ALGÈBRE ET THÉORIE DE GALOIS

ANNA CADORET

COURS DE MASTER 1 À SORBONNE UNIVERSITÉ - VERSION 2019 (EN COURS D'ACTUALISATION)

Table des matières

Références

[AM69] M.F. Atiyah et I.G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[D18] J.F. Dat, *Algèbre et théorie de Galois*, polycopié de cours disponible sur : https ://webusers.imj-prg.fr/ jean-francois.dat/enseignement/AlgebreM1/ATG1718.pdf

[L02] S. Lang, *Algebra (3rd ed.)*, G.T.M. **211**, Springer, 2002.

[S68] J.P. Serre, *Corps locaux*, Hermann, 1968.

Remerciements : Sarah Wajsbrot (promotion 2018-19).

Ne pas hésiter à me signaler les coquilles et, le cas échéant, me demander de clarifier certains arguments/définitions. Tout commentaire permettant d'améliorer l'exposition est le bienvenu.

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).

Première partie 1. **Anneaux - généralités**

1. Premières définitions et constructions

1.1. **Définitions.**

1.1.1. On rappelle qu'un monoïde est un couple $(M, \times)$ formé d'un ensemble M et d'une application $\times : M \times M \to M$ 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 $m \cdot e_M = m = e_M \cdot m$, $m \in M$;

Et on dit qu'un monoïde $(M, \times)$ est un groupe si, de plus

(3) Inverse : pour tout $m \in M$ il existe $n \in M$ tel que $m \cdot n = e_M = n \cdot m$.

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 $Hom_{Mono}(M, N)$, $End_{Mono}(M, N)$.

On dit qu'un monoïde $(M, \cdot)$ est abélien ou commutatif si $m \cdot n = n \cdot m$, $m, n \in M$.

1.1.2. 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 (ou simplement 0) 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 (ou simplement 1) 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 omet presque toujours les données $+, \cdot$ des notations.

Un anneau A est dit commutatif si $ab = ba$, $a, b \in A$.

1.1.3. Le monoïde $(A, \cdot)$ n'est pas un groupe en général ; on note $A^\times \subset A$ le sous-ensemble des éléments inversibles *i.e.* l'ensemble des $a \in A$ tel qu'il existe $b \in A$ tel que $ab = 1 = ba$; c'est un groupe d'élément neutre 1. On note alors $a^{-1} \in A^\times$ 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'anneaux).
— L'anneau $\mathbb{Z}$ des entiers. Dans ce cas $\mathbb{Z}^\times = \{\pm 1\}$.
— Les corps commutatifs, par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
— 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, $End_k(M)^\times = GL_k(M)$.
— On rencontre aussi beaucoup d'anneaux en analyse : les anneaux $\mathcal{C}(X, \mathbb{R})$ ou $\mathcal{C}(X, \mathbb{C})$ de fonctions continues à valeurs réelles ou complexes sur un espace topologique X, les anneaux $L^p(X, \mu)$ de fonctions intégrables sur un espace mesuré (X, μ), les anneaux de séries entières *etc.*

1.1.4. 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 $Hom(A, B)$ l'ensemble des morphismes d'anneaux $\phi : A \to B$ et, si $A = B$, $End(A) := Hom(A, A)$.

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 $\phi : A^\times \to B^\times$.

1.1.5. Si A est un anneau, un sous-anneau de A est un sous-ensemble $A' \subset A$ 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).

1.1.6. 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 donnés 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 $Hom_A(B, C)$ l'ensemble des morphismes de A-algèbres $\phi : B \to C$ et, si $B = C$, $End_A(B) := Hom_A(B, C)$. 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 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.

Exercice. (Quaternions) On considère le $\mathbb{R}$-espace vectoriel $\mathbb{H}$ de base $1, i, j, k$ muni du produit $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$ définie par $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

(1) Montrer que $(\mathbb{H}, +, \cdot)$ est un anneau à division, non commutatif. Déterminer son centre et en déduire que c'est une $\mathbb{R}$-algèbre.

(2) On note i une racine carré de -1 dans $\mathbb{C}$ et on considère les matrices

$$I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Montrer que le sous-$\mathbb{R}$-espace vectoriel de $M_2(\mathbb{C})$ engendré par Id, I, J, K est un sous-$\mathbb{R}$-algèbre de $(M_2(\mathbb{C}), +, \cdot)$ isomorphe à $\mathbb{H}$.

1.2. **Produits.** Si A_i, $i \in I$ est une famille d'anneaux, on peut munir le produit ensembliste $\prod_{i\in I} A_i$ d'une structure d'anneau en posant, pour $\underline{a} = (a_i)_{i\in I}$, $\underline{b} = (b_i)_{i\in I} \in \prod_{i\in I} A_i$

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

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.

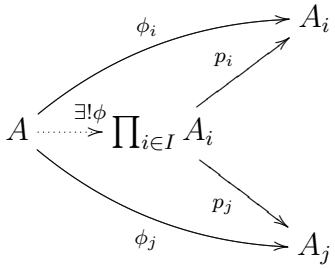
??.1 **Lemme.** (Propriété universelle du produit) *Pour toute famille d'anneaux A_i, $i \in I$ il existe un anneau Π et une famille de morphisme d'anneaux $p_i : \Pi \to A_i$, $i \in I$ tels que pour tout anneau A et famille de morphisme d'anneaux $\phi_i : A \to A_i$, $i \in I$, il existe un unique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

Démonstration. 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. □

On peut aussi réécrire **??** 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 :



??.2 **Remarque.** 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 du Lemme **??**.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. On dit de façon un peu informelle que l'anneau produit $p_i : \prod_{i\in I} A_i \to A_i$, $i \in I$ est unique à unique isomorphisme près. On rencontrera beaucoup d'autres constructions de ce type dans la suite.

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

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

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 $p_i \circ \phi = \phi_i \circ p_i$, $i \in I$.

??.3 Si $A_i = A$, $i \in I$, on note $\prod_{i\in I} A_i = A^I$. On peut voir A^I comme l'anneau des fonctions $a : I \to A$ muni de $(a+b)(i) = a(i)+b(i)$ et $(a\cdot b)(i) = a(i)\cdot b(i)$ de zéro l'application nulle et d'unité l'application constante de valeur 1_A. 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}.

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

$$(??.1)\quad (\sum_{n\in\mathbb{N}} a_n e_n) * (\sum_{n\in\mathbb{N}} b_n e_n) = \sum_{n\in\mathbb{N}} (\sum_{i,j\in\mathbb{N}, i+j=n} a_i b_j) e_n.$$

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 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 (**??**.1) se réécrit de façon plus intuitive sous la forme

$$(??.2)\quad (\sum_{n\in\mathbb{N}} a_n X^n)(\sum_{n\in\mathbb{N}} b_n X^n) = \sum_{n\in\mathbb{N}} (\sum_{i,j\in\mathbb{N}, i+j=n} a_i b_j) X^n.$$

??.3 **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 $p \in P$ 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 $ev_b^\phi(p) = b$.*

Démonstration. Vérifions que $\iota_A : A \to A[X]$ munie de 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. □

Le même argument formel que celui utilisé dans **??**.2 montre que la A-algèbre $\iota_A : A \to A[X]$ est unique à unique isomorphisme près.

On peut aussi réécrire **??**.3 en disant que, pour toute A-algèbre $\phi : A \to B$ l'application canonique

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

est bijective. 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.

Soit $\phi : A \to B$ un morphisme d'anneaux commutatifs. En appliquant la propriété universelle des $\iota_A : A \to A[X]$ à la A-algèbre

$$A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[X]$$

on obtient un unique morphisme d'anneaux $\tilde{\phi} : A[X] \to B[X]$ tel que $\iota_B \circ \phi = \phi \circ \iota_A$; explicitement $\tilde{\phi}(\sum_{n\geq 0} a_x X^n) = \sum_{n\geq 0} \phi(a_n) X^n$.

??.4 **Remarque.** 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 **??**.3, 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 **??**.3 comme suit.

??.3' **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 $\nu_A : (\mathbb{N}, +) \to (P, \cdot)$ 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 $ev_b^\phi : P \to B$ tel que $ev_b^\phi \circ \nu_A = \nu$.*

Ou encore : 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 $f(X)^n$.

??.5 Avec le point de vue développé dans la Remarque **??**.4, 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 $\underline{a} = \sum_{\underline{n} \in N^r} a_n e_n$. 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

$$(\mathbf{??}.6)\quad (\sum_{n \in N} a_n e_n) * (\sum_{n \in N} b_n e_n) = \sum_{n \in N} (\sum_{i,j \in N, i \cdot j = n} a_i b_j) e_n.$$

on obtient un anneau (commutatif si $(N, \cdot)$ est commutatif) $(A^{(N)}, +, *)$ ayant pour unité $e_{\underline{1_N}}$. 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 $\nu_A : (N, \cdot) \to (A^{(N)} \setminus \{0\}, *)$. 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 (**??**.5) se réécrit de façon plus intuitive sous la forme

$$(\mathbf{??}.7)\quad (\sum_{n \in N} a_n n) * (\sum_{n \in N} b_n n) = \sum_{n \in N} (\sum_{i,j \in N, i \cdot j = n} a_i b_j) n.$$

??.8 **Lemme.** (Propriété universelle de la A-algèbre du monoïde $(N, \cdot)$) *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A : A \to P$ et un morphisme de monoïdes $\nu_A : (N, \cdot) \to (P, \cdot)$ 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 $\tilde{\nu} : P \to B$ tel que $\tilde{\nu} \circ \nu_A = \nu$.*

Démonstration. Similaire à celle de **??**.3 en vérifiant que $\iota_A : A \to A[N]$ convient. □

Le même argument formel que celui utilisé dans **??**.2 montre que la A-algèbre $\iota_A : A \to A[N]$ est unique à unique isomorphisme près.

On peut aussi réécrire **??**.8 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 $\tilde{\nu}(\sum_{n \in N} a_n n) = \sum_{n \in N} \phi(a_n) \nu(n)$).

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 (**??**.5) 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 $A[X_1,\dots,X_r]:=A[\mathbb{N}^r]$ et on dit que $\iota_A:A\to A[X_1,\dots,X_r]$ est la A-algèbre des polynômes à r inderminées. Comme se donner un morphisme de monoïdes $\nu:(\mathbb{N}^r,+)\to(B,\cdot)$ revient à se donner les images $b_i\in B$ de $(\delta_{i,j})_{1\leq j\leq r}\in\mathbb{N}^r$, on peut reformuler **??**.7 de la façon suivante.

Pour toute A-algèbre $\phi:A\to B$, en notant

$$\mathfrak{B}_r:=\{\underline{b}=(b_1,\dots,b_r)\in B^r\mid b_ib_j=b_jb_i,\ 1\leq i,j\leq r\},$$
$$\mathrm{Hom}_A(A[X_1,\dots,X_r],B)\to\mathfrak{B}_r,\ f\to(f(X_1),\dots,f(X_r))$$

est bijective. Son inverse est l'application qui à $\underline{b}=(b_1,\dots,b_r)\in\mathfrak{B}_r$ 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 $\underline{b}$.

(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 se donner un morphisme de monoïdes $\nu:(\mathbb{Z},+)\to(B,\cdot)$ revient à se donner l'image $b\in B^\times$ de $1\in\mathbb{Z}$, on peut reformuler **??**.7 de la façon suivante.

Pour toute A-algèbre $\phi:A\to B$, l'application canonique

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

est bijective. Son inverse est l'application qui à $b\in B^\times$ associe l'unique morphisme de A-algèbres $ev_{\underline{b}}^{\phi}:A[X,X^{-1}]\to B$ tel que $ev_{\underline{b}}^{\phi}(X)=b$ (donc $ev_{\underline{b}}^{\phi}(\sum_{n\in\mathbb{Z}}a_n\underline{X}^{\underline{n}})=\sum_{n\in\mathbb{Z}}\phi(a_n)b^n$).

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 se donner un morphisme de monoïdes $\nu:(\mathbb{Z}^r,+)\to(B,\cdot)$ revient à se donner les images $b_i\in B^\times$ des $(\delta_{i,j})_{1\leq j\leq r}\in\mathbb{Z}$, $i=1,\dots,r$ on peut reformuler **??**.8 de la façon suivante.

Pour toute A-algèbre $\phi:A\to B$, en notant

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

l'application canonique

$$\mathrm{Hom}_A(A[X_1,X_1^{-1},\cdots,X_r,X_r^{-1}],B)\to\mathfrak{B}_r,\ f\to(f(X_1),\dots,f(X_r))$$

est bijective. Son inverse est l'application qui à $\underline{b} = (b_1, \dots, b_r) \in \mathfrak{B}_r^\times$ associe l'unique morphisme de A-algèbres $ev_{\underline{b}}^\phi : A[X_1, X_1^{-1}, \cdots, X_r, X_r^{-1}] \to B$ tel que $ev_{\underline{b}}^\phi(X_i) = b_i$, $i = 1, \dots r$ (donc $ev_{\underline{b}}^\phi(\sum_{\underline{n}\in\mathbb{Z}^r} a_{\underline{n}}\underline{X^n}) = \sum_{\underline{n}\in\mathbb{Z}^r} \phi(a_{\underline{n}})\underline{b^n}$).

(**??**.9) Soit $(N, \cdot)$ un monoïde et $\phi : A \to B$ un morphisme d'anneaux commutatifs. La propriété universelle de $\iota_A : A \to A[N]$ appliquée avec $A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[N]$ donne un unique morphisme de A-algèbres $\tilde{\phi} : A[N] \to B[N]$ tel que $\nu_B = \tilde{\phi} \circ \nu_A$. Explicitement $\tilde{\phi}(\sum_{n\geq 0} a_n e_n) = \sum_{n\geq 0} \phi(a_n)e_n$. Par construction, $\mathrm{im}(\phi) = \mathrm{im}(\phi)[N] \subset B[N]$ et $\ker(\tilde{\phi})$ est l'ensemble des éléments de la forme $\sum_{n\geq 0} a_n e_n \in A[N]$ tels que $a_n \in \ker(\phi)$, $n \geq 0$. On notera $\ker(\phi)[N] := \ker(\tilde{\phi}) \subset A[N]$.

??.10 **Exercice.**

(1) Montrer qu'on a un morphisme surjectif A-algèbres canonique

$$A[X_1, Y_1, \dots, X_r, Y_r] \twoheadrightarrow A[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}].$$

Correction. *Plus généralement, on peut montrer qu'on a une application canonique injective*

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

qui envoie morphismes de monoïdes injectifs (resp. surjectifs, resp. bijectifs) sur morphismes de A-algèbres injectifs (resp. surjectifs, resp. bijectifs). L'existence de $\tilde{-} : \mathrm{Hom}_{Mono}(N_1, N_2) \to \mathrm{Hom}_A(A[N_1], A[N_2])$ est une conséquence formelle de la propriété universelle de la A-algèbre de monoïdes $\iota_A : A \to A[N_1]$ appliquée avec la A-algèbre $\iota_A : A \to A[N_2]$ et le morphisme de monoïdes $N_1 \xrightarrow{\nu} N_2 \xrightarrow{\nu_A} A[N_2]$: il existe un unique morphisme de A-algèbre $\tilde{\nu} : A[N_1] \to A[N_2]$ tel que le diagramme suivant commute

$$\begin{array}{ccc} N_1 & \xrightarrow{\nu_A} & A[N_1] \\ {\scriptstyle\nu}\downarrow & & \downarrow{\scriptstyle\tilde{\nu}} \\ N_2 & \xrightarrow[\nu_A]{} & A[N_2] \end{array}$$

L'injectivité de $\tilde{-} : \mathrm{Hom}_{Mono}(N_1, N_2) \to \mathrm{Hom}_A(A[N_1], A[N_2])$ résulte de l'injectivité des $\nu_A : N_i \to A[N_i]$, $i = 1, 2$. Enfin, le fait que $\tilde{-} : \mathrm{Hom}_{Mono}(N_1, N_2) \to \mathrm{Hom}_A(A[N_1], A[N_2])$ envoie morphismes de monoïdes injectifs (resp. surjectifs, resp. bijectifs) sur morphismes de A-algèbres injectifs (resp. surjectifs, resp. bijectifs) résulte du fait que, par construction, tout élément de $A[N]$ s'écrit de façon unique sous la forme $\sum_{n\in N} ae_n$ (on verra dans le chapitre sur les modules que $A[N]$ est un A-module libre de base les e_n, $n \in N$) et que la condition $\nu_A \circ \nu = \tilde{\nu} \circ \nu_A$ impose $\tilde{\nu}(e_n) = e_{\nu(n)}$.
La question posée correspond au cas particulier du morphisme de monoïdes surjectif $\nu : (\mathbb{N}^2, +) \twoheadrightarrow (\mathbb{Z}, +)$ défini par $\nu(n_1, n_2) = n_1 - n_2$ (le $\tilde{\nu} : A[X_1, Y_1, \dots, X_r, Y_r] \twoheadrightarrow A[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}]$ correspondant étant défini par $\tilde{\nu}(X_i) = Z_i$, $\tilde{\nu}(Y_i) = Z_i^{-1}$, $i = 1, 2$).

(2) Montrer qu'on a des isomorphismes de A-algèbres canonique

$$A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_r][X_i] \tilde{\to} A[X_1, \dots, X_r],\ i = 1, \dots, r.$$

Correction. *Observons d'abord que toute permutation $\sigma \in \mathcal{S}_r$ induit un automorphisme du monoïde $(\mathbb{N}^r, +)$ par permutation des coordonnées donc, d'après (1), un automorphisme de la A-algèbre $A[X_1, \dots, X_r]$. (Explicitement, $\sigma P(X_1, \dots, X_r) = P(X_{\sigma(1)}, \dots, X_{\sigma(r)})$). Il suffit donc de montrer le résultat pour $i = r$. Par unicité à unique isomorphisme près des objets universel, il suffit de*

montrer que $\iota_A : A \to A[X_1, \dots, X_r]$ et $A \overset{\iota_A}{\to} A[X_1, \dots, X_{r-1}] \overset{\iota_{A[X_1,\dots,X_{r-1}]}}{\to} A[X_1, \dots, X_{r-1}][X_r]$ vérifie la même propriété universelle. Notons que par hypothèse $A[b_1, \dots, b_r]$ est un anneau commutatif (cf. **??** *pour la notation $A[b_1, \dots, b_{r-1}]$). Soit donc $\phi : A \to B$ une A-algèbre et $b_1, \dots, b_r \in B^r$ commutant deux à deux. Par la propriété universelle de $\iota_A : A \to A[X_1, \dots, X_{r-1}]$, il existe un unique morphisme de A-algèbre $ev^{\phi}_{(b_1,\dots,b_{r-1})} : A[X_1, \dots, X_{r-1}] \to B$ tel que $\phi_1(X_i) := ev^{\phi}_{(b_1,\dots,b_{r-1})}(X_i) = b_i$, $i = 1, \dots, r-1$. Puis, par la propriété universelle de $\iota_{A[X_1,\dots,X_{r-1}]} : A[X_1, \dots, X_{r-1}] \to A[X_1, \dots, X_r]$, il existe un unique morphisme de A-algèbre $ev^{\phi_1}_{b_r} : A[X_1, \dots, X_{r-1}][X_r] \to A[b_1, \dots, b_{r-1}][b_r] A[b_1, \dots, b_r]$ tel que $ev^{\phi_1}_{b_r}(X_r) = b_r$... On laisse le soin au lecteur de généraliser ce genre d'exercice formel un tantinet fastidieux.*

1.4. **Sous-anneau engendré par une partie.** Soit $A_i \subset A$, $i \in I$ une famille de sous-anneaux. On vérifie immédiatement que $\cap_{i\in I} A_i \subset A$ est un sous-anneau. Pour tout sous-ensemble $X \subset A$, il existe un unique sous-anneau $\langle X \rangle \subset A$, contenant X et minimal pour $\subset$ *i.e.* tel que pour tout sous-anneau $A' \subset A$, $X \subset A'$ implique $\langle X \rangle \subset A'$. On dit que $\langle X \rangle \subset A$ est le sous-anneau de A engendré par X. Explicitement $\langle X \rangle$ est l'intersection de tous les sous-anneaux de A contenant X. On peut également décrire $\langle X \rangle$ comme l'ensemble des sommes finies de produits finis d'éléments de X. Si $A = \langle X \rangle$, on dit que X est un système de générateurs de A comme anneau (ou que A est engendré par X comme anneau). Si on peut prendre de plus X fini, on dit que A est un anneau de type fini.

Lorsque les éléments de X commutent deux à deux, on note en général $\mathbb{Z}[X] := \langle X \rangle \subset A$ le sous-anneau de A engendré par X. Si $X = \{x_1, \dots, x_r\}$ est fini, on note plutôt $\mathbb{Z}[x_1, \dots, x_r] := \mathbb{Z}[X]$ et **??**.8 nous donne un unique morphisme d'anneaux - automatiquement surjectif - $ev_{\underline{x}} : \mathbb{Z}[X_1, \cdots, X_r] \twoheadrightarrow \mathbb{Z}[x_1, \dots, x_r]$ tel que $ev_{\underline{x}}(X_i) = x_i$, $i = 1, \dots, r$.

1.5. **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. On peut également décrire $\langle X \rangle_A$ comme le sous-anneau de B engendré par $X \cup \mathrm{im}(\phi)$. 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. Si $X = \{x_1, \dots, x_r\}$ est fini, , on note plutôt $A[x_1, \dots, x_r] := A[X]$ et **??**.8 nous donne un unique morphisme de A-algèbres - automatiquement surjectif - $ev^{\phi}_{\underline{x}} : A[X_1, \cdots, X_r] \twoheadrightarrow A[x_1, \dots, x_r]$ tel que $ev^{\phi}_{\underline{x}}(X_i) = x_i$, $i = 1, \dots, r$.

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

2. Idéaux et quotients

2.1. **Définitions, premiers exemples.**

2.1.1. Soit A un anneau (commutatif, donc). Un idéal de A est un sous-ensemble $I \subset A$ 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.
— 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, $A^{(I)} \subset A^I$ 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.

2.1.2. *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. Les anneaux qui ne sont pas de type fini, par exemple $A^{\mathbb{N}}$, fournissent tautologiquement des idéaux qui ne sont pas de type fini. L'idéal $A^{(\mathbb{N})} \subset A^{\mathbb{N}}$ n'est pas de type fini.

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

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

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

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

2.1.4. Si $\phi : A \to B$ 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 montrer par un contre-exemple que ce n'est plus vrai si on ne suppose pas $\phi : A \twoheadrightarrow B$ surjectif.

2.2. **Quotient.** Le noyau d'un morphisme d'anneaux $\phi : A \to B$ est un idéal. Réciproquement, on va voir que tout idéal est le noyau d'un morphisme d'anneaux. En effet, si A est un anneau, un idéal $I \subset A$ est en particulier un sous-groupe de $(A, +)$. On dispose donc 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. Le groupe quotient A/I est muni d'une unique structure d'anneau telle que la projection canonique $p_I := \overline{-} : A \twoheadrightarrow A/I$ est un morphisme d'anneaux. La condition que $p_I := \overline{-} : A \twoheadrightarrow A/I$ soit un morphisme d'anneaux impose que $\overline{ab} = \overline{a}\overline{b}$. 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

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

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 $\overline{1}$.

??.1 **Lemme.** (Propriété universelle du quotient) *Pour tout idéal $I \subset A$ il existe un morphisme d'anneaux $p : A \to Q$ 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 $\phi = \overline{\phi} \circ p$.*

Démonstration. Montrons que A/I muni de la structure d'anneau ci-dessus et la projection canonique $\overline{-} : A \twoheadrightarrow A/I$ conviennent. 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 :

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

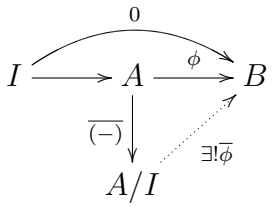
où (1) est par construction du produit sur A/I, (2) et (4) est la relation $\phi = \overline{\phi} \circ \overline{-}$ et (3) est le fait que ϕ est un morphisme d'anneaux. □

Comme d'habitude, la A-algèbre quotient $p_I := \overline{-} : A \twoheadrightarrow A/I$ est unique à unique isomorphisme près. Par construction $p_I : A \twoheadrightarrow A/I$ est surjectif de noyau I.

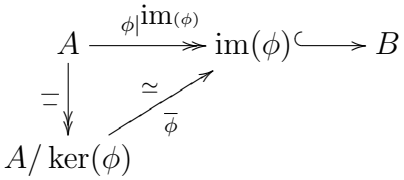
On peut aussi réécrire **??**.1 en disant que, pour tout anneau B l'application canonique

$$\mathrm{Hom}(A/I, B) \to \{A \xrightarrow{\phi} B \mid I \subset \ker(\phi)\},\ \overline{\phi} \to \overline{\phi} \circ \overline{(-)}$$

est bijective ou encore, plus visuellement :



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



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.

Exercices.

(1) Soit $I, J \subset A$ des idéaux ; notons $\overline{A} := A/I$ et $\overline{J} := P_I(J)$. Montrer que si $I \subset J$, on a un isomorphisme d'anneaux canonique $A/J \tilde{\to} \overline{A}/\overline{J}$. En déduire qu'on a toujours un isomorphisme d'anneaux canonique $A/(I+J) \tilde{\to} \overline{A}/\overline{J}$.

(2) Soit $I \subset A$ un idéal. Montrer qu'on a un isomorphisme de A-algèbres canonique $A[X]/I[X] \tilde{\to} (A/I)[X]$.

(3) Soit $f_1, \ldots f_s \in A[X_1, \ldots, X_r]$. Montrer que la A-algèbre quotient

$$A \to A[X_1, \ldots, X_n] / \sum_{1 \leq i \leq s} f_i A[X_1, \ldots, X_r]$$

munie des images $\overline{X}_1, \cdots, \overline{X}_r$ de $X_1, \ldots, X_r$ vérifie la propriété universelle suivante.

(Propriété universelle de $A \to A[X_1, \ldots, X_n]/\sum_{1 \leq i \leq s} f_i A[X_1, \ldots, X_r]$) Il existe une A-algèbre $A \to \overline{P}$ munie d'éléments $\overline{p}_1, \ldots, \overline{p}_r \in \overline{P}$ tels que pour tout A-algèbre $\phi : A \to B$ et $b_1, \ldots, b_r \in B$ vérifiant $ev^{\phi}_{\underline{b}}(f_i) = 0$, $i = 1, \ldots, s$ il existe un unique morphisme de A-algèbre $\overline{ev}^{\phi}_{\underline{b}} : \overline{P} \to B$ tel

que $\overline{ev}_{\underline{b}}^{\phi}(\overline{p}_i) = b_i$, $i = 1, \ldots, r$.

(4) Montrer qu'on a un isomorphisme de A-algèbres canonique

$$A[X_1, Y_1, \ldots, X_r, Y_r]/\sum_{1\leq i\leq r}(X_iY_i - 1)A[X_1, Y_1, \ldots, X_r, Y_r] \tilde{\to} A[X_1, X_1^{-1}, \ldots, X_r, X_r^{-1}].$$

??.2 **Lemme.** *Soit $I \subset A$ un idéal. La projection canonique $p_I : A \twoheadrightarrow A/I$ induit une bijection d'ensembles ordonnés $p_I : (V^{tot}(I), \subset) \tilde{\to} (\mathcal{I}_{A/I}, \subset)$.*

Démonstration. 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 $I_1, \ldots, I_r \subset A$ 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 **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 $I_i + I_j = A$, $1 \leq i \neq j \leq r$.*

Démonstration. 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

— $I_1 \cap (I_2 \cap \cdots \cap I_r) = I_1 \cap (I_1 \cdots I_r) = I_1 \cdot (I_2 \cdots I_r) = I_1 \cdots I_r$.
— $A \twoheadrightarrow A/I_1 \times A/(I_2 \cap \cdots \cap I_r) \twoheadrightarrow A/I_1 \times \prod_{2\leq i\leq r} A/I_i \twoheadrightarrow \prod_{1\leq i\leq r} A/I_i$

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

2.3. **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.

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

Démonstration. 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 $1 = a^{-1}a$. □

??.2 **Lemme.** *Soit $I \subsetneq A$ un idéal. Les PSSE* *(i)* *A/I est un corps ;* *(ii)* *I est maximal dans $(\mathcal{I}_A \setminus \{0\}, \subset)$.*

Démonstration. Cela résulte de **??**.2. □

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de **??**.2 est *maximal*.

??.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.*

Démonstration. 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 déja 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. D'après **??**.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.

Exercice. Soit $a \in A$. Montrer que $a \in \mathcal{J}_A$ si et seulement si $1 - ab \in A^\times$, $b \in A$.

2.3.1. *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 $at = 0$. On notera $A_{tors} \subset A$ l'ensemble des éléments de torsion de A. On dit qu'un anneau A est *intègre* si $A_{tors} = \{0\}$.

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.
— $\mathbb{Z}/n$ est intègre si et seulement si n est 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 $a \neq 0$.

??.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 $b \in I$.*

Démonstration. (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), $an \notin I$ *i.e.* $\overline{a}\overline{b} = \overline{ab} \neq 0$ in A/I. □

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de **??**.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 **??**.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, $\mathcal{N}_A = \{0\}$.

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

Démonstration. 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 $\overline{bb'} \neq 0$. □

Exercice.
— Montrer que si $a \in A$ est nilpotent, $1 + a \in A^\times$. En déduire que la somme d'un élément nilpotent et d'un élément inversible est encore inversible.
— Montrer que $A[X]^\times$ est l'ensemble des polynômes $P = \sum_{n \geq 0} a_n X^n$ tels que $a_0 \in A^\times$ et a_n est nilpotent, $n \geq 1$. Déterminer $A[X_1, \ldots, X_r]^\times$.

??.3 **Exercice.**
(1) Soit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ des idéaux premiers et $I \subset A$ un idéal. Si $I \subset \cup_{1 \leq i \leq r} \mathfrak{p}_i$ il existe $1 \leq i \leq r$ tel que $I \subset \mathfrak{p}_i$;
(2) Soit $I_1, \ldots, I_r$ des idéaux et $\mathfrak{p} \subset A$ un idéal premier. Si $\mathfrak{p} \supset \cap_{1 \leq i \leq r} I_i$ il existe $1 \leq i \leq r$ tel que $\mathfrak{p} \supset I_i$.

2.3.2. *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 A. 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 $\mathcal{I}_A^{red}$ l'ensemble des idéaux radiciels de A.

En résumé on a

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

et

I	A/I
Maximal	Corps
Premier	Intègre
Radiciel	Réduit

Classification grossière des idéaux

2.3.3. 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 $A \xrightarrow{\phi} B \overset{p_I}{\twoheadrightarrow} B/I$ 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

$$\begin{array}{ccc} (\mathcal{I}_B, \subset) & \overset{\phi^{-1}}{\to} & (\mathcal{I}_A, \subset) \\ \bigcup & & \bigcup \\ (\mathcal{I}_B^{red}, \subset) & \overset{\phi^{-1}}{\to} & (\mathcal{I}_A^{red}, \subset) \\ \bigcup & & \bigcup \\ (spec(B), \subset) & \overset{\phi^{-1}}{\to} & (spec(A), \subset) \end{array}$$

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.

3. Anneaux noetheriens

3.1. 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 $\subset$.

Démonstration. (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 (1).
(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 **??** est *noetherien*.

3.2. 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-espace vectoriel. Si A est de dimension finie sur k, elle est donc noetherienne. Par exemple l'anneau $k[X]/X^n k[X]$ est un 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 (**??**) que si k est un corps commutatif, l'anneau $k[X_1, X_2]$ est noetherien mais la sous-k-algèbre engendrée par les $X_1 X_2^n$, $n \geq 0$ n'est pas un anneau noetherien.

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

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

Démonstration. 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 $I^\circ := \sum AP_{k,l} \subset I$ 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

$a_{d+1} = \sum_{1\leq i\leq r_n} \alpha_i a_{d+1,i}$ 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°. □

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

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

3.5. Exercices.

(1) Soit A un anneau noetherien. Montrer que pour tout idéal $I \subsetneq A$, $\sqrt{I}$ est l'intersection d'un nombre fini d'idéaux premiers. En déduire que A possède un nombre fini d'idéaux premiers minimaux pour $\subset$.

(2) (Anneaux artiniens) Soit A un anneau. Montrer que les PSSE

   (a) Toute suite d'idéaux de A croissante pour $\subset$ est stationnaire à partir d'un certain rang.

   (b) Tout sous-ensemble non vide d'idéaux de A admet un élément maximal pour $\subset$.

   On dit qu'un anneau A qui vérifie les propriétés équivalente ci-dessus est *artinien*. En dépit de la similitude des définitions, les anneaux artiniens et noetheriens se comportent très différemment. Soit A un anneau artinien. Montrer que

   (a) Tout idéal premier de A est maximal.

   (b) A ne possède qu'un nombre fini d'idéaux (premiers=) maximaux.

   (c) A est noetherien.

   En fait, on peut montrer qu'un anneau est artinien si et seulement si il est noetherien et tous ses idéaux premiers sont maximaux.

4. Anneaux principaux, euclidiens

4.1. On dit qu'un anneau commutatif intègre A est

— *euclidien* s'il est munit 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

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

— *principal* si tout idéal est de la forme Aa, $a \in A$.

4.2. 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 $r-|a|\in R$: contradiction.

(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 $P\in A[X]$ s'écrit de façon unique sous la forme $f=\sum_{n\in\mathbb{N}}a_nX^n$ avec $\underline{a}:n\to a_n\in A^{(\mathbb{N})}$. Cela permet de définir l'application degré :

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

et une application 'coefficient dominant'

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

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 $g=fq+r$ et $r=0$ ou $deg(r)<deg(f)$.*

Démonstration. Montrons l'existence par récurrence sur $deg(g)$. Ecrivons $f=\sum_{0\leq n\leq d_f}a_nX^n$, $g=\sum_{0\leq n\leq d_g}b_nX^n$, 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 $r=0$ conviennet. 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 $g_1=q_1f+r_1$ 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

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

où (1) utilise encore que $CF(f)\in A^\times$. 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 $A[X_1,\ldots,X_r]\tilde{\to}A[X_1,\ldots,\hat{X}_i,\cdots,X_r][X_i]$, $i=1,\ldots,r$, 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 $aX_i^d+\sum_{\underline{n}\in\mathbb{N}^r,\mid n_i<d}a_{\underline{n}}\underline{X}^{\underline{n}}$, 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 $w = \sqrt{-1}, \sqrt[3]{-1}, \sqrt{-2}$.

4.3. Lemme. *Euclien ⇒ Principal.*

Démonstration. 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.

4.4. Exercice. Montrer que $A[X]$ est principal si et seulement si A est un corps.

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

Démonstration. On a toujours $spm(A) \subset spec(A)$. Soit $\mathfrak{p} = Ap \in spec(A)$; on veut montrer que A/Ap est un corps. Supposons le contraire. Alors A/Ap contient un idéal maximal $\{\bar{0}\} \subsetneq \mathfrak{m} \subsetneq A/Ap$. Ecrivons $p_{\mathfrak{p}}^{-1}(\mathfrak{m}) = Am$. On a des inclusions strictes $Ap \subsetneq Am \subsetneq A$ donc il existe $a \in A$ tel que $p = am$ donc $\bar{0} = \bar{a}\bar{m}$ dans A/Ap. Comme A/Ap est intègre et $\bar{m} \neq 0$, on en déduit $a \in Ap$. Ecrivons donc $a = bp$; on a $p = am = pbm$. Comme A est intègre, on peut simplifier par p pour obtenir $1 = bm$, ce qui contredit $Am \subsetneq A$. □

5. Anneaux factoriels

Soit A un anneau commutatif intègre.

Pour tout $a, b \in A$ on a $Aa = Ab$ si et seulement si $A^\times a = A^\times b$. L'implication $A^\times a = A^\times b \Rightarrow Aa = Ab$ est toujours vraie (sans supposer A intègre). Réciproquement, si $a = 0$ alors $Ab = 0$ impose $b = 0$ puisque A est intègre. Supposons donc $a, b \neq 0$ et $Aa = Ab$. On peut écrire $a = \alpha b$ et $b = \beta a$ donc $a = \alpha\beta a$ et, comme A est intègre, on peut simplifier par a, ce qui montre que $\alpha, \beta \in A^\times$. On note $a \sim b$ (et on dit que a, b sont *associés* dans A) la relation $Aa = Ab$ ($\Leftrightarrow A^\times a = A^\times b$) ; c'est une relation d'équivalence sur A.

5.1. Eléments irréductibles, éléments premiers. On dit que $0 \neq p \in A \setminus A^\times$ est *irréductible* si pour tout $a, b \in A$, $p = ab$ implique $a \in A^\times$ ou $b \in A^\times$. On notera $\mathcal{P}_A^\circ \subset A$ l'ensemble des éléments irréductibles de A. On munit $\mathcal{P}_A^\circ$ de la relation d'équivalence $\sim$ définie par : pour tout $p, q \in \mathcal{P}_A^\circ$, $p \sim q$ si et seulement si $Ap = Aq$, ce qui est aussi équivalent à $A^\times p = A^\times q$.

On notera $\mathcal{P}_A \subset \mathcal{P}_A^\circ$ un système de représentants de $\mathcal{P}_A^\circ / \sim$.

Exemple. On a $\mathbb{Z}^\times = \{\pm 1\}$ et les irrd́uctibles 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 rṕartition 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.

Exercice. Montrer directement le théorème de la progression arithmétique pour $(m, n) = (3, 4)$.

On dit que $0 \neq p \in A \setminus A^\times$ est *premier* si $Ap \in spec(A)$. On notera $\mathcal{P}_A^\dagger \subset A$ l'ensemble des éléments premiers de A.

??.1 Lemme. *On a toujours* $\mathcal{P}_A^\dagger \subset \mathcal{P}_A^\circ$.

Démonstration. En effet, si $Ap \in spec(A)$, pour tout $a, b \in A$, $p = ab$ implique $ab \in Ap$ donc comme Ap est premier, $a \in Ap$ 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 $b \in A^\times$. □

(Contre-)exemple. En général $\mathcal{P}_A^\dagger \subsetneq \mathcal{P}_A^\circ$. Par 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 d'abord que $2 \in \mathcal{P}_A^\circ$. 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 $y \in A^\times$. Montrons ensuite que 2 n'est pas premier. Pour cela, observons que

$$2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) = 2 \times 3 \in 2A$$

mais que $1 \pm i\sqrt{5} \notin 2A$ car $N(1 \pm i\sqrt{5}) = 6 \notin N(2A) = 4N(A) \subset 4\mathbb{Z}_{\geq 0}$.

??.2 On dit qu'un anneau commutatif intègre A est *factoriel* si pour tout système de représentants $\mathcal{P}_A$ de $\mathcal{P}_A^\circ$ l'application

$$\begin{array}{rccl} (??.2.1) & A^\times \times \mathbb{N}^{(\mathcal{P}_A)} & \to & A \setminus \{0\} \\ & (u, \nu) & \to & u \displaystyle\prod_{p \in \mathcal{P}_A} p^{\nu(p)} \end{array}$$

est bijective *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 prendra garde au fait que l'élément $u_a \in A^\times$ dépend du choix du système de représentants $\mathcal{P}_A$ de $\mathcal{P}_A^\circ/\sim$ qu'on s'est fixé. Par contre, l'application $v_-(a) : \mathcal{P}_A \to \mathbb{N}$ n'en dépend pas ; si on note $\mathfrak{p} := Ap$, on peut la définir intrinsèquement par $v_\mathfrak{p}(a) = \max\{n \in \mathbb{N} \mid a \in \mathfrak{p}^n\}$. On dit que $v_p(a)$ est la multiplicité ou l'ordre de a en p ou, encore, la valuation p-adique de a.

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

On déduit de (1) et (3) que

??.4 **Lemme.** *A factoriel* $\Rightarrow \mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$.

Démonstration. On sait déjà que $\mathcal{P}_A^\dagger \subset \mathcal{P}_A^\circ$. Inversement, soit $p \in \mathcal{P}_A^\circ$. 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 $b \in Ap$. □

5.2. Proposition.
(1) Principal $\Rightarrow$ *(Noetherien intègre +* $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$*)* $\Rightarrow$ *factoriel.*
(2) [Utilise le Lemme de Zorn] Factoriel + $spm(A) = spec(A) \setminus \{0\}$ $\Rightarrow$ *Principal.*

??.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, l'application*

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

est surjective.

Démonstration. Notons $\mathcal{F} \subset A$ l'image de $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \to A \setminus \{0\}$. Observons que $\mathcal{F}$ est stable par produit et qu'il contient $\mathcal{P}_A^\circ$, $A^\times$. Si $a \notin \mathcal{F}$, $a \notin \mathcal{P}_A$ donc il existe $a_1, a_2 \notin A^\times$ tels que $a = a_1a_2$. En particulier, $Aa \subsetneq Aa_1, Aa_2$. De plus, comme $\mathcal{F}$ est stable par produit, on a $a_1 \notin \mathcal{F}$ ou $a_2 \notin \mathcal{F}$. Supposons $a_1 \notin \mathcal{F}$. En itérant, $a_1 = a_{1,1}a_{1,2}$ avec $a_{1,1}, a_{1,2} \notin A^\times$ - donc $Aa_1 \subsetneq Aa_{1,1}, Aa_{1,2}$ - et $a_{1,1} \notin \mathcal{F}$ *etc.* on construit ainsi une suite strictement croissante $Aa \subsetneq Aa_1 \subsetneq Aa_{1,1,1} \subsetneq Aa_{1,1,1,1} \subsetneq \cdots$ d'idéaux de A, ce qui contredit la noetherianité de A. □

Démonstration. (1) Principal $\Rightarrow$ (Noetherien intègre + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$).

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). Soit $p \in A$ irréductible ; on veut montrer que Ap est premier. Il suffit de montrer qu'il est maximal. Considérons donc un idéal $Ap \subsetneq I$. Fixons $a \in I \setminus Ap$. Commme A est principal, $Ap \subsetneq Ap + Aa = Ab$ donc $p = \alpha b$ avec $\alpha \in A \setminus A^\times$ (puisque $Ap \subsetneq Ab$). Mais puisque p est irréductible, on a nécessairement $b \in A^\times$ *i.e.* $Ab = A$. En particulier $A = Ap + Aa \subset I$.

(Noetherien intègre + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$) $\Rightarrow$ factoriel.

Par le Lemme **??**.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 $p \in \mathcal{P}_A^\dagger$, A/p est intègre et comme $\overline{v} \in (A/p)^\times$, 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 $spm(A) = spec(A)$ 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

$$J := \{a \in A \mid ap \in I\}$$

Puisque I est un idéal, $I \subset J$ et J est un idéal de A. De plus $I = Jp$. Par définition de J on a $Jp \subset I$ et, inversement, puisque $I \subset Ap$, tout $a \in I$ sécrit sous la forme $a = bp$ avec, par définition de J, $b \in J$. 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 signifie que la multiplication par p induit une bijection (rappelons que A est intègre) $- \cdot p : I \tilde{\to} I$. 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 par définition de J, $p^{v_p(a)-1} b \in J = I = pI \Rightarrow p^{v_p(a)-2} b \in J = I = pI \Rightarrow ... \Rightarrow b \in J = I = pI \Rightarrow v_p(b) \geq 1$.

□

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

??.2 **(Contre-)Exemples.** Les implications de **??** ne sont pas des équivalences. Par exemple,
— Anneau noetherien + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$ non principal : $k[X_1, X_2]$, où k est un corps commutatif ;
— Anneau factoriel non noetherien : $k[X_1, \ldots, X_n, \ldots, X_{n+1}, \ldots]$, où k est un corps commutatif.

5.3. Polynômes sur les anneaux factoriels.

5.3.1. 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.

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,

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

Démonstration. 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 que $\tilde{\phi} : Frac(A) \to B$ est unique puisqu'on doit nécessairement avoir

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

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 $\tilde{\phi} : A \setminus \{0\} \to B$ se factorise en

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

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.

Exercice. On dit qu'un anneau A intègre de corps des fraction K est intégralement clos si

$$A = \{x \in K[X] \mid \exists\ P_x = T^d + \sum_{0 \leq n \leq d-1} a_n T^n \in A[X] \text{ tel que } P_x(x) = 0\}.$$

Montrer qu'un anneau factoriel est intégralement clos.

Exercice. On note $\mathbb{Q} := Frac(\mathbb{Z})$ et si K est un corps, on note $K(X_1, \ldots, X_n) := Frac(K[X_1, \ldots, X_n])$. Montrer que si A est un anneau intègre de corps des fractions K alors $Frac(A[X_1, \ldots, X_n]) = K(X_1, \ldots, X_n)$.

5.3.2. *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,

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

La bijection (**??**.2.1) s'étend également en une bijection

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

d'inverse

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

5.3.3. *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 $C_A(PQ) = C_A(P)C_A(Q)$.*

Démonstration. 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 $F \in K[X]$ in $K[X]$ on a $C_A(F) = 1$ si et seulement si

(1) $F \in A[X]$;

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

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. □

5.3.4. 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.

Démonstration. L'idée est bien sûr d'exploiter que $K[X]$ est factoriel car euclidien. Fixons un système $\mathcal{P}_{K[X]}$ de représentants de $\mathcal{P}^\circ_{K[X]}$ de contenu 1 (il suffit de remplacer un système de représentants $\mathcal{P}$ donné par les $P/C_A(P)$, $P \in \mathcal{P}$). 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 **??**, $C_A(F) = C_A(P)C_A(Q) = C_A(Q)$ 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) L'application canonique $A^\times \times \mathbb{N}^{(\mathcal{P}_A \cup \mathcal{P}_{K[X]})} \to A[X] \setminus \{0\}$ est bijective.

Comme $K[X]$ est factoriel, l'application $K \setminus \{0\} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \to K[X] \setminus \{0\}$ est bijective. Elle se restreint en une application (injective !) $A \setminus \{0\} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \to A[X] \setminus \{0\}$. Cette dernière est en fait bijective car si $F = x \prod_{p \in \mathcal{P}_{K[X]}} P^{v(P)}$ (ici $x \in K \setminus \{0\}$) est dans $A[X]$, par multiplicativité du contenu, $C_A(F) = x \prod_{p \in \mathcal{P}_{K[X]}} C_A(P)^{v(P)}$ et comme par hypothèse $C_A(P) = 1$, $x \in A$. Enfin, par factorialité de A, l'application $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \tilde{\to} A \setminus \{0\}$ est bijective donc on obtient la bijection voulue comme

$$A^\times \times \mathbb{N}^{(\mathcal{P}_A \cup \mathcal{P}_{K[X]})} \tilde{\to} A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \tilde{\to} A \setminus \{0\} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \tilde{\to} A[X] \setminus \{0\}.$$

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 $p \neq q \in \mathcal{P}_A \cup \mathcal{P}_{K[X]}$ □

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

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

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

□

5.3.6. 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.

(1) **(Critère d'Eisenstein)** Soit A un anneau factoriel de corps des fractions K et $P = \sum_{n \geq 0} a_n X^n \in A[X]$. Montrer que 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 $K[X]$.

Application. Montrer que $P \in K[X]$ est irréductible si et seulement si $P(X + 1) \in K[X]$ est irréductible. En déduire que pour tout nombre premier p, le polynôme $X^p + X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

(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. La propriété universelle de $\iota_A : A \to A[X]$ appliquée avec $A \xrightarrow{\phi} B \xhookrightarrow{\iota_B} B[X]$ donne un unique morphisme d'anneaux $\tilde{\phi} : A[X] \to B[X]$ tel que $\tilde{\phi} \circ \iota_A = \iota_B \circ \phi$ (explicitement $\tilde{\phi}(\sum_{n \geq 0} a_n X^n) = \sum_{n \geq 0} \phi(a_n) X^n$). Soit $P \in A[X]$. Montrer que si $deg(\tilde{\phi}(P)) = deg(P)$ et $\tilde{\phi}(P)$ 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.

Correction. *Ecrivons $P = P_1P_2$ avec $P_1, P_2 \in A[X]$ et $deg(P_1) \leq deg(P_2)$. On veut montrer que $P_1 \in A$. Notons que par construction $deg(\tilde{\phi}(P)) \leq deg(P)$. Puisque $\tilde{\phi} : A[X] \to B[X]$ est un morphisme d'anneaux, on a $\tilde{\phi}(P) = \tilde{\phi}(P_1)\tilde{\phi}(P_2)$ dans $L[X]$. Puisque $\tilde{\phi}(P) \in L[X]$ est irréductible par hypothèse, on a $\tilde{\phi}(P_1) \in K$ ou $\tilde{\phi}(P_2) \in K$. Enfin, puisque*

$$deg(P_1) + deg(P_2) \geq deg(\tilde{\phi}(P_1)) + deg(\tilde{\phi}(P_2)) = deg(\tilde{\phi}(P)) = deg(P) = deg(P_1) + deg(P_2),$$

on a $deg(\tilde{\phi}(P_i)) = deg(P_i)$, $i = 1, 2$. Donc (on a supposé $deg(P_1) \leq deg(P_2)$) $\tilde{\phi}(P_1) \in K$, ce qui implique $deg(P_1) = deg(\tilde{\phi}(P_1)) = 0$ donc $P_1 \in A$ comme annoncé.

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 $\mathbb{Z}/p[X]$. On verra dans la partie du cours sur la théorie de Galois, qu'on comprend plutôt bien les irréductibles de $\mathbb{Z}/p[X]$.

Application. Montrer que $P = X^5 - 5X^3 - 6X - 1$ est irréductible dans $\mathbb{Q}[X]$.

Correction. *En considérant $\phi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$, on a $\tilde{\phi}(P) =: \overline{P} = X^5 + X^3 + 1$ dans $\mathbb{F}_2[X]$. Clairement $\overline{P}$ n'a pas de racine dans $\mathbb{F}_2$. Donc si $\overline{P}$ n'est pas irréductible, il s'écrit comme produit d'un polynôme de degré 2 et d'un polynôme de degré 3 :*

$$\overline{P} = (X^3 + aX^2 + bX + c)(X^2 + dX + e).$$

En développant et en identifiant les coefficients, on obtient le systèmes d'équations dans $\mathbb{F}_2$

$$\begin{aligned} &d + a = 0 \\ &e + ad + b = 1 \\ &ae + bd + c = 0 \\ &be + cd = 0 \; ce = 1 \end{aligned}$$

Mais dans $\mathbb{F}_2$, $d + a = 0$ implique $a = d$. Si $a = d = 0$, $c = 0$: contradiction. Si $a = d = 1$, $e + b = 0$, $e + b + c = 0$ donc $c = 0$: contradiction. Cela montre que $\overline{P}$ est irréductible dans $\mathbb{F}_2[X]$. Donc si $P = P_1P_2$ dans $\mathbb{Z}[X]$ avec $deg(P_1) \leq deg(P_2)$, on a forcément $P_1 \in \mathbb{Z}$ (et en fait $P_1 = \pm 1$ car $C_{\mathbb{Z}}(P) = 1 = C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2) = P_1C_{\mathbb{Z}}(P_2)$). Si $P = P_1P_2$ dans $\mathbb{Q}[X]$ avec $deg(P_1) \leq deg(P_2)$, on a $C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2) = C_{\mathbb{Z}}(P) = 1$ donc $P = P_1P_2 = \frac{P_1}{C_{\mathbb{Z}}(P_1)}\frac{P_2}{C_{\mathbb{Z}}(P_2)}$ avec, cette fois-ci, $\frac{P_1}{C_{\mathbb{Z}}(P_1)}, \frac{P_2}{C_{\mathbb{Z}}(P_2)} \in \mathbb{Z}[T]$. Donc $P_1 = C_{\mathbb{Z}}(P_1) \in \mathbb{Q}$. Cela montre bien que P est irréductible dans $\mathbb{Q}[X]$.

5.4. Valuations et anneaux factoriels.

Soit K un corps.

5.4.1. Une *valuation* (de rang 1) sur K est une application surjective[1] $v : K \to \overline{\mathbb{Z}}$ 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) $v(x) = \infty \Leftrightarrow x = 0$.

1. 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 $\mathbb{Z}$.

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.

5.4.2. Lemme. *L'ensemble $A_v \subset K$ 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 $v(\pi) = 1$.*

Démonstration. 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 idéal $I \subset A_v$ 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 $I \subset A\pi^n$. 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 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. En voici quelques unes.

Exercice. [Difficile - *cf.* [**?**, I,§2]] Soit A un anneau commutatif. Montrer que les propriétés suivantes sont équivalentes.

(1) A est un anneau de valuation discrète.
(2) A est local, noetherien et son idéal maximal est principal, engendré par un élément non nilpotent.
(3) A est intégralement clos et possède un unique idéal premier non nul.

5.4.3. 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 :

— (**??**.1) Pour tout $0 \neq x \in K$,

$$|\{v \in \mathcal{V} \mid v(x) \neq 0\}| < +\infty;$$

— (**??**.2) Il existe une famille d'élements $(p_v)_{v \in \mathcal{V}} \in K$ telle que $v(p_w) = \delta_{v,w}$, $v, w \in \mathcal{V}$;

— (**??**.3) $A = \bigcap_{v \in \mathcal{V}} A_v$

Inversement, on a

5.4.4. Proposition. *Soit K un corps muni d'une famille $\mathcal{V}$ de valuation $v : K \to \overline{\mathbb{Z}}$ vérifiant les propriétés (??.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 de $\mathcal{P}_A^\circ$.

Démonstration. Observons d'abord que $A \subset K$ est un sous-anneau comme intersection de sous-anneaux (Lemme ??). 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 (??.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 (??.2) que $v'(a) = v(a)$, $v \in \mathcal{V}$ et donc $u' = u_a$. □

5.4.5. 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 $u_1a_1 + \cdots + u_ra_r = 1$.

6. Localisation, anneaux de fractions.

On va maintenant généraliser la construction du corps des fractions d'un anneau intègre à des anneaux non nécessairement intègre. Soit A un anneau commutatif.

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

6.1.1. Exemples.

??.1 $S := A \setminus A_{tors}$; en particulier, si A est intègre, $S := A \setminus \{0\}$;

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

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

6.1.2. 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

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

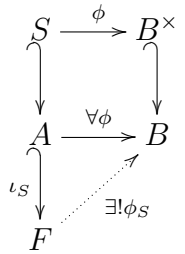
On laisse en exercice le soin de vérifier que $S^{-1}A$ muni des lois $+,\cdot : S^{-1}A \times S^{-1}A \to S^{-1}A$ ainsi définies vérifie bien les axiomes d'un anneau commutatif de zéro $0/1$ et d'unité $1/1$ et que, pour cette structure d'anneau, l'application canonique

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

est un morphisme d'anneaux de noyau $\ker(\iota_S) = \{a \in A \mid \exists s \in S,\ sa = 0\}$. 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 $s/1 \cdot 1/s = s/s = 1/1$.

6.1.3. Lemme. (Propriété universelle de la localisation) *Pour toute partie multiplicative $S \subset A \setminus \{0\}$ il existe un morphisme d'anneaux $\iota_S : A \to F$ 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 $phi_S : F \to B$ tel que $\phi = \phi_S \circ \iota_S$.*

Plus visuellement,



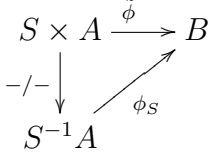
Démonstration. Montrons que $S^{-1}A$ muni de la structure d'anneau ci-dessus et le morphisme canonique $\iota_S : A \to S^{-1}A$ conviennent. Soit $\phi : A \to B$ un morphisme d'anneaux tel que $\phi(S) \subset B^\times$. Si $\phi_S : S^{-1}A \to B$ existe la relation $\phi = \phi_S \circ \iota_S$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

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

Considérons donc l'application $\begin{array}{rccc} \phi_S : & S \times A & \to & B \\ & (a,s) & \to & \phi(s)^{-1}\phi(a). \end{array}$ 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

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

Cela montre que l'application $\phi_S : S \times A \to B$ se factorise en



Par construction $\phi = \phi_S \circ \iota_S$ et on vérifie que $\phi_S : S^{-1}A \to B$ est bien un morphisme d'anneaux. □

Comme d'habitude, le morphisme d'anneaux $\iota_S : A \to S^{-1}A$ est unique à unique isomorphisme près et on dit que c'est 'la' localisation de A en S. Localiser A en S revient donc à inverser formellement les éléments de S.

6.1.4. Exercice.

(1) Montrer qu'on a un isomorphisme d'anneaux canonique $S^{-1}(A[X]) \tilde{\to} (S^{-1}A)[X]$.

(2) Soit p, q deux premiers distincts. Déterminer les idéaux premiers $\mathfrak{p}$ de $A := \mathbb{Z}/pq$ et déterminer dans chaque cas le localisé $(A \setminus \mathfrak{p})^{-1}A$.

(3) Montrer que si A est intègre (resp. réduit, resp. intégralement clos, resp. factoriel) alors $S^{-1}A$ l'est aussi.

6.1.5. Exemples.

??.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).

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

??.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, $A_{\{0\}} = Frac(A)$.

6.1.6. 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 $\tilde{\phi} : S^{-1}A \to T^{-1}B$ tel que $\iota_T \circ \phi = \tilde{\phi} \circ \iota_S$; explicitement $\tilde{\phi}(a/s) = \phi(a)/\phi(s)$ 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 $S^{-1}(\psi \circ \phi) = (\tilde{\phi}) \circ (T^{-1}\psi)$.

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.

6.2. 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. 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 :

6.2.1. 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
$$\iota_S^{-1} : \mathcal{I}_{S^{-1}A} \tilde{\to} \{I \in \mathcal{I}_A \mid I = \bigcup_{s \in S}(s\cdot)^{-1}I\}.$$

6.2.2. 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*
$$spec(S^{-1}A) \underset{S^{-1}}{\overset{\iota_S^{-1}}{\rightleftarrows}} \{\mathfrak{p} \in spec(A) \mid \mathfrak{p} \cap S = \emptyset\}$$

Démonstration. 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. Si $\mathfrak{p} \in spec(A)$, $A_\mathfrak{p}$ 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 **??**, 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 $\kappa(\mathfrak{p}) \hookrightarrow \kappa(\mathfrak{q})$.

6.2.3. Corollaire. *Si A est noetherien (resp. principal) alors $S^{-1}A$ l'est aussi.*

6.2.4. Exercice.

(1) Soit $\mathfrak{p} \in spec(A)$. Montrer qu'on a un morphisme d'anneaux canonique injectif $A/\mathfrak{p} \to \kappa(\mathfrak{p})$. Montrer que si $\mathfrak{p}$ est maximal, ce morphisme est un isomorphisme.

(2) Montrer que les localisés d'un anneau principal en ses idéaux premiers sont des anneaux de valuation discrète.

(3) Si $I, J \subset A$ sont des idéaux, montrer que $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$ et $S^{-1}(I + J) = S^{-1}I + S^{-1}J$.

(4) Si $I \subset J$ sont des idéaux et si on note $\overline{S} \subset A/I$ l'image de S *via* la projection canonique $A \twoheadrightarrow A/I$, montrer qu'on a un isomorphisme canonique
$$S^{-1}I/S^{-1}J \tilde{\to} \overline{S}^{-1}(I/J).$$

7. Completion (Hors programme)

7.1. Limites projectives. Un système projectif d'ensembles est une suite d'applications ensemblistes

$$(X_\bullet, \phi_\bullet) \quad \cdots X_{n+1} \overset{\pi_{n+1}}{\to} X_n \overset{\pi_n}{\to} X_{n-1} \overset{\pi_{n-1}}{\to} \cdots \overset{\pi_1}{\to} X_0.$$

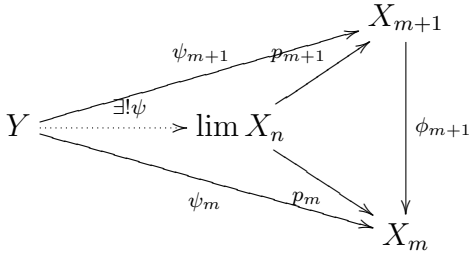
Etant donné un système projectif $(X_\bullet, \phi_\bullet)$ d'ensembles, on note

$$\lim X_n := \{\underline{x} = (x_n)_{n\geq 0} \in \prod_{n\geq 0} X_n \mid \pi_{n+1}(x_{n+1}) = x_n,\ n \geq 0\} \subset \prod_{n\geq 0} X_n$$

et pour chaque $m \geq 0$, on note $p_m : \lim X_n \to X_m$ la restriction à $\lim X_n$ de la $m$ième projection $p_m : \prod_{n\geq 0} X_n \to X_m$.

7.1.1. Lemme. (Propriété universelle de la limite projective) *Pour tout système projectif $(X_\bullet, \phi_\bullet)$ d'ensembles il existe des applications ensemblistes $p_m : P \to X_m$, $m \geq 0$ telles que pour toute famille d'applications ensemblistes $\psi_m : Y \to X_m$, $m \geq 0$ telles que $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, il existe une unique application ensembliste $\psi : Y \to \lim X_n$ telle que $p_m \circ \psi = \psi_m$, $m \geq 0$.*

Plus visuellement



Démonstration. Comme d'habitude, on montre que les $p_m : \lim X_n \to X_m$, $m \geq 0$ vérifie la propriété universelle. La condition $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, $m \geq 0$ impose que si $\psi : Y \to \lim X_n$ existe, elle est unique, définie par

$$\psi : Y \to \prod_{n\geq 0} X_n,\ y \to (\psi_n(y))_{n\geq 0}.$$

On vérifie ensuite immédiatement que $\psi(Y) \subset \lim X_n$ et que $p_m \circ \psi = \psi_m$, $m \geq 0$. □

Comme d'habitude, la suite d'applications $p_m : \lim X_n \to X_m$, $m \geq 0$ est unique à unique isomorphisme près et on dit que c'est 'la' limite projective de $(X_\bullet, \phi_\bullet)$.

Si les applications $\phi_{n+1} : X_{n+1} \to X_n$, $n \geq 0$ sont des morphismes de monoïdes (resp. de groupes, resp. d'anneaux), on verifie immédiatement que $\lim X_n \subset \prod_{n\geq 0} X_n$ est un sous-monoïde (resp. unesous-groupe, resp. un sous-anneaux) et que les projections $p_m : \prod_{n\geq 0} X_n \to X_m$, $m \geq 0$ sont des morphismes de monoïdes (resp. de groupes, resp. d'anneaux). Le Lemme **??** admet la variante suivante dont on laisse la preuve en exercice au lecteur.

7.1.2. Lemme. *Pour tout système projectif $(X_\bullet, \phi_\bullet)$ de monoïdes (resp. de groupes, resp. d'anneaux), il existe des morphismes de monoïdes (resp. de groupes, resp. d'anneaux) $p_m : P \to X_m$, $m \geq 0$ telles que pour toute famille de morphismes de monoïdes (resp. de groupes, resp. d'anneaux) $\psi_m : Y \to X_m$, $m \geq 0$ telles que $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, il existe un unique morphismes de monoïdes (resp. de groupes, resp. d'anneaux) $\psi : Y \to \lim X_n$ tel que $p_m \circ \psi = \psi_m$, $m \geq 0$.*

7.2. Soit A un anneau commutatif et

$$A := I_0 \supset I_1 \supset I_2 \supset \cdots \supset I_n \supset I_{n+1} \supset \cdots$$

une suite décroissante d'idéaux tels que $I_m I_n \subset I_{m+n}$. Par définition, la projection canonique $p_n : A \to A/I_n$ se factorise en

$$\begin{array}{ccc} A & \xrightarrow{p_n} & A/I_n \\ \downarrow{\scriptstyle p_{n+1}} & \nearrow{\scriptstyle \pi_{n+1}} & \\ A/I_{n+1} & & \end{array}$$

d'où un système projectif de morphismes d'anneaux

$$\cdots A/I_{n+1} \overset{\pi_{n+1}}{\to} A/I_n \overset{\pi_n}{\to} A/I_{n-1} \overset{\pi_{n-1}}{\to} \cdots \overset{\pi_1}{\to} A/I$$

et, par propriété universelle de la limite projective, un unique morphisme d'anneaux

$$c_I : A \to \widehat{A} := \lim A/I_n.$$

On note

$$\widehat{I_n} := \{\underline{a} \in \widehat{A} \mid a_m = 0,\ m \leq n\}$$

7.2.1. Toute suite décroissante d'idéaux

$$A := I_0 \supset I_1 \supset I_2 \supset \cdots \supset I_n \supset I_{n+1} \supset \cdots$$

tels que $I_m I_n \subset I_{m+n}$ munit A d'une topologie définie par les systèmes fondamentaux de voisinages $a + I_n$, $n \geq 0$. Pour cette topologie, $+, \cdot : A \times A \to A$ sont continues. Une suite de Cauchy dans A est alors une suite $\underline{a} \in A^{\mathbb{N}}$ telle que pour tout $N \geq 0$ il existe $n \geq 0$ tel que $a_{n+p} - a_n \in I_N$, $p \geq 0$. Si toute suite de Cauchy est convergente dans A, on dit que A est complet. On laisse la preuve du lemme suivant en exercice.

Lemme. *Avec les notations ci-dessus, le morphisme canonique d'anneaux $c_I : A \to \widehat{A}$ est continu (pour les topologies défines par les suites I_n, $n \geq 0$ et $\widehat{I}_n$, $n \geq 0$). De plus, $\widehat{A}$ est complet, séparé et $c_I : A \to \widehat{A}$ induit des isomorphismes canoniques $A/I_n \tilde{\to} \widehat{A}/\widehat{I}_n$.*

On dit que $c_I : A \to \widehat{A}$ est 'la' completion de A pour la topologie définie par la suites I_n, $n \geq 0$ (ce morphisme vérifie une propriété universelle que le lecteur devrait à peu près deviner mais que nous ne formulerons pas).

7.2.2. Le cas le plus fréquent d'application de la construction ci-dessus est pour $I_n = I^n$, $n \geq 0$ et $I \subset A$ un idéal. On parle alors de topologie I-adique et de completion I-adique. Voici deux exemples importants.

(1) $A = \mathbb{Z}$, $I = p\mathbb{Z}$ pour p un nombre premier. Dans ce cas on note $\widehat{\mathbb{Z}} := \mathbb{Z}_p$ et on dit que $\mathbb{Z} \to \mathbb{Z}_p$ est la complétion p-adique de $\mathbb{Z}$ (ou l'anneau des entiers p-adiques). Si on munit $\mathbb{Z}$ de la valeur absolue p-adique définie par $|n| = p^{-v_p(n)}$, on peut vérifier que $\mathbb{Z} \to \mathbb{Z}_p$ est la complétion de $\mathbb{Z}$ (au sens usuel des espaces métriques) pour la distance $d_p(m, n) = |m - n|_p$).

Remarque. On peut montrer (théorème d'Ostrowski) que les seules valeurs absolues sur $\mathbb{Q}$ sont (à équivalence près) la valeur absolue usuelle est les valeurs absolues p-adiques.

Exercice. Montrer que si $n \in \mathbb{Z}$ est premier à p alors $c_{p\mathbb{Z}}(n) \in \mathbb{Z}_p^\times$. En déduire qu'on a un isomorphisme canonique $\widehat{\mathbb{Z}_{p\mathbb{Z}}} \tilde{\to} \mathbb{Z}_p$, où $\widehat{\mathbb{Z}_{p\mathbb{Z}}} \to \widehat{\mathbb{Z}_{p\mathbb{Z}}}$ est la complétion $p\mathbb{Z}_{p\mathbb{Z}}$-adique de $\mathbb{Z}_{p\mathbb{Z}}$.

(2) Soit A un anneau commutatif intègre. $A = A[X]Z$, $I = XA[X]$. Plus précisément, reprenons les notations du paragraphe **??**. On munit $A^{\mathbb{N}}$ des lois $+, \cdot : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$ définies par

$$\underline{a} + \underline{b} = (a_n + b_n)_{n\geq 0}, \quad \underline{a} \cdot \underline{b} = (\sum_{0\leq k\leq n} a_k b_{n-k}).$$

On vérifie facilement que $(A^{\mathbb{N}}, +, \cdot)$ est un anneau de zéro la suite nulle et d'unité la suite e_0. On note cet anneau $A[[X]]$ et ses éléments $\underline{a} = (a_n)_{n\geq 0} \sum_{n\geq 0} a_n X^n$. L'inclusion naturelle $A^{(\mathbb{N})} \hookrightarrow A^{\mathbb{N}}$ induit un morphisme d'anneaux $A[X] \hookrightarrow A[[X]]$, dont on vérifie facilement que c'est la complétion de $A[X]$ par rapport à l'idéal $XA[X]$. On dit que $A[[X]]$ est l'anneau des séries formelles de A en l'indéterminée X.

Exercice. Montrer que si $P \in A[X]$ est premier à X alors $c_{XA[X]}(P) \in A[[X]]^\times$. En déduire qu'on a un isomorphisme canonique $\widehat{A[X]_{XA[X]}} \tilde{\to} A[[X]]$, où $A[X] \to A[[X]]$ est la complétion $XA[X]_{XA[X]}$-adique de $A[X]_{XA[X]}$.

8. Un peu de géométrie (Hors programme)

Deuxième partie 2. Modules sur un anneaux

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

9. Premières définitions et constructions

9.1. Définitions.

9.1.1. 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 $\cdot : A \times A \to A$ - 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.

9.1.2. *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 N, 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 $\phi^* B$ 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, $End_A(M)$ 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.

9.1.3. Si M est un A-module, un *sous A-module* de M est un sous-ensemble $M' \subset M$ tel que $am' + bn' \in M'$, $a, b \in A$, $m', n' \in M'$.

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 $I \subset A$ est un idéal et M un A-module, $IM := \{am \mid a \in I,\ m \in M\} \subset M$ est un sous-A-module.

9.2. 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

$$|\{i \in I \mid m_i \neq 0\}| < +\infty.$$

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 $f \circ \iota_i = f_i$, $i \in I$.

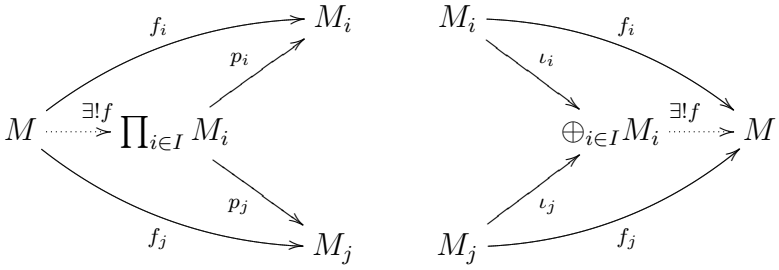
Démonstration. On vérifie comme d'habitude que les morphismes de A-modules $p_j : \prod_{i\in I} M_i \to M_j$, $j \in I$ et $\iota_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$, $j \in I$ construits ci-dessus conviennent. □

On peut aussi réécrire **??** 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 :



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

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

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 $f \circ \iota_i = \iota_i \circ f$, $i \in I$.

9.3. 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 $-\dot{x} : A \to M$, $x \in X$ nous donne un unique morphisme de A-modules $p_X : A^{(X)} \to M$ tel que $p \circ \iota_x(a) = ax$, $x \in X$. On vérifie immédiatement que les propri 'etés 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 $p \circ \iota_i(m_i) = m_i$, $m_i \in M_i$, $i \in I$.

9.4. 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

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

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,

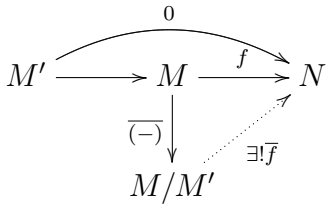
9.4.1. Lemme. (Propriété universelle du quotient) *Pour tout sous-A-module $M' \subset M$ il existe un morphisme de A-modules $p : M \to Q$ tel que pour tout morphisme de A-modules $f : M \to N$ tels que $M' \subset \ker(f)$, il existe unique morphisme de A-modules $\overline{f} : Q \to N'$ tel que $\overline{f}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

Démonstration. On vérifie comme d'habitude que le morphisme de A-modules $p_M : M \twoheadrightarrow M/M'$ construit ci-dessus convient. □

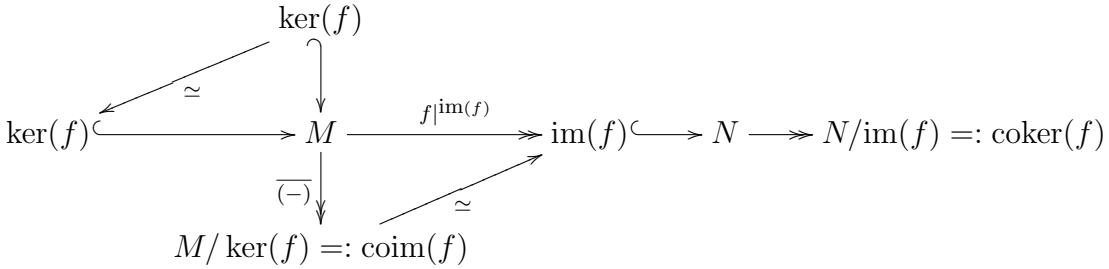
On peut aussi réécrire **??** en disant que, pour tout A-module N le morphisme canonique

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

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 $\mathrm{coker}(f) := M'/\mathrm{im}(f)$ (conoyaux).

9.4.2. 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'').

??.1 **Lemme.** *Soit*

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

une suite exacte courte de A-modules. Montrer que 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 $s : M' \to M'$ tel que $s \circ u = Id_{M'}$;

(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*.

Démonstration. 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 $vs(m) = vf^{-1}\iota_{M''} = p_{M''}\iota_{M''} = Id_{M''}$. □

??.2 **Exemple.**

(1) Si $n \geq 2$ est un entier, la suite de $\mathbb{Z}$-modules $0 \to \mathbb{Z} \xrightarrow{n.} \mathbb{Z} \to \mathbb{Z}/n \to 0$ n'est pas scindée.

(2) On considère les structure de $\mathbb{Z}[X]$-modules suivantes sur $\mathbb{Z}^2$

(a) $X \cdot (a, b) = (b, a)$

(b) $X \cdot (a, b) = (a + b, b)$

Dans le cas (a), la suite exacte courte de $\mathbb{Z}[X]$-modules

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

est-elle scindée ? Même question avec dans le cas (b), la suite exacte courte de $\mathbb{Z}[X]$-modules

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

??.3 **Exercice.** (Lemme du serpent)

(1) 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. Montrer que $u' : M' \to M$ induit un morphisme canonique $\ker(\alpha') \to \ker(\alpha)$ et que $v' : N' \to N$ induit un morphisme canonique $\mathrm{coker}(\alpha') \to \mathrm{coker}(\alpha)$.

(2) 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.

(a) Construire un morphisme 'naturel' $\delta : \ker(\alpha'') \to \mathrm{coker}(\alpha')$;

(b) Montrer que la suite de morphismes

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

est exacte.

(c) Montrer que si α', α'' sont injectives (resp. surjectives) alors α est injective (resp. surjective).

(d) 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.

(e) Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de groupes abéliens et soit p un nombre premier. Montrer qu'on a une suite exacte longue canonique de groupes abéliens

$$M'[p] \to M[p] \to M''[p] \to\to M'/p \to M/p \to M''/p \to 0,$$

(où on a noté $M[p] := \{m \in M \mid pm = 0\}$ et $M/p := M/(pM)$).

(3) 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.

(a) Montrer que si α_1 est surjective et α_2, α_4 sont injectives alors α_3 est injective.

(b) Montrer que si α_5 est injective et α_2, α_4 sont surjectives alors α_3 est surjective.

10. Conditions de finitude

Soit A un anneau commutatif.

10.1. 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 **??** est dit *noetherien*.

Démonstration. (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 **??** s'il l'est comme A-module sur lui-même.

10.2. 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 **??** est dit *artinien*. On laisse en exercice la preuve du Lemme **??**, qui est exactement similaire à celle du Lemme **??**

10.3. 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 (observer que les sous $\mathbb{Z}$-modules de $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ sont les $(\mathbb{Z}\frac{1}{p^n} + \mathbb{Z})/\mathbb{Z}$, $n \geq 0$).

(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.

10.4. 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). Montrer que tout module de type fini sur un anneau noethérien est de présentation finie.

Démonstration. (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.

10.5. 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.

Démonstration. (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

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

(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 $m = f^N(m) + m - f^N(m)$ mais ça ne marche pas. Il faut ajuster en utilisant que $\mathrm{im}(f^N) = \mathrm{im}(f^{2N})$ et donc qu'il existe $\mu \in M$ tel que $f^N(m) = f^{2N}(\mu)$. La décomposition $m = f^N(\mu) + m - f^N(\mu)$ elle, convient.

□

* * *

Syllabus prochaines séances :

Modules indécomposables, Krull-Schmidt
Modules de type fini sur les anneaux principaux

anna.cadoret@imj-prg.fr
IMJ-PRG, Sorbonne Université
Paris, FRANCE