une structure de B-module sur $M \otimes_A N$. Tout morphisme de A-modules $f : N \to N'$ induit alors un morphisme de B-modules $Id_M \otimes f : M \otimes_A N \to M \otimes_A N'$. Si $M = B$, on note parfois $\phi^* N := B \otimes_A N$ et $\phi^* f := Id_B \otimes f : \phi^* N \to \phi^* N'$. Là aussi on notera que $\phi^*(Id) = Id$ et que si $M' \overset{f}{\to} M \overset{g}{\to} M''$ est une suite de morphismes de A-modules, $\phi^*(g \circ f) = \phi^*(g) \circ \phi^*(f)$.

Les constructions ϕ_*, ϕ^* sont liées par le lemme suivant.

12.3.2.1. Lemme. (Adjonction-2) *Soit M un A-module et N un B-module. On a un isomorphisme canonique (de $\mathbb{Z}$-modules)*

$$\begin{array}{ccc} \mathrm{Hom}_A(M, N|_A) & \tilde{\to} & \mathrm{Hom}_B(B \otimes_A M, N) \\ f & \to & b \otimes m \to bf(m) \\ f(1 \otimes -) & \leftarrow & f \end{array}$$

12.3.2.2. Exercice (Transitivité de l'extension des scalaires).

(1) Soit M, M' des B-modules et N un A-module. Montrer qu'on a un isomorphisme canonique de B-modules
$$M' \otimes_B (M \otimes_A N) \tilde{\to} (M' \otimes_B M) \otimes_A N.$$
En déduire qu'on a un isomorphisme canonique de B-modules $M \otimes_B (B \otimes_A N) \tilde{\to} M \otimes_A N$;

(2) Soit $A \to B \to C$ des morphismes d'anneaux et M un A-module. Montrer qu'on a un isomorphisme canonique
$$C \otimes_B (B \otimes_A M) \tilde{\to} C \otimes_A N.$$

On va maintenant étudier l'extension des scalaires dans les deux cas particuliers suivants:

- Par un quotient $A \to A/I$;
- Par une localisation $A \to S^{-1}A$.

12.3.2.3. Extension des scalaires par un quotient. Soit M un A-module et $I \subset A$ un idéal. Notons $IM \subset M$ le sous-A-module engendré par les éléments de la forme am, $a \in I$, $m \in M$. Par propriété universelle du quotient, l'application

$$\begin{array}{ccc} A \times M/IM & \to & M/IM \\ (a, \overline{m}) & \to & a\overline{m} = \overline{am} \end{array}$$

donnée par la structure de A-module sur M/IM se factorise en une application $A/I \times M/IM \to M/IM$, qui fait de M/IM un A/I-module.

Lemme. (Propriété universelle de $M \to M/IM$) *Pour tout A-module M et idéal $I \subset A$, il existe un A/I-module Q et un morphisme de A-modules $p : M \to (p_I)_*Q$ tel que pour tout A/I-module N et tout morphisme de A-module $\phi : M \to (p_I)_*N$ il existe un unique morphisme de A/I-module $\overline{\phi} : Q \to N$ tel que $\overline{\phi} \circ p = \phi$.*

Proof. On vérifie que $p_{IM} : M \to M/IM$ convient. Si $\overline{\phi} : M/IM \to N$ existe la condition $\overline{\phi} \circ p_{IM} = \phi$ impose $\overline{\phi}(\overline{m}) = \phi(m)$, $m \in M$, d'où l'unicité de $\overline{\phi}$ sous réserve de son existence. Par ailleurs, pour tout $a \in I$, $m \in M$, $\phi(am) = p_I(a)\phi(m) = 0$ donc $IM \subset \ker(\phi)$ et $\phi : M \to N$ se factorise en un morphisme de A-modules $\overline{\phi} : M/IM \to (p_I)_*M$ qui induit tautologiquement un morphisme $\overline{\phi} : M/IM \to N$ de A/I-modules. □

On peut réécrire le Lemme en disant que pour tout A/I-module N l'application canonique

$$\mathrm{Hom}_{A/I}(M/IM, N) \to \mathrm{Hom}_A(M, N),\ \phi \to (\phi \circ p_{IM})$$

est bijective. Or 12.3.2.1 dit que le morphisme de A-module $p : M \to A/I \otimes_A M$, $m \to \overline{1} \otimes m$ vérifie la même propriété. Par unicité des objets universels, on a donc un unique morphisme de A/I-modules $\phi : A/I \otimes M \to M/IM$ tel que $\phi \circ p = p_{IM}$. On peut aussi démontrer cela 'à la main', comme suit.

L'application canonique

$$\begin{array}{ccc} A \times M & \to & M/IM \\ (a, m) & \to & \overline{am} \end{array}$$

est 2-A-linéaire et passe au quotient en une application 2-A-linéaire $A/I \times M \to M/IM$ donc se factorise en un morphisme de A-modules $f : (A/I) \otimes_A M \to M/IM$. Inversement, l'application $M \to (A/I) \otimes_A M$, $m \to 1 \otimes m$ est un morphisme de A-modules dont le noyau contient IM donc se factorise en un morphisme de A-modules $M/IM \to (A/I) \otimes_A M$. Par construction, f et g sont inverses l'une de l'autre. On a donc montré qu'on avait un isomophisme de A-modules canoniques

$$(A/I) \otimes_A M \tilde{\to} M/IM.$$

Exemple. Soit A un anneau principal, $a, b \in A$ des éléments premiers entre eux et M un A-module tel que $aM = 0$. Par Bézout on a alors $bM = M$ donc $(A/b) \otimes_A M = 0$. Par exemple si $p \neq q$ sont deux nombres premiers, $\mathbb{Z}/p \otimes_{\mathbb{Z}} \mathbb{Z}/q = 0$.

12.3.2.4. Extension des scalaires par une localisation. Soit $S \subset A$ une partie multiplicative et M un A-module. Munissons le produit cartésien $S \times M$ de la relation $\sim$ définie par $(s, m) \sim (s', m')$ s'il existe $s'' \in S$ tel que $s''(s'm - sm') = 0$.

On vérifie que $\sim$ est une relation d'équivalence. On remarquera que si M est sans S-torsion, on peut, dans la définition de $\sim$, simplifier par s'' et la relation $\sim$ devient simplement $(s, m), (s', m') \in S \times M$, $(s, m) \sim (s', m')$ si $s'm - sm' = 0$. Mais on prendra garde que si M a de la S-torsion, la relation $(s, m) \sim (s', m')$ si $s'm - sm' = 0$ n'est pas transitive donc ne définit pas une relation d'équivalence.

On note $S^{-1}M := S \times M/\sim$ et

$$\begin{array}{rccc} -/- : & S \times M & \to & S^{-1}M \\ & (s, m) & \to & m/s \end{array}$$

la projection canonique.

On vérifie que les applications

$$\begin{array}{rccc} + \ : S^{-1}M \times S^{-1}M & \to & S^{-1}M \\ (m/s, n/t) & \to & (tm + sn)/(st) \end{array} \quad , \quad \begin{array}{rccc} \cdot \ : S^{-1}A \times S^{-1}M & \to & S^{-1}A \\ (a/s, n/t) & \to & (an)/(st) \end{array}$$

munissent $S^{-1}M$ d'une structure de $S^{-1}A$-module et que l'application canonique $\iota_S := -/1 : M \to (\iota_S)_* S^{-1}M$ est un morphisme de A-modules de noyau $\ker(\iota_S) = \{m \in M \mid \exists s \in S \text{ tel que } sm = 0\}$.

Lemme. (Propriété universelle de la localisation des A-modules) *Pour toute partie multiplicative $S \subset A \setminus \{0\}$ et pour tout A-module M il existe un $S^{-1}A$-module L et un morphisme de A-modules $\iota_S : M \to (\iota_S)_* L$ tel que pour tout $S^{-1}A$-module N et pour tout morphisme de A-modules $f : M \to (\iota_S)_* N$, il existe un unique morphisme de $S^{-1}A$-modules $\tilde{f} : L \to N$ tel que $f = \tilde{f} \circ \iota_S$.*

Proof. On vérifie que $\iota_S := -/1 : M \to (\iota_S)_* S^{-1}M$ convient... □

En particulier, pour tout morphisme de A-modules $f : M \to N$, en appliquant la propriété universelle de $\iota_S : M \to S^{-1}M$ au morphisme de A-modules $M \xrightarrow{f} N \xrightarrow{\iota_S} S^{-1}N$ on obtient un morphisme de $S^{-1}A$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ donné explicitement par $f(m/s) = f(m)/s$, $s \in S$, $m \in M$.

On peut réécrire le Lemme en disant que pour tout $S^{-1}A$-module N l'application canonique

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, N) \to \mathrm{Hom}_A(M, (\iota_S)_* N), \ \phi \to (\phi \circ \iota_S)$$

est bijective. Or 12.3.2.1 dit que le morphisme de A-modules $\iota : M \to (\iota_S)_*(S^{-1}A \otimes_A M)$, $m \to 1/1 \otimes m$ vérifie la même propriété. Par unicité des objets universels, on a donc un unique morphisme de $S^{-1}A$-modules $\phi : S^{-1}A \otimes M \to S^{-1}M$ tel que $\phi \circ \iota = \iota_S$. Là encore, on peut aussi démontrer

cela 'à la main'.

L'application canonique

$$\begin{array}{lll} S^{-1}A \times M & \to & S^{-1}M \\ (a/s, m) & \to & (am)/s (= a(m/s) \end{array}$$

est bien définie et 2-A-linéaire donc se factorise en un morphisme de A-modules $f : S^{-1}A \otimes_A M \to S^{-1}M$ qui est, automatiquement, un morphisme de $S^{-1}A$-modules. Inversement, l'application $S \times M \to S^{-1}A \otimes_A M$, $(s, m) \to (1/s) \otimes m$ se factorise en un morphisme de $S^{-1}A$-modules $g : S^{-1}M \to S^{-1}A \otimes_A M$. Par construction, f et g sont inverses l'une de l'autre. On a donc montré qu'on avait un isomophisme de $S^{-1}A$-modules canonique

$$S^{-1}A \otimes_A M \tilde{\to} S^{-1}M.$$

Notations. Comme pour les anneaux, on note, pour $a \in A \setminus \sqrt{\{0\}}$, $M_a := S_a^{-1}M$, où $S_a = \{a^n \mid n \geq 0\}$ et pour $\mathfrak{p} \in spec(A)$, $M_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$. Avec ces notations, on a en particulier $A_a \otimes_A M \tilde{\to} M_a$, $A_{\mathfrak{p}} \otimes_A M \tilde{\to} M_{\mathfrak{p}}$.

Exemple. Si pour tout $m \in M$ il existe $s \in S$ tel que $sm = 0$, $S^{-1}M = 0$. Si pour tout $s \in S$ l'application $s\cdot - : M \to M$ de multiplication par s est bijective, $\iota_S : M \to S^{-1}M$ est un isomorphisme de A-modules. En particulier, si A est un anneau principal de corps des fractions K et M est un A-module de type fini, que l'on écrit sous la forme $M = A^r \oplus \oplus_{\mathfrak{p} \in \mathrm{spec}(A)} M(\mathfrak{p})$ (*cf.* notations de l'exercice 12.3.2.3).

- $K \otimes_A M = K^{\oplus r}$. En effet, $K = S^{-1}A$ avec $S := A \setminus \{0\}$ et pour tout $\mathfrak{p} = Ap \in \mathrm{spec}(A)$ il existe $n \geq 1$ tel que $p^n M(\mathfrak{p}) = 0$. Or $p^n \in S$ donc $S^{-1}M(\mathfrak{p}) = 0$ et

$$\begin{array}{ll} K \otimes_A M & \simeq S^{-1}A \otimes (A^r \oplus \oplus_{\mathfrak{p} \in \mathrm{spec}(A)} M(\mathfrak{p}) \\ & \simeq (S^{-1}A \otimes A)^r \oplus \oplus_{\mathfrak{p} \in \mathrm{spec}(A)} (S^{-1}A \otimes M(\mathfrak{p})) \\ & \simeq (S^{-1}A)^r \simeq K^r \end{array}$$

- et pour tout $\mathfrak{p} \in spec(A) \setminus \{0\}$, $A_{\mathfrak{p}} \otimes_A M = A_{\mathfrak{p}}^{\oplus r} \oplus M(\mathfrak{p})$. En effet, $A_{\mathfrak{p}} = S^{-1}A$ avec $S = A \setminus \mathfrak{p}$ hence for every $\mathfrak{q} = Aq \neq \mathfrak{p} \in \mathrm{spec}(A)$, il existe $n \geq 1$ tel que $q^n M(\mathfrak{q}) = 0$. Or $q^n \in S$ donc $S^{-1} \otimes M(\mathfrak{q}) = 0$. Par contre, par Bézout, tout $s \in S$ induit un isomorphisme $s \cdot - : M(\mathfrak{p}) \tilde{\to} M(\mathfrak{p})$ donc $S^{-1} \otimes M(\mathfrak{p}) \simeq M(\mathfrak{p})$. Et on conclut comme précedemment.

Par exemple $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = 0$, $\mathbb{Z}_{2\mathbb{Z}} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, $\mathbb{Z}_{3\mathbb{Z}} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = \mathbb{Z}/3 \times \mathbb{Z}/3$, $\mathbb{Z}_{p\mathbb{Z}} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = 0$ pour $p \neq 2, 3$.
L'exemple précédent montre que, si A est un anneau principal, on peut reconstruire un A-module de type fini M à partir de la donnée de ses localisés $M_{\mathfrak{p}}$ en $\mathfrak{p} \in spec(A)$ (on peut même, se restreindre aux $\mathfrak{p} \in spm(A) = spec(A) \setminus \{0\}$). C'est un cas particulier d'une "philosophie" générale s'appliquant à l'étude des propriétés dites locales. On dit qu'une propriété (P) d'un A-module M (resp. d'un morphisme de A-modules $\varphi : M \to N$) est locale si le A-module M (resp. le morphisme de A-modules $\varphi : M \to N$) a (P) si et seulement si le $A_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ (resp. le morphisme de $A_{\mathfrak{p}}$-modules $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$) a (P) pour tout $\mathfrak{p} \in spec(A)$. Par exemple, la propriété $M = 0$ et la propriété $\ker(\phi) = 0$ sont locales.

12.4. Produit tensoriel de A-algèbres. Soit $\phi : A \to B$ et $\psi : A \to C$ deux A-algèbres. Les applications produits $B \times B \to B$ et $C \times C \to C$ sont 2-A-bilinéaires donc se factorisent en des morphismes de A-modules $\mu_B : B \otimes_A B \to B$ et $\mu_C : C \otimes_A C \to C$. On en déduit une application

$$(B \otimes_A C) \otimes_A (B \otimes_A C) \tilde{\to} (B \otimes_A B) \otimes_A (C \otimes_A C) \overset{\mu_B \otimes \mu_C}{\to} B \otimes_A C$$

dont on vérifie qu'elle munit le A-module $B \otimes_A C$ d'une structure de A-algèbre telle que les applications $\iota_B : B \to B \otimes_A C$, $b \to b \otimes 1$ et $\iota_C : C \to B \otimes_A C$, $c \to 1 \otimes c$ sont des morphismes de A-algèbres.

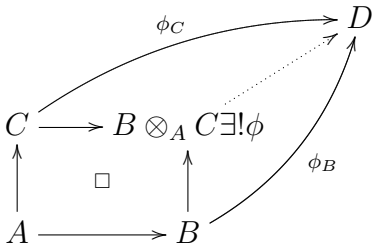
12.4.1. Lemme. (Propriété universelle du produit tensoriel de A-algèbres) *Pour toutes A-algèbres $A \to B$ et $A \to C$, il existe une A-algèbre T et des morphismes de A-algèbres $\iota_B : B \to T$, $\iota_C : C \to T$ tels que pour toute A-algèbre $A \to D$ et morphismes de A-algèbres $\phi_B : B \to D$, $\phi_C : C \to D$ il existe un unique morphisme de A-algèbres $\phi : T \to D$ tel que $\phi \circ \iota_B = \phi_B$ et $\phi \circ \iota_C = \phi_C$*

Proof. On vérifie comme d'habitude que $B \otimes_A C$ et $\iota_B : B \to B \otimes_A C$, $\iota_C : C \to B \otimes_A C$ conviennent. Si $\phi : B \otimes_A C \to D$ existe les conditions $\phi \circ \iota_B = \phi_B$ et $\phi \circ \iota_C = \phi_C$ forcent $\phi(b \otimes c) = \phi_B(b)\phi_C(c)$, d'où l'unicité de ϕ sous réserve de son existence. Considérons l'application $B \times C \to D$, $(b, c) \to \phi_B(b)\phi_C(c)$. Elle est 2-$A$-bilinéaire donc se factorise en un morphisme de A-modules $\phi : B \otimes_A C \to D$ tel que $\phi(b \otimes c) = \phi_B(b)\phi_C(c)$ et on vérifie sur la construction que c'est automatiquement un morphisme de A-algèbres. □

On peut aussi réécrire 12.4.1 en disant que pour toutes A-algèbres $A \to B$, $A \to C$ et $A \to C$ l'application canonique

$$\mathrm{Hom}_{Alg/_A}(B \otimes_A C, D) \to \mathrm{Hom}_{Alg/_A}(B, D) \times \mathrm{Hom}_{Alg/_A}(C, D),\ \phi \to (\phi \circ \iota_B, \phi \circ \iota_C)$$

est bijective ou encore, plus visuellement,



Part 3. Compléments

13. Un peu de vocabulaire catégoriel (hors-programme)

Nous introduisons ici le strict minimum du langage catégoriel. Ce langage permet d'unifier formellement les mathématiques et de formuler de façon très synthétique certains résultats. Sa puissance vient du fait que tout résultat prouvé au niveau catégoriel s'applique automatiquement à toute catégorie qui en vérifie les hypothèses. Même si nous n'utiliserons ce langage que pour formuler des énoncés, nous encourageons vivement le lecteur à poursuivre plus avant; il pourra par exemple consulter les notes de cours [S10].

13.1. Catégories. Une catégorie $\mathcal{C}$ est la donnée de
- Un ensemble d' objets, noté $Ob(\mathcal{C})$;
- Pour tout $X, Y \in Ob(\mathcal{C})$, un ensemble de morphismes, noté $\mathrm{Hom}_{\mathcal{C}}(X, Y)$;
- Pour tout $X, Y, Z \in Ob(\mathcal{C})$, une *loi de composition*

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

devant satisfaire aux deux axiomes suivants
- $\circ$ est associative;
- Pour tout $X \in Ob(\mathcal{C})$ il existe $Id_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ tel que
  - $Id_X \circ f = f$, pour tout $Y \in Ob(\mathcal{C})$ et $f \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$;
  - $f \circ Id_X = f$, pour tout $Y \in Ob(\mathcal{C})$ et $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

En général, on écrira $X \in \mathcal{C}$ plutôt que $X \in Ob(\mathcal{C})$ et $f : X \to Y$ (un morphisme dans $\mathcal{C}$) plutôt que $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

Etant donnée une catégorie $\mathcal{C}$, on note $\mathcal{C}^{op}$ la catégorie définie par
- $Ob(\mathcal{C}^{op}) = Ob(\mathcal{C})$;
- Pour tout $X, Y \in \mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}^{op}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$.

Exemples. Voici quelques catégories classiques.
- Ens: catégorie des ensembles et des applications ensemblistes;
- $Mono$: catégorie des monoïdes et des morphismes de monoïdes;
- Grp: catégorie des groupes et des morphismes de groupes;
- Ann: catégorie des anneaux et des morphismes d'anneaux;
- Etant donné un anneau A, A-Alg: catégorie des A-algèbres associatives unitaires et des morphismes de A-algèbres;
- Top: catégorie des espaces topologiques et des applications continues *etc.*

On dit qu'un morphisme $f : X \to Y$ dans $\mathcal{C}$ est un *isomorphisme* s'il existe un morphisme $g : Y \to X$ dans $\mathcal{C}$ tel que $f \circ g = Id_Y$ et $g \circ f = Id_X$.

13.2. Foncteurs. Un foncteur $F : \mathcal{C} \to \mathcal{C}'$ entre deux catégories est la donnée de
- Une application $F : Ob(\mathcal{C}) \to Ob(\mathcal{C}')$;
- Pour tout $X, Y \in \mathcal{C}$, une application $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$ compatible avec $\circ$ et les identités *i.e.* telle que
  - $F(Id_X) = Id_{F(X)}$, pour tout $X \in \mathcal{C}$;
  - $F(g \circ f) = F(g) \circ F(f)$, pour tout $X \xrightarrow{f} Y \xrightarrow{g} Z$ dans $\mathcal{C}$.

Exemples. Les exemples les plus courant de foncteurs sont les
- Foncteurs d'oubli, qui consiste à oublier des structures; par exemple, on a des foncteurs d'oubli tautologiques A-$Alg \to Ann \to Grp \to Mono \to Ens$;
- Foncteurs pleinement fidèles (ou sous-catégories) $F : \mathcal{C} \hookrightarrow \mathcal{C}'$ *i.e.* tels que pour tout $X, Y \in \mathcal{C}$ l'application $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$ est bijective. Par exemple, le foncteur d'oubli $Grp \to Mono$ est une sous-catégorie; ce n'est par contre pas le cas par exemple pour les foncteurs d'oubli A-$Alg \to Ann$, $Ann \to Grp$ ou $Mono \to Ens$;
- Etant donnée une catégorie $\mathcal{C}$ et $X \in \mathcal{C}$, les foncteurs:
  - $Hom_C(X, -) : \mathcal{C} \to Ens$;
  - $Hom_C(-, X) : \mathcal{C}^{op} \to Ens$.

13.3. Morphismes de foncteurs. Etant donnés deux foncteurs $F, G : \mathcal{C} \to \mathcal{C}'$, un morphisme de foncteurs $\Theta : F \to G$ est la donnée d'un ensemble de morphismes dans $\mathcal{C}'$

$$\Theta(X) : F(X) \to G(X),\ X \in \mathcal{C}$$

tels que, pour tout $X, Y \in \mathcal{C}$ et $f : X \to Y$ dans $\mathcal{C}$, le diagramme suivant commute

$$\begin{array}{ccc} F(X) & \xrightarrow{\Theta(X)} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow[\Theta(Y)]{} & G(Y). \end{array}$$

On vérifie facilement que l'ensemble des foncteurs de $\mathcal{C} \to \mathcal{C}'$ muni des morphismes de foncteurs forme une catégorie $F(\mathcal{C}, \mathcal{C}')$ (avec les lois de composition et les identités évidentes).

On dit qu'un foncteur $F : \mathcal{C} \to \mathcal{C}'$ est une équivalence de catégories s'il existe un morphismes de foncteurs $G : \mathcal{C}' \to \mathcal{C}$ tel que $F \circ G$ soit isomorphe à $Id_{\mathcal{C}'}$ dans $F(\mathcal{C}', \mathcal{C}')$ et $G \circ F$ soit isomorphe à $Id_{\mathcal{C}}$ dans $F(\mathcal{C}, \mathcal{C})$. Cela revient à dire que $F : \mathcal{C} \to \mathcal{C}'$ est essentiellement surjectif (*i.e.* pour tout $X' \in \mathcal{C}'$ il existe $X \in \mathcal{C}$ tel que $F(X)$ soit isomorphe à X' dans $\mathcal{C}'$) et pleinement fidèle (*i.e.* pour tout $X, Y \in \mathcal{C}$ l'application $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$ est bijective[7]).

Montrer que deux catégories sont équivalentes est souvent utile car cela permet de considérer un problème sous deux angles distincts. Parmi les exemples classiques, on peut citer l'équivalence entre la catégorie des revêtements topologiques d'un espace topologique et la catégorie des représentations discrètes de son groupe fondamental topologique ou l'équivalence entre la catégorie des schémas et la catégorie opposée des anneaux.

13.3.1. *Foncteur représentable.* Une autre notion essentielle, est celle de foncteur représentable, derrière laquelle se cache la notion d'objet universel, dont (vous avez déjà rencontré et dont) nous rencontrerons de nombreux exemples. On dit qu'un foncteur $F : \mathcal{C} \to Ens$ (resp. $F : \mathcal{C}^{op} \to Ens$) est représentable (dans $\mathcal{C}$) s'il existe $X \in \mathcal{C}$ et un isomorphisme de foncteurs

$$\Theta : \mathrm{Hom}_{\mathcal{C}}(X, -) \tilde{\to} F \ \ (\text{resp. } \Theta : \mathrm{Hom}_{\mathcal{C}}(-, X) \tilde{\to} F).$$

On dit alors que $(X, e := \theta(X)(Id_X))$ représente F ou est universel pour F. Dans ce cas, pour tout $Y \in \mathcal{C}$ l'isomorphisme $\Theta(Y) : \mathrm{Hom}_{\mathcal{C}}(X, Y) \tilde{\to} F(Y)$ est donné par $(f : X \to Y) \mapsto F(f)(e)$.

Etant donnée une catégorie $\mathcal{C}$, introduisons le foncteur

$$\begin{array}{rccl} h_{\mathcal{C}}: & \mathcal{C}^{op} & \to & F(\mathcal{C}, Ens) \\ & X & \to & \mathrm{Hom}_{\mathcal{C}}(X, -) \\ & u : Y \to X & \to & - \circ u. \end{array}$$

Le lemme suivant, bien qu'élémentaire, est essentiel.

Lemme 13.1. (Yoneda) *Pour tout $X \in \mathcal{C}$ et pour tout foncteur $F : \mathcal{C} \to Ens$, on a un isomorphisme*

$$\begin{array}{rccl} \Phi(X, F): & \mathrm{Hom}_{F(\mathcal{C}, Ens)}(h_{\mathcal{C}}(X), F) & \tilde{\to} & F(X) \\ & \Theta = (\Theta(Y))_{Y \in \mathcal{C}} & \to & \Theta(X)(Id_X) \end{array}$$

fonctoriel en X et F. Son inverse est donné par

$$\begin{array}{rccl} \Psi(X, F): & F(X) & \tilde{\to} & \mathrm{Hom}_{F(\mathcal{C}, Ens)}(h_{\mathcal{C}}(X), F) \\ & e & \to & (f : X \to Y \mapsto F(f)(e))_{Y \in \mathcal{C}}. \end{array}$$

Preuve. On vérifie que les deux constructions sont inverses l'une de l'autre:

$$\begin{array}{rl} \Psi(X, F) \circ \Phi(X, F)(\Theta) & = \Psi(X, F)(\Theta(X)(Id_X)) \\ & = (f : X \to Y \mapsto F(f)(\Theta(X)(Id_X)))_{Y \in \mathcal{C}} \\ & = (f : X \to Y \mapsto \Theta(Y)(h_{\mathcal{C}}(f)(Id_X)))_{Y \in \mathcal{C}} \\ & = (f : X \to Y \mapsto \Theta(Y)(f))_{Y \in \mathcal{C}} = \Theta \end{array}$$

et

$$\begin{array}{rl} \Phi(X, F) \circ \Psi(X, F)(e) & = \Phi(X, F)((f : X \to Y \mapsto F(f)(e))_{Y \in \mathcal{C}}) \\ & F(Id_X)(e) = Id_{F(X)}(e) = e. \end{array}$$ □

[7]Plus précisément, si ces applications sont injectives, on parle de foncteur fidèle et si elles sont surjectives, de foncteur plein.

En appliquant le lemme 13.1 au cas $F = h_{\mathcal{C}}(Y)$, on obtient que le foncteur $h_{\mathcal{C}} : \mathcal{C}^{op} \to F(\mathcal{C}, Ens)$ est pleinement fidèle. Il est alors facile d'en déduire

- qu'un morphisme $u : X \to Y$ est un isomorphisme dans $\mathcal{C}$ si et seulement si pour tout $Z \in \mathcal{C}$ l'application
$$- \circ u : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$
est bijective.
- que si (X, e) et (X', e') représentent dans $\mathcal{C}$ un même foncteur $F : \mathcal{C} \to Ens$, alors il existe un unique isomorphisme $f : X \to X'$ dans $\mathcal{C}$ tel que $F(f)(e) = e'$. On dit que l'objet universel (X, e) pour $F : \mathcal{C} \to Ens$ est unique à un unique isomorphisme près (toujours dans $\mathcal{C}$ bien sûr).

Exemples. (Produits et coproduits) Etant donnée une catégorie $\mathcal{C}$ et une famille d'objets $\underline{X} = X_i$, $i \in I$, on peut définir les foncteurs
$$\Pi^{\underline{X}} = \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(-, X_i) : \mathcal{C}^{op} \to Ens$$
et
$$\Pi_{\underline{X}} = \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(X_i, X) : \mathcal{C} \to Ens$$
Si $\Pi^{\underline{X}}$ (resp. $\Pi_{\underline{X}}$) est représentable, on dit que le couple $(Z, \underline{p} = (p_i : Z \to X_i)_{i \in I})$ (resp. $(Z, \underline{\iota} = (\iota_i : X_i \to Z)_{i \in I})$) qui le représente est le produit (resp. coproduit) des X_i, $i \in I$ et on le note $(\prod_{i \in I} X_i, \underline{p})$ (resp. $(\bigsqcup_{i \in I} X_i, \underline{\iota})$).

On peut citer bien d'autres exemples élémentaires d'objets universels: les noyaux conoyaux, les produits tensoriels, les limites inductives et projectives, les objets 'libres' (groupes libres, anneaux de polynômes *etc.*).

On vient de voir que les objets universels (X, e), *lorsqu'ils existent* sont donc toujours uniques à unique isomorphisme près; ils sont donc uniquement déterminés par leur propriété universelle (le foncteur $F : \mathcal{C} \to Ens$ qu'ils représentent) et c'est presque toujours cela qu'on utilise quand on les manipulent. Par contre, leur existence est souvent un problème délicat (et central!).

13.4. Adjonction. Deux foncteurs $F : \mathcal{C} \to \mathcal{C}'$ et $G : \mathcal{C}' \to \mathcal{C}$ sont dits adjoints[8] si on a un isomorphisme de foncteurs $\mathcal{C} \times \mathcal{C}' \to Ens$
$$\mathrm{Hom}_{\mathcal{C}'}(F(-), +) \tilde{\to} \mathrm{Hom}_{\mathcal{C}}(-, G(+)).$$
Supposons $F : \mathcal{C} \to \mathcal{C}'$ donné alors, d'après le lemme de Yoneda, si $G : \mathcal{C}' \to \mathcal{C}$ existe, il est unique (Pour tout $X' \in \mathcal{C}'$, l'objet $G(X') \in \mathcal{C}$ représente le foncteur $\mathrm{Hom}_{\mathcal{C}'}(F(-), X') : \mathcal{C} \to Ens$.

anna.cadoret@imj-prg.fr
IMJ-PRG, Sorbonne Université
Paris, FRANCE

[8]Plus précisément, F est adjoint à gauche de G et G est adjoint à droite de F.