

Algèbre et théorie de Galois

Anna Cadoret

Cours de Master 1 à Sorbonne Université - version 2019 (en cours d'actualisation)

18 novembre 2019

Table des matières

I	Anneaux - généralités	6
1	Premières définitions et constructions	7
1.1	Définitions	7
1.1.1	Monoides	7
1.1.2	Anneaux	8
1.1.3	Inversibles	8
1.1.4	Morphismes d'anneaux	9
1.1.5	Sous-anneaux	10
1.1.6	Algèbres	10
1.2	Produits	12
1.2.1	Produit d'anneaux	12
1.2.2	Anneau des fonctions	14
1.3	Algèbres de polynômes	15
1.3.1	Construction de $A[X]$	15
1.3.2	Construction de $A[N]$	18
1.3.3	Exemples et autres constructions	19
1.3.4	Exercices	22
1.4	Sous-anneau engendré par une partie	23
1.5	Sous- A -algèbre engendrée par une partie	24
2	Idéaux et quotients	26
2.1	Définitions, premiers exemples	26
2.1.1	26
2.1.2	Idéal engendré par une partie, sommes d'idéaux	27
2.1.3	Produits d'idéaux	27
2.1.4	28
2.2	Quotient	28

2.3	Corps et idéaux maximaux	32
2.3.1	Anneaux intègres et idéaux premiers	33
2.3.2	Anneaux réduits et idéaux radiciels	35
2.3.3	36
3	Anneaux noethériens	37
3.1	Lemme	37
3.2	Exemples	38
3.3	Proposition	38
3.4	Corollaire	39
3.5	Exercices	39
4	Anneaux principaux, euclidiens	41
4.1	41
4.2	Exemples	41
4.3	Lemme	43
4.4	Exercice	43
4.5	Lemme	43
5	Anneaux factoriels	45
5.1	Éléments irréductibles, éléments premiers	45
5.2	Proposition	48
5.3	Polynômes sur les anneaux factoriels	50
5.3.1	50
5.3.2	Valuations p -adiques	52
5.3.3	Contenu	53
5.3.4	54
5.3.5	55
5.3.6	56
5.4	Valuations et anneaux factoriels	57
5.4.1	Définitions et anneaux de valuation discrète	57
5.4.2	Factorialité	59
5.4.3	ppcm et pgcd	60
6	Localisation, anneaux de fractions.	62
6.1	Localisations	62
6.1.1	Parties multiplicatives	62

6.1.2	Définition	62
6.1.3	Propriété universelle	64
6.1.4	Morphismes	67
6.2	Idéaux	68
7	Complétion (Hors programme)	71
7.1	Limites projectives	71
7.1.1	71
7.1.2	72
7.2	73
7.2.1	73
7.2.2	74
8	Un peu de géométrie (Hors programme)	76
II	Modules sur un anneaux	80
9	Premières définitions et constructions	82
9.1	Définitions	82
9.1.1	Exemples	83
9.2	Produits et sommes directes	84
9.3	Sous-module engendré par une partie, sommes	87
9.4	Quotients	88
9.4.1	Suites exactes, lemme du serpent, lemme des cinq	90
10	Conditions de finitude	94
10.1	Lemme	94
10.2	Lemme	95
10.3	Exemple	95
10.4	Lemme	96
10.5	Lemme	97
11	Modules indécomposables, Krull-schmidt	99
11.1	Modules indécomposables	99
11.2	99
11.3	Théorème de Krull-Schmidt	100
11.3.1	100

11.3.2	102
12 Modules de type fini sur les anneaux principaux	103
12.1 Préambule	103
12.2 Classification des A -modules de type fini sans torsion	105
12.3 Classification des A -modules de type fini de torsion	107
12.3.1	110
12.4 Applications	111
12.4.1 Classification des groupes abéliens de type fini	111
12.4.2	111
12.4.3	112
13 Produit tensoriel	115
13.1 Construction	115
13.1.1	116
13.2 Propriétés élémentaires	117
13.2.1	117
13.2.2	117
13.2.3	118
13.2.4	118
13.2.5	119
13.3 Adjonctions	119
13.3.1	119
13.3.2	120
13.4 Produit tensoriel de A -algèbres	124
13.4.1	125
13.4.2	125

Bibliographie

- [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 $X \twoheadrightarrow Y$, $X \hookrightarrow Y$, $X \xrightarrow{\sim} Y$ (ou $X \xrightarrow{\cong} Y$) pour une application ensembliste $X \rightarrow Y$ 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

Anneaux - généralités

Chapitre 1

Premières définitions et constructions

1.1 Définitions

1.1.1 Monoïdes

Définition 1.1.1 (Monoïde et groupe). On rappelle qu'un monoïde est un couple (M, \times) formé d'un ensemble M et d'une application $\times : M \times M \rightarrow M$ 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 $m \cdot n = e_M = n \cdot m$.

Définition 1.1.2 (Morphisme). Étant donnés deux monoïdes M, N , un morphisme de monoïdes est une application $\phi : M \rightarrow N$ 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 $\text{Id} : M \rightarrow M$ est un morphisme de monoïdes et que si $\phi : L \rightarrow M$ et $\psi : M \rightarrow N$ sont des morphismes de monoïdes alors $\psi \circ \phi : L \rightarrow N$ est un morphisme de monoïdes.

Définition 1.1.3. On notera $\text{Hom}_{\text{Mono}}(M, N)$ l'ensemble des morphismes de monoïdes $\phi : M \rightarrow N$ et, si $M = N$, $\text{End}_{\text{Mono}}(M) := \text{Hom}_{\text{Mono}}(M, M)$. Étant donnés deux groupes M, N ,

un morphisme de groupes $\phi : M \rightarrow N$ est un morphisme entre les monoïdes sous-jacents. Dans ce cas, on notera plutôt $\text{Hom}_{Grp}(M, N)$ et $\text{End}_{Grp}(M)$ que $\text{Hom}_{Mono}(M, N)$, $\text{End}_{Mono}(M, N)$.

Définition 1.1.4. 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 Anneaux

Définition 1.1.5. Un anneau est un triplet $(A, +, \cdot)$ formé d'un ensemble A et de deux applications $+, \cdot : A \times A \rightarrow A$ - 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.

Définition 1.1.6. Un anneau A est dit commutatif si $ab = ba$, $a, b \in A$.

1.1.3 Inversibles

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 $a \in A^\times$.

Définition 1.1.7. 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 1.1.8. — 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 $\text{End}_{\text{Grp}}(M)$ 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, $\text{End}_{\text{Grp}}(M)^\times = \text{Aut}_{\text{Grp}}(M)$.
- Si M est un espace vectoriel sur un corps commutatif k , l'ensemble $\text{End}_k(M)$ 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, $\text{End}_k(M)^\times = \text{GL}_k(M)$.
- 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 Morphismes d'anneaux

Définition 1.1.9. Étant donnés deux anneaux A, B , un morphisme d'anneaux est une application $\phi : A \rightarrow B$ qui induit à la fois un morphisme de groupes $\phi : (A, +) \rightarrow (B, +)$ et de monoides unitaires $\phi : (A, \cdot) \rightarrow (B, \cdot)$ *i.e* qui vérifie :

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

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

On dit qu'un morphisme d'anneaux $\phi : A \rightarrow B$ est injectif, (resp. surjectif, resp. un isomorphisme) si l'application d'ensembles sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $\phi : A \rightarrow B$ est un isomorphisme d'anneaux l'application inverse $\phi^{-1} : B \rightarrow A$ est automatiquement un morphisme d'anneaux. Comme un morphisme d'anneaux $\phi : A \rightarrow B$ est en particulier un morphisme de groupes, $\phi : A \rightarrow B$ est injectif si et

seulement si $\ker(\phi) := \phi^{-1}(0_B) = \{0_A\}$. On notera aussi $\operatorname{im}(\phi) := \phi(A)$.

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

1.1.5 Sous-anneaux

Si A est un anneau, un sous-anneau de A est un sous-ensemble $A' \subset A$ tel que $1_A \in A'$ et $a' - b' \in A'$, $a' \cdot b' \in A'$, $a', b' \in A'$.

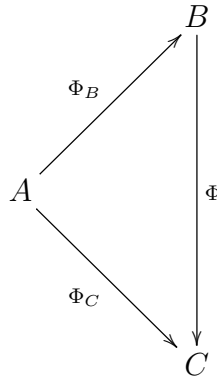
Exemples 1.1.10. — \mathbb{Z} est un sous anneau de \mathbb{Q} , \mathbb{Q} est un sous-anneau de \mathbb{R} , \mathbb{R} est un sous-anneau de \mathbb{C} .

- Si M est un espace vectoriel sur un corps commutatif k , $\operatorname{End}_k(M)$ est un sous-anneau de $\operatorname{End}_{\operatorname{Grp}}(M)$.
- $Z(A) := \{a \in A \mid a \cdot b = b \cdot a, b \in A\} \subset A$ est un sous-anneau de A , appelé le centre de A . Par exemple $Z(\operatorname{End}_k(M)) = k \operatorname{Id}_M$ et $Z(A) = A$ si et seulement si A est commutatif.
- Si $\phi : A \rightarrow B$ 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, $\operatorname{im}(\phi) \subset B$ 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 Algèbres

Définition 1.1.11. Soit A un anneau commutatif. Une A -algèbre est un couple (B, ϕ) où B est un anneau et $\phi : A \rightarrow B$ est un morphisme d'anneaux tel que $\operatorname{im}(\phi) \subset Z(B)$. On notera en général $\phi : A \rightarrow B$ ou simplement (lorsque la donnée de $\phi : A \rightarrow B$ ne peut prêter à confusion) B la A -algèbre (B, ϕ) .

Définition 1.1.12. Étant données deux A -algèbres $\phi_B : A \rightarrow B$, $\phi_C : A \rightarrow C$, un morphisme de A -algèbres est un morphisme d'anneaux $\phi : B \rightarrow C$ tel que $\phi \circ \phi_B = \phi_C$.



On remarquera que l'application identité $\text{Id} : B \rightarrow B$ est un morphisme de A -algèbres et que si $\phi : B \rightarrow C$ et $\psi : C \rightarrow D$ sont des morphismes de A -algèbres alors $\psi \circ \phi : B \rightarrow D$ est un morphisme de A -algèbres. On notera $\text{Hom}_A(B, C)$ l'ensemble des morphismes de A -algèbres $\phi : B \rightarrow C$ et, si $B = C$, $\text{End}_A(B) := \text{Hom}_A(B, C)$. On dit encore qu'un morphisme de A -algèbres $\phi : B \rightarrow C$ est injectif, (resp. surjectif, resp. un isomorphisme) si l'application d'ensembles sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $\phi : B \rightarrow C$ est un isomorphisme de A -algèbres l'application inverse $\phi^{-1} : C \rightarrow B$ est automatiquement un morphisme de A -algèbres.

Remarque 1.1.13. On verra dans la partie II du cours, qu'une A -algèbre $\phi : A \rightarrow B$ 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 1.1.14 (Caractéristique). — Le morphisme caractéristique $c_A : \mathbb{Z} \rightarrow A$, $1 \rightarrow 1_A$ munit tout anneau A d'une structure de \mathbb{Z} -algèbre canonique et tout morphisme d'anneaux $\phi : A \rightarrow B$ 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 $\phi : A \rightarrow B$ munit B d'une structure de A -algèbre.

Exercice 1.1.15 (Quaternions). On considère le \mathbb{R} -espace vectoriel \mathbb{H} de base $1, i, j, k$ muni du

produit $\mathbb{H} \times \mathbb{H} \rightarrow \mathbb{H}$ 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

1.2.1 Produit d'anneaux

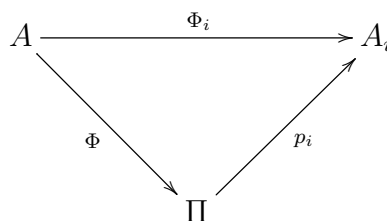
Si A_i , $i \in I$ est une famille d'anneaux, on peut munir le produit ensembliste $\prod_{i \in I} A_i$ d'une structure d'anneau en posant, pour $\underline{a} = (a_i)_{i \in I}$, $\underline{b} = (b_i)_{i \in I} \in \prod_{i \in I} A_i$

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

On a alors $0 = (0_{A_i})_{i \in I}$, $1 = (1_{A_i})_{i \in I}$. De plus, les projections $p_i : \prod_{i \in I} A_i \rightarrow A_i$, $\underline{a} \rightarrow a_i$, $i \in I$ sont automatiquement des morphismes d'anneaux.

1.2.1.1

Lemme 1.2.1 (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 $p_i : \Pi \rightarrow A_i$, $i \in I$ tels que pour tout anneau A et famille de morphisme d'anneaux $\phi_i : A \rightarrow A_i$, $i \in I$, il existe un unique morphisme d'anneaux $\phi : A \rightarrow \Pi$ tel que $p_i \circ \phi = \phi_i$, $i \in I$.*



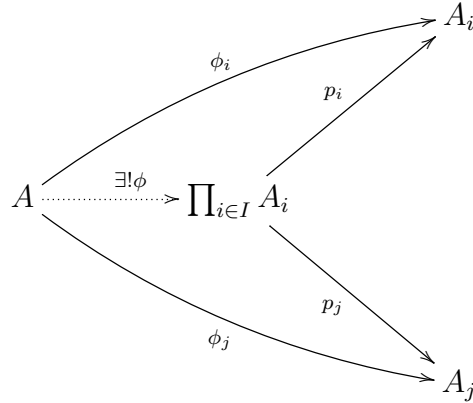
Démonstration. Vérifions que $\Pi := \prod_{i \in I} A_i$ et les $p_i : \prod_{i \in I} A_i \rightarrow A_i, a \mapsto a_i, i \in I$ conviennent. Si $\phi : A \rightarrow \prod_{i \in I} A_i$ existe, la condition $p_i \circ \phi = \phi_i, i \in I$ force $\phi(a) = (\phi_i(a))_{i \in I}, a \in A$. Cela 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. \square

Remarque 1.2.2. On peut aussi réécrire 1.2.1 en disant que, pour tout anneau A l'application canonique

$$\begin{aligned} \text{Hom}(A, \prod_{i \in I} A_i) &\rightarrow \prod_{i \in I} \text{Hom}(A, A_i) \\ \phi &\mapsto (p_i \circ \phi)_{i \in I} \end{aligned}$$

est bijective.

Plus visuellement :



Remarque 1.2.3 (Unicité). Supposons que l'on ait un autre anneau Π' et une famille de morphisme d'anneaux $p'_i : \Pi' \rightarrow A_i, i \in I$ vérifiant aussi la propriété du Lemme 1.2.1.1. On a alors, formellement :

1. un unique morphisme d'anneaux $\phi : \Pi \rightarrow \Pi'$ tel que $p'_i \circ \phi = p_i, i \in I$;
2. un unique morphisme d'anneaux $\phi' : \Pi' \rightarrow \Pi$ tel que $p_i \circ \phi' = p'_i, i \in I$;
3. un unique morphisme d'anneaux $\psi : \Pi \rightarrow \Pi$ tel que $p_i \circ \psi = p_i, i \in I$;
4. un unique morphisme d'anneaux $\psi' : \Pi' \rightarrow \Pi'$ tel que $p'_i \circ \psi' = p'_i, i \in I$.

Mais on voit que dans (3) $\psi = \phi' \circ \phi$ et $\psi = \text{Id}_\Pi$ conviennent. L'unicité de ψ dans (3) impose donc $\phi' \circ \phi = \text{Id}_\Pi$. Le même argument dans (4) montre que $\phi \circ \phi' = \text{Id}_{\Pi'}$. Autrement dit, les morphismes d'anneaux $\phi : \Pi \rightarrow \Pi'$ de (1) et $\phi' : \Pi' \rightarrow \Pi$ de (2) sont inverses l'un de l'autre.

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

Soit $\phi_i : A_i \rightarrow B_i$, $i \in I$ une famille de morphismes d'anneaux. En appliquant la propriété universelle des $p_j : \prod_{i \in I} B_i \rightarrow B_j$, $j \in I$ 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 $\phi := \prod_{i \in I} \phi_i : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$ tel que $p_i \circ \phi = \phi_i \circ p_i$, $i \in I$.

$$\begin{array}{ccc} A_i & \xrightarrow{\phi_i} & B_i \\ \pi_i^A \uparrow & & \uparrow \pi_i^B \\ \prod_{i \in I} A_i & \xrightarrow{\Phi} & \prod_{i \in I} B_i \end{array}$$

1.2.2 Anneau des fonctions

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 $a : I \rightarrow A$ 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

$$\begin{aligned} \Delta_A : A &\hookrightarrow A^I \\ a &\mapsto (i \mapsto a(i) = a) \end{aligned}$$

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 $\text{supp}(\underline{a}) := \{i \in I \mid a_i \neq 0\} \subset I$ le *support* de \underline{a} . Notons

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

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.

1.3.1 Construction de $A[X]$

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 monoïde 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

$$\left(\sum_{n \in \mathbb{N}} a_n e_n \right) * \left(\sum_{n \in \mathbb{N}} b_n e_n \right) = \sum_{n \in \mathbb{N}} \left(\sum_{i,j \in \mathbb{N}, i+j=n} a_i b_j \right) e_n \quad (1.1)$$

On vérifie facilement que $(A^{(\mathbb{N})}, +, *)$ est un anneau commutatif ayant pour unité e_0 . L'application canonique $\iota_A : A \rightarrow A^{(\mathbb{N})}$, $a \rightarrow ae_0$ est un morphisme d'anneaux. On note traditionnellement cet anneau $(A[X], +, \cdot)$ et on dit que $\iota : A \rightarrow A[X]$ est la A -algèbre des polynômes à une indéterminée. On pose aussi $X^n := e_n$, $n \in \mathbb{N}$ et $1 := X^0$ de sorte que (1.3.1) se réécrit de façon plus intuitive sous la forme :

$$\left(\sum_{n \in \mathbb{N}} a_n X^n \right) \left(\sum_{n \in \mathbb{N}} b_n X^n \right) = \sum_{n \in \mathbb{N}} \left(\sum_{i,j \in \mathbb{N}, i+j=n} a_i b_j \right) X^n. \quad (1.2)$$

Lemme 1.3.1 (Propriété universelle de la A -algèbre des polynômes à une indéterminée). *Pour tout anneau commutatif A , il existe une A -algèbre $\iota_A : A \rightarrow P$ munie d'un élément $p \in P$ tels que pour toute A -algèbre $\phi : A \rightarrow B$ et $b \in B$, il existe un unique morphisme de A -algèbres $ev_b^\phi : P \rightarrow B$ tel que $ev_b^\phi(p) = b$.*

$$\begin{array}{ccc}
 A & \xrightarrow{\varphi} & (B, b) \\
 & \searrow \iota_A & \nearrow ev_b^\phi \\
 & (P, p) &
 \end{array}$$

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

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

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. \square

Remarque 1.3.2. Le même argument formel que celui utilisé dans 1.2.1.2 montre que la A -algèbre $\iota_A : A \rightarrow A[X]$ est unique à unique isomorphisme près.

Remarque 1.3.3. On peut aussi réécrire 1.3.3 en disant que, pour toute A -algèbre $\phi : A \rightarrow B$ l'application canonique

$$\begin{aligned}
 \text{Hom}_A(A[X], B) &\rightarrow B \\
 f &\mapsto f(X)
 \end{aligned}$$

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

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

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

$$\begin{array}{ccc}
 A & \xrightarrow{\Phi} & B \\
 \downarrow \iota_A & & \downarrow \iota_B \\
 A[X] & \xrightarrow{\tilde{\Phi}} & B[X]
 \end{array}$$

Remarque 1.3.4. 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

$$\text{Hom}_{\text{Mono}}(\mathbb{N}, M) \rightarrow M, f \rightarrow f(1)$$

est bijective d'inverse l'application qui à $m \in M$ associe le morphisme de monoïdes $f_m : (\mathbb{N}, +) \rightarrow (M, \cdot)$, $n \rightarrow m^n (= m \cdots m \text{ } n \text{ fois})$. Dans 1.3.3, se donner $p \in P$ et $b \in B$ revient donc à se donner des morphismes de monoïdes $\nu_A : (\mathbb{N}, +) \rightarrow (P, \cdot)$, $n \rightarrow p^n$ et $\nu : (\mathbb{N}, +) \rightarrow (B, \cdot)$, $n \rightarrow b^n$ 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 1.3.3 comme suit.

Lemme 1.3.5 (Propriété universelle de la A -algèbre des polynômes à une indéterminée bis). *Pour tout anneau commutatif A , il existe une A -algèbre $\iota_A : A \rightarrow P$ et un morphisme de monoïdes $\nu_A : (\mathbb{N}, +) \rightarrow (P, \cdot)$ tels que pour toute A -algèbre $\phi : A \rightarrow B$ et tout morphisme de monoïdes $\nu : (\mathbb{N}, +) \rightarrow (B, \cdot)$, il existe un unique morphisme de A -algèbres $ev_b^\phi : P \rightarrow B$ tel que $ev_b^\phi \circ \nu_A = \nu$.*

$$\begin{array}{ccccc}
 & & B & & \\
 & \nearrow \Phi & & \nwarrow \nu & \\
 A & & & & \mathbb{N} \\
 & \searrow \iota_A & & \swarrow \nu_A & \\
 & & P & &
 \end{array}$$

ev (vertical arrow from B to P)

Ou encore : pour toute A -algèbre $\phi : A \rightarrow B$ l'application canonique

$$\text{Hom}_A(A[X], B) \rightarrow \text{Hom}_{\text{Mono}}(\mathbb{N}, B) \quad (1.3)$$

$$f \mapsto f \circ \nu_A. \quad (1.4)$$

est bijective. Explicitement, $\nu_A : (\mathbb{N}, +) \rightarrow (A[X], \cdot)$ est le morphisme qui envoie n sur X^n donc si $f : A[X] \rightarrow B$ est un morphisme de A -algèbres, $f \circ \nu_A : (\mathbb{N}, +) \rightarrow (B, \cdot)$ est le morphisme qui envoie n sur $f(X)^n$.

1.3.2 Construction de $A[N]$

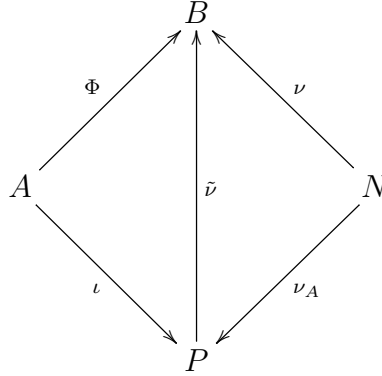
Avec le point de vue développé dans la remarque 1.3.4, on peut faire la construction précédente en remplaçant $(\mathbb{N}, +)$ par n'importe quel monoïde (N, \cdot) (non nécessairement commutatif, non nécessairement dénombrable) d'unité 1_N . Notons toujours $e_n := (\delta_{m,n} 1_A)_{m \in N}$, $n \in N$ 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 $\underline{a} = \sum_{n \in N} a_n e_n$. En munissant $A^{(N)}$ de l'addition héritée de celle de A^N et du produit 'de convolution' $*$ défini sur les éléments e_n , $n \in N$ par $e_m * e_n = e_{m \cdot n}$ et en général par

$$\left(\sum_{n \in N} a_n e_n \right) * \left(\sum_{n \in N} b_n e_n \right) = \sum_{n \in N} \left(\sum_{i, j \in N, i \cdot j = n} a_i b_j \right) e_n \quad (1.5)$$

on obtient un anneau (commutatif si (N, \cdot) est commutatif) $(A^{(N)}, +, *)$ ayant pour unité e_{1_N} . L'application canonique $\iota_A : A \rightarrow A^{(N)}$, $a \rightarrow ae_{1_N}$ est un morphisme d'anneaux et l'application $\nu_A : N \rightarrow A^{(N)}$, $n \rightarrow e_n$ prend ses valeurs dans $A^{(N)} \setminus \{0\}$ et induit un morphisme de monoïdes $\nu_A : (N, \cdot) \rightarrow (A^{(N)} \setminus \{0\}, *)$. On note traditionnellement cet anneau $(A[N], +, \cdot)$ et on dit que $\iota_A : A \rightarrow A[N]$ est la A -algèbre du monoïde (N, \cdot) . On pose aussi $n := e_n$, $n \in N$ et $1 := 1_N$ de sorte que (1.3.5) se réécrit de façon plus intuitive sous la forme

$$(1.3.7) \quad \left(\sum_{n \in N} a_n n \right) * \left(\sum_{n \in N} b_n n \right) = \sum_{n \in N} \left(\sum_{i, j \in N, i \cdot j = n} a_i b_j \right) n.$$

Lemme 1.3.6 (Propriété universelle de la A -algèbre du monoïde (N, \cdot)). *Pour tout anneau commutatif A , il existe une A -algèbre $\iota_A : A \rightarrow P$ et un morphisme de monoïdes $\nu_A : (N, \cdot) \rightarrow (P, \cdot)$ tels que pour toute A -algèbre $\phi : A \rightarrow B$ et tout morphisme de monoïdes $\nu : (N, \cdot) \rightarrow (B, \cdot)$ il existe un unique morphisme de A -algèbres $\tilde{\nu} : P \rightarrow B$ tel que $\tilde{\nu} \circ \iota_A = \nu$.*



Démonstration. Similaire à celle de 1.3.3 en vérifiant que $\iota_A : A \rightarrow A[N]$ convient. \square

Le même argument formel que celui utilisé dans 1.2.1.2 montre que la A -algèbre $\iota_A : A \rightarrow A[N]$ est unique à unique isomorphisme près.

Remarque 1.3.7. On peut aussi réécrire 1.3.8 en disant que, pour toute A -algèbre $\phi : A \rightarrow B$ l'application canonique

$$\text{Hom}_A(A[N], B) \rightarrow \text{Hom}_{\text{Mono}}(N, B), \quad f \rightarrow f \circ \nu_A$$

est bijective. Son inverse est l'application qui à $\nu : (N, \cdot) \rightarrow (B, \cdot)$ associe l'unique morphisme de A -algèbres $\tilde{\nu} : A[N] \rightarrow B$ tel que $\tilde{\nu}(n) = \nu(n)$ (donc $\tilde{\nu}(\sum_{n \in N} a_n n) = \sum_{n \in N} \phi(a_n) \nu(n)$).

1.3.3 Exemples et autres constructions

Remarque 1.3.8. Si $(N, \cdot) = (\mathbb{N}, +)$, on retrouve $A[\mathbb{N}] = A[X]$

Soit (N, \cdot) un monoïde et $\phi : A \rightarrow B$ un morphisme d'anneaux commutatifs. La propriété universelle de $\iota_A : A \rightarrow A[N]$ appliquée avec $A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[N]$ donne un unique morphisme de A -algèbres $\tilde{\phi} : A[N] \rightarrow B[N]$ 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, $\text{im}(\tilde{\phi}) = \text{im}(\phi)[N] \subset B[N]$ 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 $\ker(\phi)[N] := \ker(\tilde{\phi}) \subset A[N]$.

$$\begin{array}{ccc}
A & \xrightarrow{\Phi} & B \\
\downarrow \iota_A & & \downarrow \iota_B \\
A[N] & \xrightarrow{\bar{\Phi}} & B[N]
\end{array}$$

Définition 1.3.9. Pour (N, \cdot) un groupe, pour toute A -algèbre $\phi : A \rightarrow B$, tout morphisme de monoïdes $\nu : (N, \cdot) \rightarrow (B, \cdot)$ 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) .

1.3.3.1 Polynômes à plusieurs indéterminées

Posons $(N, \cdot) = (\mathbb{N}^r, +)$, 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 (1.3.5) se réécrit de façon plus intuitive sous la forme

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

On note également $A[X_1, \dots, X_r] := A[\mathbb{N}^r]$ et on dit que $\iota_A : A \rightarrow A[X_1, \dots, X_r]$ est la A -algèbre des polynômes à r indéterminées. Comme se donner un morphisme de monoïdes $\nu : (\mathbb{N}^r, +) \rightarrow (B, \cdot)$ 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 1.3.7 de la façon suivante.

Définition 1.3.10 (Morphisme d'évaluation). Pour toute A -algèbre $\phi : A \rightarrow B$, notons :

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

$$\begin{aligned}
\text{Hom}_A(A[X_1, \dots, X_r], B) &\rightarrow \mathfrak{B}_r \\
f &\mapsto (f(X_1), \dots, f(X_r))
\end{aligned}$$

Cette application est bijective et 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 $ev_{\underline{b}}^\phi : A[X_1, \dots, X_r] \rightarrow B$ 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} .

1.3.3.2 Polynômes de Laurent à une indéterminée

Prenons cette fois le groupe $(N, \cdot) = (\mathbb{Z}, +)$, on obtient la A -algèbre (notations : $A[X, X^{-1}] := A[\mathbb{Z}]$, $X^n := e_n$, $n \in \mathbb{Z}$ donc en particulier $X^n X^{-n} = e_n e_{-n} = e_{n-n} = e_0 = 1$) des polynômes de Laurent à une indéterminée. Comme se donner un morphisme de monoïdes $\nu : (\mathbb{Z}, +) \rightarrow (B, \cdot)$ revient à se donner l'image $b \in B^\times$ de $1 \in \mathbb{Z}$, on peut reformuler 1.3.7 de la façon suivante.

Définition 1.3.11 (Morphisme d'évaluation). Pour toute A -algèbre $\phi : A \rightarrow B$, l'application canonique

$$\begin{aligned} \text{Hom}_A(A[X, X^{-1}], B) &\rightarrow B^\times \\ f &\mapsto f(X) \end{aligned}$$

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

1.3.3.3 Polynômes de Laurent à plusieurs indéterminées

De même, pour $(N, \cdot) = (\mathbb{Z}^r, +)$, on obtient la A -algèbre (notations : $A[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}] := A[\mathbb{Z}^r]$, $\underline{X}^{\underline{n}} := X_1^{n_1} \cdots X_r^{n_r} := e_{\underline{n}}$, $\underline{n} \in \mathbb{Z}^r$ 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 $\nu : (\mathbb{Z}^r, +) \rightarrow (B, \cdot)$ 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 1.3.8 de la façon suivante.

Définition 1.3.12 (Morphisme d'évaluation). Pour toute A -algèbre $\phi : A \rightarrow B$, en notant

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

l'application canonique

$$\begin{aligned} \text{Hom}_A(A[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}], B) &\rightarrow \mathfrak{B}_r^\times \\ f &\rightarrow (f(X_1), \dots, f(X_r)) \end{aligned}$$

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 $ev_{\underline{b}}^\phi : A[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}] \rightarrow B$ tel que $ev_{\underline{b}}^\phi(X_i) = b_i$, $i = 1, \dots, r$ (donc $ev_{\underline{b}}^\phi(\sum_{\underline{n} \in \mathbb{Z}^r} a_{\underline{n}} X_{\underline{n}}) = \sum_{\underline{n} \in \mathbb{Z}^r} \phi(a_{\underline{n}}) \underline{b}^{\underline{n}}$)

1.3.4 Exercices

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

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

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

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

L'injectivité de $\tilde{-} : \text{Hom}_{\text{Mono}}(N_1, N_2) \rightarrow \text{Hom}_A(A[N_1], A[N_2])$ résulte de l'injectivité des $\nu_A : N_i \rightarrow A[N_i]$, $i = 1, 2$. Enfin, le fait que $\tilde{-} : \text{Hom}_{\text{Mono}}(N_1, N_2) \rightarrow \text{Hom}_A(A[N_1], A[N_2])$ 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 $\sum_{n \in N} a e_n$ (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 $\tilde{\nu}(X_i) = Z_i$, $\tilde{\nu}(Y_i) = Z_i^{-1}$, $i = 1, \dots, r$.

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

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

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 $\iota_A : A \rightarrow A[X_1, \dots, X_r]$ et $A \xrightarrow{\iota_A} A[X_1, \dots, X_{r-1}] \xrightarrow{\iota_{A[X_1, \dots, X_{r-1}]}} A[X_1, \dots, X_{r-1}][X_r]$ vérifie la même propriété universelle. Notons que par hypothèse $A[b_1, \dots, b_r]$ est un anneau commutatif (cf. 1.5 pour la notation $A[b_1, \dots, b_{r-1}]$). Soit donc $\phi : A \rightarrow B$ une A -algèbre et $b_1, \dots, b_r \in B^r$ commutant deux à deux. Par la propriété universelle de $\iota_A : A \rightarrow A[X_1, \dots, X_{r-1}]$, il existe un unique morphisme de A -algèbre $ev_{(b_1, \dots, b_{r-1})}^\phi : A[X_1, \dots, X_{r-1}] \rightarrow B$ tel que $\phi_1(X_i) := ev_{(b_1, \dots, b_{r-1})}^\phi(X_i) = b_i$, $i = 1, \dots, r-1$. Puis, par la propriété universelle de $\iota_{A[X_1, \dots, X_{r-1}]} : A[X_1, \dots, X_{r-1}] \rightarrow A[X_1, \dots, X_r]$, il existe un unique morphisme de A -algèbre $ev_{b_r}^{\phi_1} : A[X_1, \dots, X_{r-1}][X_r] \rightarrow A[b_1, \dots, b_{r-1}][b_r] = A[b_1, \dots, b_r]$ tel que $ev_{b_r}^{\phi_1}(X_r) = b_r$... 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 $\bigcap_{i \in I} A_i \subset A$ 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 $\langle X \rangle \subset A'$.

Définition 1.4.1. 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 .

Définition 1.4.2. 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.

Définition 1.4.3. 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 1.3.8 nous donne un unique morphisme d'anneaux - automatiquement surjectif - $ev_{\underline{x}} : \mathbb{Z}[X_1, \dots, X_r] \rightarrow \mathbb{Z}[x_1, \dots, x_r]$ tel que $ev_{\underline{x}}(X_i) = x_i$, $i = 1, \dots, r$.

1.5 Sous- A -algèbre engendrée par une partie

Soit $\phi : A \rightarrow B$ une A -algèbre.

Définition 1.5.1. Une sous- A -algèbre de $\phi : A \rightarrow B$ est un sous-anneau $B' \subset B$ tel que $\text{im}(\phi) \subset B'$ (noter que $Z(B) \cap B' \subset Z(B')$)

Le morphisme $\phi|^{B'} : A \rightarrow B'$ 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, $\bigcap_{i \in I} B_i \subset B$ 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

Définition 1.5.2. 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 $X \cup \text{im}(\phi)$.

Définition 1.5.3. 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 1.3.8 nous donne un unique morphisme de A -algèbres - automatiquement surjectif - $ev_{\underline{x}}^\phi : A[X_1, \dots, X_r] \rightarrow A[x_1, \dots, x_r]$ tel que $ev_{\underline{x}}^\phi(X_i) = x_i$, $i = 1, \dots, r$.

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

Chapitre 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, $I[X_1, \dots, X_r] := \{\sum_{\underline{n} \in \mathbb{N}^r} a_{\underline{n}} X_{\underline{n}} \mid a_{\underline{n}} \in I\} \subset A[X_1, \dots, X_r]$ 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

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

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 $k[X_1, \dots, X_r]$ (et, partant, de toute k -algèbre de type fini) sont de type fini. Un anneau ayant cette propriété est dit noethérien. 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 $m_1, \dots, m_r \in \mathbb{Z}$, $m_1\mathbb{Z} \cdots m_r\mathbb{Z} = (m_1 \cdot m_r)\mathbb{Z}$, $m_1\mathbb{Z} \cap \cdots \cap m_r\mathbb{Z} = \text{ppcm}(m_1, \dots, m_r)\mathbb{Z}$, $m_1\mathbb{Z} + \cdots + m_r\mathbb{Z} = \text{pgcd}(m_1, \dots, m_r)\mathbb{Z}$. Les inclusions (*) ci-dessus correspondent aux relations de divisibilité

$$\text{pgcd}(m_1, \dots, m_r) | m_i | \text{ppcm}(m_1, \dots, m_r) | m_1 \cdots m_r.$$

2.1.4

Si $\phi : A \rightarrow B$ 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 $\phi : A \rightarrow B$ 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

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

se factorise en

$$\begin{array}{ccc} A \times A & \xrightarrow{(a,b) \rightarrow \overline{ab}} & A/I \\ \downarrow \overline{} \times \overline{} & \nearrow (\overline{a}, \overline{b}) \rightarrow \overline{a}\overline{b} = \overline{ab} & \\ A/I \times A/I & & \end{array}$$

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

$\bar{0}$ et d'unité $\bar{1}$.

2.2.1 Lemme. (Propriété universelle du quotient) *Pour tout idéal $I \subset A$ il existe un morphisme d'anneaux $p : A \rightarrow A/I$ tel que pour tout morphisme d'anneaux $\phi : A \rightarrow B$ avec $I \subset \ker(\phi)$, il existe un unique morphisme d'anneaux $\bar{\phi} : A/I \rightarrow B$ tel que $\phi = \bar{\phi} \circ p$.*

Démonstration. Montrons que A/I muni de la structure d'anneau ci-dessus et la projection canonique $\bar{-} : A \rightarrow A/I$ conviennent. Soit $\phi : A \rightarrow B$ un morphisme d'anneaux tel que $I \subset \ker(\phi)$. Si $\bar{\phi} : A/I \rightarrow B$ existe, la condition $\phi = \bar{\phi} \circ p$ force $\bar{\phi}(\bar{a}) = \phi(a)$, $a \in A$. Cela montre l'unicité de $\bar{\phi}$ sous réserve de son existence. Il reste à voir que $\bar{\phi} : A/I \rightarrow B$ 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 :

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

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

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

On peut aussi réécrire 2.2.1 en disant que, pour tout anneau B l'application canonique

$$SHom(A/I, B) \rightarrow \{A \xrightarrow{\phi} B \mid I \subset \ker(\phi)\}, \quad \bar{\phi} \mapsto \bar{\phi} \circ \bar{-}$$

est bijective ou encore, plus visuellement :

$$\begin{array}{ccccc} & & 0 & & \\ & \curvearrowright & & \curvearrowright & \\ I & \xrightarrow{\quad} & A & \xrightarrow{\quad \phi \quad} & B \\ & \downarrow \bar{(-)} & & \nearrow \exists! \bar{\phi} & \\ & & A/I & & \end{array}$$

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

forme

$$\begin{array}{ccccc}
 A & \xrightarrow{\phi|_{\text{im}(\phi)}} & \text{im}(\phi) & \hookrightarrow & B \\
 \downarrow \cong & & \nearrow \cong & & \\
 A/\ker(\phi) & & & &
 \end{array}$$

Exemples. (Caractéristique d'un anneau) Le noyau du morphisme caractéristique $c_A : \mathbb{Z} \rightarrow A$ 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 $\prod_{p \in \mathcal{P}} \mathbb{Z}/p\mathbb{Z}$ est de caractéristique 0.
- Si $\phi : A \rightarrow B$ 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 $A/J \xrightarrow{\sim} \overline{A}/\overline{J}$. En déduire qu'on a toujours un isomorphisme d'anneaux canonique $A/(I+J) \xrightarrow{\sim} \overline{A}/\overline{J}$.
2. Soit $I \subset A$ un idéal. Montrer qu'on a un isomorphisme de A -algèbres canonique $A[X]/I[X] \xrightarrow{\sim} (A/I)[X]$.
3. Soit $f_1, \dots, f_s \in A[X_1, \dots, X_r]$. Montrer que la A -algèbre quotient

$$A \rightarrow A[X_1, \dots, X_r] / \sum_{1 \leq i \leq s} f_i A[X_1, \dots, X_r]$$

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

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

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

$$A[X_1, Y_1, \dots, X_r, Y_r] / \sum_{1 \leq i \leq r} (X_i Y_i - 1) A[X_1, Y_1, \dots, X_r, Y_r] \xrightarrow{\sim} A[X_1, X_1^{-1}, \dots, X_r, X_r^{-1}].$$

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

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

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

2.2.3 Lemme. (Restes chinois) Si $I_i + I_j = A$, $1 \leq i \neq j \leq r$ alors $\cap_{1 \leq i \leq r} I_i = I_1 \cdots I_r$ et $p : A \rightarrow \prod_{1 \leq i \leq r} A/I_i$ est surjective. Inversement, si $p : A \rightarrow \prod_{1 \leq i \leq r} A/I_i$ 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 $p := \prod_{1 \leq i \leq r} p_{I_i} : A \rightarrow \prod_{1 \leq i \leq r} A/I_i$, 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 $i = 2, \dots, r$ il existe $a_i \in I_1$, $b_i \in I_i$ tels que $a_i + b_i = 1$. On a donc $1 = \prod_{2 \leq i \leq r} (a_i + b_i) = \prod_{2 \leq i \leq r} a_i + \cdots \in I_1 + I_2 \cdots I_r$.

Inversement, si $p : A \rightarrow \prod_{1 \leq i \leq r} A/I_i$ 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 $1 = (1 - x) + x \in I_i + I_j$. \square

2.3 Corps et idéaux maximaux

Le singleton $\{0\}$ et A sont des idéaux 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.

2.3.1 Lemme. *Les propositions suivantes sont équivalentes :* (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 $1 = a^{-1}a$. \square

2.3.2 Lemme. *Soit $I \subsetneq A$ un idéal. Les propositions suivantes sont équivalentes* (i) A/I est un corps ;
(ii) I est maximal dans

Démonstration. Cela résulte de 2.2.2. \square

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de 2.3.2 est *maximal*.

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

Démonstration. Il suffit d'observer que si $I_1 \subset I_2 \subset \dots \subsetneq A$ est une suite d'idéaux de A distincts de A et croissante pour \subset , $I := \cup_{n \geq 1} I_n \subsetneq A$ est encore un idéal de A distincts de A . En effet, pour tout $a, b \in I$ il existe n tel que $a, b \in I_n$ donc $a - b \in I_n \subset I$ et pour tout $\alpha \in A$, $\alpha a \in I_n \subset I$; cela montre déjà que $I \subset A$ est un idéal. Dans ce cas, $I = A$ si et seulement si $1 \in I$. Mais si $1 \in I$, il existerait $n \geq 1$ tel que $1 \in I_n$, ce qui n'est pas possible puisque par hypothèse $I_n \subsetneq A$. \square

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 $\text{spm}(A)$ l'ensemble des idéaux maximaux de A et on dit que c'est le *spectre maximal* de A . D'après 1.2.1.1, les projections canoniques $p_{\mathfrak{m}} : A \rightarrow A/\mathfrak{m}$, $\mathfrak{m} \in \text{spm}(A)$ induisent un morphisme d'anneaux canonique

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

dont le noyau $\mathcal{J}_A := \ker(p_{\max}) = \bigcap_{\mathfrak{m} \in \text{spm}(A)} \mathfrak{m} \subset A$ 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 $A_{\text{tors}} \subset A$ l'ensemble des éléments de torsion de A . On dit qu'un anneau A est *intègre* si $A_{\text{tors}} = \{0\}$.

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

2.3.1.1 Lemme. Soit $I \subsetneq A$ un idéal. Les propositions suivantes sont équivalentes

- (i) A/I est intègre ;
- (ii) Pour tout $a, b \in A$

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

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de 2.3.2 est *premier*. On notera $\text{Spec}(A)$ l'ensemble des idéaux premiers de A et on dit que c'est le *Spectre* de A . D'après 1.2.1.1, les projections canoniques $p_{\mathfrak{p}} : A \twoheadrightarrow A/\mathfrak{p}$, $\mathfrak{p} \in \text{Spec}(A)$ induisent un morphisme d'anneaux canonique

$$p_{\text{prem}} : A \rightarrow \prod_{\mathfrak{p} \in \text{Spec}(A)} A/\mathfrak{p}$$

dont le noyau $\mathcal{R}_A := \ker(p_{\text{prem}}) = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p} \subset A$ 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, $\mathcal{N}_A = \{0\}$.

2.3.1.2 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

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

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 morphisme d'anneaux $\phi : A \rightarrow B$ 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 $p_{\mathfrak{p}} : A \twoheadrightarrow A/\mathfrak{p}$, $\mathfrak{p} \in \text{Spec}(A)$, 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 $\mathfrak{p} \in \text{Spec}(A)$ 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 (Σ_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 \bar{a} l'image de a dans A/I . Par définition de I , $0 \notin X_{\bar{a}}$ mais pour tout idéal $\{0\} \subsetneq \bar{J} \subset A/I$, $X_{\bar{a}} \cap \bar{J} \neq \emptyset$. En particulier, pour tout $0 \neq \bar{b} \in A/I$, il existe $n_b \geq 1$ tel que $\bar{a}^{n_b} \in (A/I)\bar{b}$ donc pour tout $0 \neq \bar{b}, \bar{b}' \in A/I$, $\bar{a}^{n_b n_{b'}} \in (A/I)\bar{b}\bar{b}'$ donc $\bar{b}\bar{b}' \neq 0$. \square

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 $A[X_1, \dots, X_r]^\times$.

2.3.1.3 Exercice.

1. Soit $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 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, \dots, 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 n ème nombre premier, l'anneau $\prod_{n \geq 1} \mathbb{Z}/p_n^n$ n'est pas réduit et contient un élément d'indice de nilpotence n pour tout $n \geq 1$.

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

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

On dit que \sqrt{I} est la racine de I . Avec cette notation, $\mathcal{N}_A = \sqrt{\{0\}}$. Il résulte des définitions que pour un idéal $I \subsetneq A$ les propositions suivantes sont équivalentes

- (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

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

et

I	A/I
Maximal	Corps
Premier	Intègre
Radiciel	Réduit

Classification grossière des idéaux

2.3.3

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

$$\begin{array}{ccccc}
 A & \xrightarrow{\Phi} & B & \xrightarrow{p_I} & B/J \\
 & \searrow \pi_A & & \nearrow p_i \circ \Phi & \\
 & & A/\Phi^{-1}(J) & & \\
 \\
 (\mathcal{I}_B, \subset) & & \xrightarrow{\phi^{-1}} & & (\mathcal{I}_A, \subset) \\
 \cup & & & & \cup \\
 (\mathcal{I}_B^{red}, \subset) & & \xrightarrow{\phi^{-1}} & & (\mathcal{I}_A^{red}, \subset) \\
 \cup & & & & \cup \\
 (\text{Spec}(B), \subset) & & \xrightarrow{\phi^{-1}} & & (\text{Spec}(A), \subset)
 \end{array}$$

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.

Chapitre 3

Anneaux noethériens

3.1 Lemme

Lemme 3.1.1. *Soit A un anneau. Les propositions suivantes sont équivalentes.*

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 $I_0 \subset \dots \subset I_n \subset I_{n+1} \subset \dots \subset A$ 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 $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \dots$ d'éléments 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 . \square

Définition 3.1.2 (anneau noethérien). On dit qu'un anneau A qui vérifie les propriétés équivalentes du Lemme 3.1.1 est *noethérien*.

3.2 Exemples

- Exemple 3.2.1.** 1. Les anneaux principaux (*e.g.* k , \mathbb{Z} , $k[X]$, où k est un corps commutatif) sont noethériens.
2. Si k est un corps commutatif, une k -algèbre $\phi : k \rightarrow A$ est toujours munie d'une structure de k -espace vectoriel : $k \times A \rightarrow A$, $(\lambda, a) \rightarrow \phi(\lambda)a$. 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 noethérienne. Par exemple l'anneau $k[X]/X^n k[X]$ est un noethérien.
3. Tout quotient d'un anneau noethérien est noethérien. En effet, soit A est un anneau noethérien 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, \dots, a_r d'éléments. Mais alors, $J = p_I p_I^{-1}(J)$ est engendré par les $p_I(a_1), \dots, p_I(a_r)$.
4. Par contre un sous-anneau d'un anneau noethérien n'est pas forcément noethérien. Par exemple, on va voir (3.3.1) que si k est un corps commutatif, l'anneau $k[X_1, X_2]$ est noethérien mais la sous- k -algèbre engendrée par les $X_1 X_2^n$, $n \geq 0$ n'est pas un anneau noethérien.

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

3.3 Proposition

Proposition 3.3.1 (transfert de noethérianité). *A noethérien $\Rightarrow A[X]$ noethérien.*

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 dans I i.e. $a \in \mathfrak{I}_n$ si et seulement si il existe $a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + a X^n \in I$. Comme $I \subset A[X]$ est un idéal, les $\mathfrak{I}_n \subset A$ sont automatiquement des idéaux. De plus,

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

donc on a

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

Comme A est noethérien, cette suite devient stationnaire à partir d'un certain rang, disons n . De plus, chaque \mathfrak{I}_k est de type fini ; notons $a_{k,1}, \dots, a_{k,r_k} \in \mathfrak{I}_k$ un ensemble fini de générateurs

de \mathfrak{J}_k . Enfin, pour $k = 0, \dots, n$, $l = 1, \dots, r_k$, 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 $P_{k,l}$, $l = 1, \dots, r_k$, $k = 0, \dots, n$. 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 $\mathfrak{J}_0 \subset I^\circ$. Supposons que I° contient tous les éléments de I de degré $\leq d$. Soit $P = a_0 + \dots + a_d X^d + a_{d+1} X^{d+1} \in I$ de degré $d+1$. Si $d+1 \geq n$, on a $a_{d+1} \in \mathfrak{J}_{d+1} = \mathfrak{J}_n$ 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 $d+1 \leq n$, $a_{d+1} \in \mathfrak{J}_{d+1}$ donc on peut écrire $a_{d+1} = \sum_{1 \leq i \leq r_{d+1}} \alpha_i a_{d+1,i}$ et $P - \sum_{1 \leq i \leq r_{d+1}} \alpha_i P_{d+1,i}$ est encore dans I mais de degré $\leq d$ donc, par hypothèse de récurrence, dans I° . \square

3.4 Corollaire

Corollaire 3.4.1. *Si A est un anneau noethérien, toute A -algèbre de type fini est un anneau noethérien.*

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

$$A[X_1, \dots, X_n] \xrightarrow{\sim} A[X_1, \dots, X_{n-1}][X_n]$$

et la proposition 3.3.1 impliquent que $A[X_1, \dots, X_n]$ est un anneau noethérien. On conclut par l'exemple 3.2.1 (3) puisque toute A -algèbre de type fini est quotient d'une A -algèbre de la forme $A[X_1, \dots, X_n]$. \square

3.5 Exercices

Exercice 3.5.1. 1. Soit A un anneau noethérien. 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 propositions suivantes sont équivalentes

- (a) Toute suite d'idéaux de A décroissante pour \subset est stationnaire à partir d'un certain rang.
- (b) Tout sous-ensemble non vide d'idéaux de A admet un élément minimal pour \subset .

On dit qu'un anneau A qui vérifie les propriétés équivalentes ci-dessus est *artinien*. En dépit de la similitude des définitions, les anneaux artiniens et noethériens 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 noethérien.

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

Chapitre 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 - $\sigma : A \setminus \{0\} \rightarrow \mathbb{N}$ vérifiant la propriété suivante (division euclidienne) : pour tout $0 \neq a, b \in A$ il existe $q, r \in A$ tels que

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

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

4.2 Exemples

1. La valeur absolue usuelle $|-| : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ 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 $A[X_1, \dots, X_r]$ 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 $f = \sum_{n \in \mathbb{N}} a_n X^n$ avec $\underline{a} : n \rightarrow a_n \in A^{(\mathbb{N})}$. Cela permet de définir l'application degré :

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

et une application 'coefficient dominant'

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

La définition du produit dans $A[X]$ montre que $\deg(fg) \leq \deg(f) + \deg(g)$ et que si l'un au moins de $\text{CD}(f), \text{CD}(g)$ n'est pas de torsion dans A , $\deg(fg) = \deg(f) + \deg(g)$, $\text{CD}(fg) = \text{CD}(f) \text{CD}(g)$. 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 $\text{CD}(f) \in A^\times$. 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 $\deg(g)$. Écrivons $f = \sum_{0 \leq n \leq d_f} a_n X^n$, $g = \sum_{0 \leq n \leq d_g} b_n X^n$, où $d_f := \deg(f)$, $d_g := \deg(g)$. Si $d_g = 0$ et $d_f > 0$, $q = 0$ et $r = g$ conviennent. Si $d_g = d_f = 0$, $f = a_0 = a_{d_f} \in A^\times \subset A[X]^\times$ donc $q = f^{-1}g$ et $r = 0$ conviennent. Si $d_g \geq 1$ et $d_f > d_g$, $q = 0$ et $r = g$ conviennent. Supposons donc $d_f \leq d_g$. Comme $a_{d_f} \in A^\times$ on peut écrire

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

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

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

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

□

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

- $r \geq 1$. En utilisant les isomorphismes canoniques $A[X_1, \dots, X_r] \xrightarrow{\sim} A[X_1, \dots, \hat{X}_i, \dots, X_r][X_i]$, $i = 1, \dots, r$, on peut encore appliquer le Lemme ci-dessus dans $A[X_1, \dots, X_r]$: les polynômes par lesquels on peut diviser sont ceux de la forme $aX_i^d + \sum_{\underline{n} \in \mathbb{N}^r, |\underline{n}| < d} a_{\underline{n}} X^{\underline{n}}$, avec $a \in A[X_1, \dots, \hat{X}_i, \dots, X_r]^\times = A^\times$ (car A est intègre donc réduit).

3. On peut montrer que le carré de la valeur absolue usuelle $|\cdot|^2 : \mathbb{Z}[w] \rightarrow \mathbb{N}$ 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 $w = \sqrt{-1}, {}^3\sqrt{-1}, \sqrt{-2}$.

4.3 Lemme

Euclien \Rightarrow 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, $\text{spm}(A) = \text{Spec}(A) \setminus \{0\}$.

Démonstration. On a toujours $\text{spm}(A) \subset \text{Spec}(A)$. Soit $\mathfrak{p} = Ap \in \text{Spec}(A)$; on veut montrer que A/Ap est un corps. Supposons le contraire. Alors A/Ap contient un idéal maximal $\{\bar{0}\} \subsetneq \mathfrak{m} \subsetneq A/Ap$. Écrivons $p_{\mathfrak{p}}^{-1}(\mathfrak{m}) = Am$. 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 $a \in Ap$. Écrivons donc $a = bp$; on a $p = am = pbm$. Comme A est intègre, on peut simplifier par p pour obtenir $1 = bm$, ce qui contredit $Am \subsetneq A$. \square

Chapitre 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° 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 irréductibles de \mathbb{Z} sont les nombres premiers. Si l'on veut déterminer si un entier $n \in \mathbb{Z}_{\geq 1}$ est premier, on dispose d'un algorithme évident consistant à lister tous les premiers $\leq \sqrt{n}$ et vérifier s'ils divisent n mais cet algorithme devient très vite inutilisable sur machine. Les arithméticiens ont beaucoup étudié et étudient encore le problème de la construction et de la répartition des nombres premiers. L'une de leurs motivations est

l'application des nombres premiers en cryptographie. Parmi les énoncés classiques les plus spectaculaires, on trouve par exemple le théorème des nombres premiers, qui dit que si on note $\pi(n)$ le nombre de nombre premiers $0 \leq p \leq n$, on a $\pi(n) \sim_{n \rightarrow +\infty} \ln(n)/n$ 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 $Ap \in \text{Spec}(A)$. On notera $\mathcal{P}_A^\dagger \subset A$ l'ensemble des éléments premiers de A .

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

Démonstration. En effet, si $Ap \in \text{spec}(A)$, 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 $b \in A^\times$. \square

(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 $N : A \rightarrow \mathbb{Z}_{\geq 0}$, $a + ib\sqrt{5} \mapsto |a + ib\sqrt{5}|^2 = a^2 + 5b^2$. 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 $N(1 \pm i\sqrt{5}) = 6 \notin N(2A) = 4N(A) \subset 4\mathbb{Z}_{\geq 0}$.

5.1.2 On dit qu'un anneau commutatif intègre A est *factoriel* si pour tout système de représentants

\mathcal{P}_A de \mathcal{P}_A° l'application

$$(5.1.2.1) \quad \begin{aligned} A^\times \times \mathbb{N}^{(\mathcal{P}_A)} &\rightarrow A \setminus \{0\} \\ (u, \nu) &\rightarrow u \prod_{p \in \mathcal{P}_A} p^{\nu(p)} \end{aligned}$$

est bijective *i.e.* pour tout $0 \neq a \in A$ il existe une unique application $v_-(a) : \mathcal{P}_A \rightarrow \mathbb{N}$ 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 $v_-(a) : \mathcal{P}_A \rightarrow \mathbb{N}$ 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 .

5.1.3 Soit A un anneau factoriel. On prolonge les applications $v_p : A \setminus \{0\} \rightarrow \mathbb{N}$ en $v_p : A \rightarrow \overline{\mathbb{N}} := \mathbb{N} \cup \{\infty\}$ 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 $v_p : A \rightarrow \overline{\mathbb{N}}$, $p \in \mathcal{P}_A$ 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 $v_p(a'p^{v_p(a)-v_p(b)} + b') = 0$ 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

5.1.4 **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 $b \in Ap$. \square

5.2 Proposition

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

5.2.1 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 noetherien intègre, l'application*

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

est surjective.

Démonstration. Notons $\mathcal{F} \subset A$ l'image de $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \rightarrow A \setminus \{0\}$. Observons que \mathcal{F} est stable par produit et qu'il contient \mathcal{P}_A° , A^\times . Si $a \notin \mathcal{F}$, $a \notin \mathcal{P}_A$ donc il existe $a_1, a_2 \notin A^\times$ tels que $a = a_1 a_2$. 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 $Aa \subsetneq Aa_1 \subsetneq Aa_{1,1} \subsetneq Aa_{1,1,1} \subsetneq \dots$ d'idéaux de A , ce qui contredit la noetherianité de A . \square

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

Soit A un anneau principal. On sait déjà que A est intègre (par définition) et noethérien (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 $a \in I \setminus Ap$. Comme 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 $A = Ap + Aa \subset I$.

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

Par le Lemme 5.2.1, on sait déjà que l'application $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \rightarrow A \setminus \{0\}$ 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 $\nu(p) > 0$, $\bar{a} = 0$ dans A/p . Comme $p \in \mathcal{P}_A^\dagger$, A/p est intègre et comme $\bar{v} \in (A/p)^\times$, il existe forcément $q \in \mathcal{P}_A$ tel que $\bar{q} = 0$ dans A/p i.e. $q \in Ap$, ce qui force $q = p$ puisque p, q sont irréductibles : contradiction.

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

— 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, $Ap \in \text{Spec}(A)$ et comme $\text{spm}(A) = \text{Spec}(A)$ 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 $a \in I$ s'écrit 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) $-\cdot p : I \xrightarrow{\sim} I$. 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 , $p^{v_p(a)-1}b \in J = I = pI \Rightarrow p^{v_p(a)-2}b \in J = I = pI \Rightarrow \dots \Rightarrow b \in J = I = pI \Rightarrow v_p(b) \geq 1$.

□

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

5.2.2 (Contre-)Exemples. Les implications de 5.2 ne sont pas des équivalences. Par exemple,

— Anneau noethérien + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$ non principal : $k[X_1, X_2]$, où k est un corps commutatif;

— Anneau factoriel non noethérien : $k[X_1, \dots, X_n, \dots, X_{n+1}, \dots]$, 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 $\text{Frac}(A) := A \setminus \{0\} \times A / \sim$ et

$$\begin{aligned} -/- : A \setminus \{0\} \times A &\rightarrow \text{Frac}(A) \\ (s, a) &\rightarrow a/s =: s^{-1}a \end{aligned}$$

la projection canonique. Considérons les applications $+, \cdot : (A \setminus \{0\} \times A) \times (A \setminus \{0\} \times A) \rightarrow \text{Frac}(A)$ 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 $+, \cdot : (A \setminus \{0\} \times A) \times (A \setminus \{0\} \times A) \rightarrow \text{Frac}(A)$ se factorisent en

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

On laisse en exercice le soin de vérifier que $\text{Frac}(A)$ muni des lois $+, \cdot : \text{Frac}(A) \times \text{Frac}(A) \rightarrow$

$\text{Frac}(A)$ 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

$$\begin{aligned} \iota_A : A &\rightarrow \text{Frac}(A) \\ a &\rightarrow a/1 \end{aligned}$$

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

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

Plus visuellement,

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

Démonstration. Montrons que $\text{Frac}(A)$ muni de la structure d'anneau ci-dessus et le morphisme canonique $\iota_A : A \rightarrow \text{Frac}(A)$ conviennent. Soit $\phi : A \rightarrow B$ un morphisme d'anneaux tel que $\phi(A \setminus \{0\}) \subset B^\times$. Si $\tilde{\phi} : \text{Frac}(A) \rightarrow B$ existe la relation $\phi = \tilde{\phi} \circ \iota_A$ impose que $\tilde{\phi} : \text{Frac}(A) \rightarrow B$ est unique puisqu'on doit nécessairement avoir

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

Considérons donc l'application $\tilde{\phi} : A \setminus \{0\} \times A \rightarrow B$ Si $(s, a) \sim (s', a')$ on a

$$(s, a) \rightarrow \phi(s)^{-1}\phi(a).$$

$\phi(s')\phi(a) - \phi(s)\phi(a') = \phi((s'a - sa')) = \phi(0) = 0$. 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 $\tilde{\phi} : A \setminus \{0\} \rightarrow B$ se factorise en

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

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

Comme d'habitude, le morphisme d'anneaux $\iota_A : A \rightarrow \text{Frac}(A)$ 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 $\mathbb{Q} := \text{Frac}(\mathbb{Z})$ et si K est un corps, on note $K(X_1, \dots, X_n) := \text{Frac}(K[X_1, \dots, X_n])$. Montrer que si A est un anneau intègre de corps des fractions K alors $\text{Frac}(A[X_1, \dots, X_n]) = K(X_1, \dots, X_n)$.

5.3.2 Valuations p -adiques

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

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

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

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

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 (5.1.2.1) s'étend également en une bijection

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

d'inverse

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

5.3.3 Contenu

Supposons toujours A factoriel. Pour tout $p \in \mathcal{P}_A$ on étend $v_p : K \rightarrow \overline{\mathbb{Z}}$ en $v_p : K[X] \rightarrow \overline{\mathbb{Z}}$ 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 $C_A : K[X] \rightarrow K$ 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 $A[X] \rightarrow A[X]/pA[X] \xrightarrow{\sim} (A/pA)[X]$. 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. \square

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 $\mathcal{P}_{K[X]}^\circ$ 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 $A[X]/pA[X] \xrightarrow{\sim} (A/pA)[X]$.

- 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 5.3.3, $C_A(F) = C_A(P)C_A(Q) = C_A(Q)$ donc $C_A(Q) \in A$ i.e. $Q \in A[X]$. Donc $F \in PA[X]$ et le morphisme $\phi : A[X] \hookrightarrow K[X] \twoheadrightarrow K[X]/PK[X]$ se factorise en un morphisme d'anneaux injectif $A/PA[X] \hookrightarrow K[X]/PK[X]$. Comme $K[X]$ est factoriel et P est irréductible, P est premier donc $K[X]/PK[X]$ est intègre. Comme un sous-anneau d'un anneau intègre est intègre, $A[X]/PA[X]$ est donc intègre.

2. L'application canonique $A^\times \times \mathbb{N}^{(\mathcal{P}_A \cup \mathcal{P}_{K[X]})} \rightarrow A[X] \setminus \{0\}$ est bijective.

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

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

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 $\Rightarrow A[X_1, \dots, X_n]$ factoriel.

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

$$A[X_1, \dots, X_n] \xrightarrow{\sim} A[X_1, \dots, X_{n-1}][X_n].$$

□

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 $X^p + X^{p-1} + \dots + X + 1$ 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 $\phi : A \rightarrow B$ un morphisme d'anneaux. La propriété universelle de $\iota_A : A \rightarrow A[X]$ appliquée avec $A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[X]$ donne un unique morphisme d'anneaux $\tilde{\phi} : A[X] \rightarrow B[X]$ 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 $P = P_1 P_2$ 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 $\tilde{\phi} : A[X] \rightarrow B[X]$ 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 $p_I : A \rightarrow A/I$ 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 système d'équations dans \mathbb{F}_2

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

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 $P = P_1 P_2$ 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 $C_{\mathbb{Z}}(P) = 1 = C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2) = P_1 C_{\mathbb{Z}}(P_2)$). Si $P = P_1 P_2$ 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 $P = P_1 P_2 = \frac{P_1}{C_{\mathbb{Z}}(P_1)} \frac{P_2}{C_{\mathbb{Z}}(P_2)}$ 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 Définitions et anneaux de valuation discrète

Définition 5.4.1. Une *valuation* (de rang 1) sur K est une application surjective¹ $v : K \rightarrow \overline{\mathbb{Z}}$ qui vérifie

1. $v(xy) = v(x) + v(y), x, y \in K$;

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

2. $v(x + y) \geq \min\{v(x), v(y)\}, x, y \in K;$
3. $v(x) = \infty \iff x = 0.$

Remarque 5.4.2. La propriété (1) peut se réécrire en disant que $v : (K^\times, \cdot) \rightarrow (\mathbb{Z}, +)$ est un morphisme de groupes.

Notons $A_v := v^{-1}([0, \infty]) \subset K$.

Définition 5.4.3. On dit qu'un anneau est *local* s'il possède un unique idéal maximal.

Lemme 5.4.4. *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 $x \in K$ s'écrit sous la forme $x = (x\pi^{-v(x)})\pi^{v(x)}$ avec $x\pi^{-v(x)} \in A_v^\times$. \square

Remarque 5.4.5. 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 5.4.6 (Difficile – cf. [S68, 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, noethérien 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.

5.4.2 Factorialité

Remarque 5.4.7. Si A est factoriel de corps des fractions $\iota_A : A \hookrightarrow K := \text{Frac}(A)$, les applications $v_p : K \rightarrow \overline{\mathbb{Z}}$ pour $p \in \mathcal{P}_A$ sont donc des valuations sur K et la famille de valuations

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

vérifie les propriétés suivantes :

- (5.4.1.1) pour tout $0 \neq x \in K$,

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

- (5.4.1.2) il existe une famille d'éléments $(p_v)_{v \in \mathcal{V}} \in K$ telle que $v(p_w) = \delta_{v,w}$, $v, w \in \mathcal{V}$;

- (5.4.1.3) $A = \bigcap_{v \in \mathcal{V}} A_v$.

Inversement, on a

Proposition 5.4.8. Soit K un corps muni d'une famille \mathcal{V} de valuations $v : K \rightarrow \overline{\mathbb{Z}}$ vérifiant les propriétés (5.4.1.1), (5.4.1.2). 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 , $v \in \mathcal{V}$ forment un système de représentants de \mathcal{P}_A° .

Démonstration. Observons d'abord que $A \subset K$ est un sous-anneau comme intersection de sous-anneaux (lemme 5.4.4). 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 $p \notin A^\times$. Écrivons $p_v = ab$ pour $a, b \in A$. On doit avoir $v(p_v) = 1 = v(a) + v(b)$ et $w(p_v) = 0 = w(a) + w(b)$ où $v \neq w \in \mathcal{V}$. 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 (5.4.1.1), on peut définir

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

qui vérifie par construction et la propriété (1) d'une valuation $v(u_a) = 0, v \in \mathcal{V}$ i.e. $u_a \in A^\times$. L'écriture $a = u_a \prod_{v \in \mathcal{V}} p_v^{v(a)}$ montre déjà que les $p_v, v \in \mathcal{V}$ forment un système de représentants des classes d'irréductibles 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 $u' \in A^\times, v'_-(a) : \mathcal{V} \rightarrow \mathbb{N} \in \mathbb{N}^{(\mathcal{V})}$, 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 (5.4.1.2) que $v'(a) = v(a), v \in \mathcal{V}$ et donc $u' = u_a$. \square

5.4.3 ppcm et pgcd

Exercice 5.4.9. Soit A un anneau factoriel.

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

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

On dit que les éléments de $A^\times \text{ppcm}(a, b)$ 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

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

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

3. Généraliser (1) et (2) à un nombre fini a_1, \dots, a_r d'éléments de A .
4. (Bézout) Supposons A principal. Montrer que $\text{pgcd}(a_1, \dots, a_r)A^\times = A^\times$ si et seulement si il existe $u_1, \dots, u_r \in A$ tels que $u_1 a_1 + \dots + u_r a_r = 1$.

Chapitre 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 non réduit à $\{0\}$.

6.1 Localisations

6.1.1 Parties multiplicatives

Définition 6.1.1. Une *partie multiplicative* de A est un sous-ensemble $S \subset A \setminus \{0\}$ stable par multiplication et contenant 1.

Exemples 6.1.2. — $S := A \setminus A_{\text{tors}}$; en particulier, si A est intègre, $S := A \setminus \{0\}$;

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

— Pour $\mathfrak{p} \in \text{Spec}(A)$, $S_{\mathfrak{p}} := A \setminus \mathfrak{p}$.

6.1.2 Définition

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

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

la projection canonique.

Considérons les applications

$$\begin{aligned} + : (S \times A) \times (S \times A) &\rightarrow S^{-1}A \\ ((s, a), (t, b)) &\rightarrow (ta + sb)/(st) \end{aligned}$$

et

$$\begin{aligned} \cdot : (S \times A) \times (S \times A) &\rightarrow S^{-1}A \\ ((s, a), (t, b)) &\rightarrow (ab)/(st) \end{aligned}$$

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

$$\begin{aligned} s''t''(s't'(ta + sb) - st(t'a' + s'b')) &= s''s'a'tt't'' - t'bss's'' - s''t''st(t'a' + s'b') \\ &= s''sa''tt't'' - tb'ss's'' - s''t''st(t'a' + s'b') \\ &= 0. \end{aligned}$$

et

$$\begin{aligned} s''t''(s't'ab - sta'b') &= s''s'at''t'b - s''sa't''tb' \\ &= s''sa't''t'b - s''sa't''tb' \\ &= s''sa't''(t'b - tb') \\ &= 0. \end{aligned}$$

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

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

On laisse en exercice le soin de vérifier que $S^{-1}A$ muni des lois $+, \cdot : S^{-1}A \times S^{-1}A \rightarrow S^{-1}A$ 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

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

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), $\iota_S : A \rightarrow S^{-1}A$ 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 Propriété universelle

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

Plus visuellement,

$$\begin{array}{ccc} S & \xrightarrow{\phi} & B^\times \\ \downarrow & & \downarrow \\ A & \xrightarrow{\forall \phi} & B \\ \downarrow \iota_S & \nearrow \exists! \phi_S & \\ F & & \end{array}$$

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

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

Considérons donc l'application $\tilde{\phi} : S \times A \rightarrow B$ 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 $\phi_S : S \times A \rightarrow B$ se factorise en

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

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

Comme d'habitude, le morphisme d'anneaux $\iota_S : A \rightarrow S^{-1}A$ 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 .

Exercices 6.1.4. 1. Montrer qu'on a un isomorphisme d'anneaux canonique

$$S^{-1}(A[X]) \xrightarrow{\sim} (S^{-1}A)[X].$$

Correction. On va utiliser les propriétés universelles de la localisation et de l'algèbre des polynômes à une indéterminée pour construire un morphisme dans les deux sens. Considérons le morphisme d'anneaux $\phi : A \xrightarrow{\iota_S} S^{-1}A \xrightarrow{\iota_{S^{-1}A}} (S^{-1}A)[X]$. Par propriété universelle de $\iota_A : A \rightarrow A[X]$, il s'étend en un unique morphisme de A -algèbre $\phi : A[X] \rightarrow (S^{-1}A)[X]$ tel que $\phi(X) = X$. De plus, $\phi(S) = \iota_{S^{-1}A}(\iota_S(S)) \subset \iota_{S^{-1}A}((S^{-1}A)^\times) = (S^{-1}A)[X]^\times$ donc par propriété universelle de $\iota_S : A[X] \rightarrow S^{-1}(A[X])$, $\phi : A[X] \rightarrow$

$(S^{-1}A)[X]$ s'étend en un unique morphisme d'anneaux $\phi_S : S^{-1}(A[X]) \rightarrow (S^{-1}A)[X]$ tel que $\phi_S \circ \iota_S = \phi$. Dans l'autre sens, considérons le morphisme d'anneaux $\psi : A \xrightarrow{\iota_A} A[X] \xrightarrow{\iota_S} S^{-1}A([X])$. On a $\psi(S) = \iota_S(\iota_A(S)) \subset S^{-1}A([X])^\times$ donc par propriété universelle de $\iota_S : A \rightarrow S^{-1}A$ il existe un unique morphisme d'anneaux $\psi_S : S^{-1}A \rightarrow S^{-1}A([X])$ tel que $\psi_S \circ \iota_S = \psi$. Enfin, par la propriété universelle de $\iota_{S^{-1}A} : S^{-1}A \rightarrow S^{-1}A$, il existe un unique morphisme de $S^{-1}A$ -algèbre $\psi_S : (S^{-1}A)[X] \rightarrow S^{-1}(A[X])$ tel que $\psi_S(X) = X$. On vérifie immédiatement sur les constructions que $\psi_S \circ \phi_S = \text{Id}$ et $\phi_S \circ \psi_S = \text{Id}$.

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 $(A \setminus \mathfrak{p})^{-1}A$.

Correction. Les idéaux de A sont les images par la projection canonique $\mathbb{Z} \twoheadrightarrow A$ des idéaux de \mathbb{Z} contenant l'idéal $pq\mathbb{Z}$. Or \mathbb{Z} est principal donc ses idéaux sont tous de la forme $n\mathbb{Z}$ et la condition $pq\mathbb{Z} \subset n\mathbb{Z}$ est équivalente à $n \mid pq$. On n'a donc que quatre possibilités : A , $\{0\}$, $\mathfrak{p} := p\mathbb{Z}/pq\mathbb{Z}$ et $\mathfrak{q} := q\mathbb{Z}/pq\mathbb{Z}$. On a $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} A/\mathfrak{p}$ et $\mathbb{Z}/q\mathbb{Z} \xrightarrow{\sim} A/\mathfrak{q}$ donc $\text{spec}(A) = \{\mathfrak{p}, \mathfrak{q}\}$. J'affirme qu'on a un isomorphisme (nécessairement unique) $\phi_{\mathfrak{p}} : A/\mathfrak{p} \xrightarrow{\sim} A_{\mathfrak{p}}$ tel que le diagramme canonique suivant commute

$$\begin{array}{ccc} & A & \\ p_{\mathfrak{p}} \swarrow & & \searrow \iota_{A \setminus \mathfrak{p}} \\ A/\mathfrak{p} & \xrightarrow[\phi_{\mathfrak{p}}]{\cong} & A_{\mathfrak{p}} \end{array}$$

(et idem pour \mathfrak{q}). On va utiliser les propriétés universelles de $p_{\mathfrak{p}} : A \rightarrow A/\mathfrak{p}$ et $\iota_{A \setminus \mathfrak{p}} : A \rightarrow A_{\mathfrak{p}}$. Par le lemme chinois $A \xrightarrow{\sim} \mathbb{Z}/p \times \mathbb{Z}/q$ et \mathfrak{p} s'identifie à l'idéal engendré par $e_2 := (0, 1)$; notons aussi $e_1 := (1, 0)$. Soit $\iota_{\mathfrak{p}} : A \rightarrow A_{\mathfrak{p}}$ le morphisme de localisation. On a pour tout $a \in \mathfrak{p}$, $e_1 a = 0$. Or, comme $e_1 \in A \setminus \mathfrak{p}$, on a $\iota_{\mathfrak{p}}(e_1) \in A_{\mathfrak{p}}^\times$ donc $0 = \iota_{\mathfrak{p}}(e_1 a) = \iota_{\mathfrak{p}}(e_1) \iota_{\mathfrak{p}}(a)$ implique en simplifiant par $\iota_{\mathfrak{p}}(e_1) \in A_{\mathfrak{p}}^\times$, $\iota_{\mathfrak{p}}(a) = 0$. Autrement dit, on vient de montrer que $\mathfrak{p} \subset \ker(\iota_{\mathfrak{p}})$; le morphisme canonique $\iota_{\mathfrak{p}} : A \rightarrow A_{\mathfrak{p}}$ se factorise donc en un unique morphisme $\phi_{\mathfrak{p}} : A/\mathfrak{p} \rightarrow A_{\mathfrak{p}}$ tel que $\phi_{\mathfrak{p}} \circ p_{\mathfrak{p}} = \iota_{\mathfrak{p}}$. Considérons maintenant la projection canonique $p_{\mathfrak{p}} : A \rightarrow A/\mathfrak{p}$. Puisque \mathfrak{p} est maximal, pour tout $a \in A \setminus \mathfrak{p}$ il existe $b \in A$ tel que $ab - 1 \in \mathfrak{p}$ donc $1 = p_{\mathfrak{p}}(ab) = p_{\mathfrak{p}}(a)p_{\mathfrak{p}}(b)$. Ce qui montre que $p_{\mathfrak{p}}(A \setminus \mathfrak{p}) \subset (A/\mathfrak{p})^\times$. Donc il existe un unique morphisme d'anneaux $\psi_{\mathfrak{p}} : A_{\mathfrak{p}} \rightarrow A/\mathfrak{p}$ tel que $\psi_{\mathfrak{p}} \circ \iota_{A \setminus \mathfrak{p}} = p_{\mathfrak{p}}$. Mais on a alors par construction $\psi_{\mathfrak{p}} \circ \phi_{\mathfrak{p}} \circ p_{\mathfrak{p}} = p_{\mathfrak{p}}$, ce qui par unicité dans la propriété universelle de $p_{\mathfrak{p}} : A \rightarrow A/\mathfrak{p}$ (appliquée à $p_{\mathfrak{p}} : A \rightarrow A/\mathfrak{p}$!) impose $\psi_{\mathfrak{p}} \circ \phi_{\mathfrak{p}} = \text{Id}$. De même avec la localisation, $\phi_{\mathfrak{p}} \circ \psi_{\mathfrak{p}} \circ \iota_{A \setminus \mathfrak{p}} = \iota_{A \setminus \mathfrak{p}}$ impose $\phi_{\mathfrak{p}} \circ \psi_{\mathfrak{p}} = \text{Id}$.

3. Montrer que si A est intègre (resp. réduit, resp. intégralement clos, resp. factoriel) alors

$S^{-1}A$ l'est aussi.

- Exemples 6.1.5.** 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 $\mathfrak{p} \in \text{Spec}(A)$, on note $A_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}A$. Noter que si A est intègre $\{0\} \in \text{Spec}(A)$ et, dans ce cas, $A_{\{0\}} = \text{Frac}(A)$.

6.1.4 Morphismes

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

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow \iota_S & & \downarrow \iota_T \\ S^{-1}A & \xrightarrow{\tilde{\phi}} & T^{-1}B \end{array}$$

- Exemples 6.1.6.** 1. Soit $\phi : A \rightarrow B$ un morphisme d'anneaux et $\mathfrak{q} \in \text{Spec}(B)$. On a alors $\mathfrak{p} := \phi^{-1}(\mathfrak{q}) \in \text{Spec}(A)$ et $\phi(A \setminus \mathfrak{p}) \subset B \setminus \mathfrak{q}$ donc $\phi : A \rightarrow B$ induit un morphisme d'anneaux canonique $\phi_{\mathfrak{p}} : A_{\mathfrak{p}} \rightarrow B_{\mathfrak{q}}$.
2. Si A est intègre, $\{0\} \in \text{Spec}(A)$ et pour toute partie multiplicative $S \subset A \setminus \{0\}$, en appliquant ce qui précède à $\phi = \text{Id} : A \rightarrow A$, $S = S$, $T = A \setminus \{0\}$, on obtient un morphisme canonique $\phi : S^{-1}A \rightarrow A_{\{0\}} = \text{Frac}(A)$ dont on vérifie immédiatement qu'il est injectif.

$$\begin{array}{ccc}
A & \xrightarrow{\text{Id}} & A \\
\downarrow \iota_S & & \downarrow \iota_T \\
S^{-1}A & \xrightarrow{\tilde{\text{Id}}} & \text{Frac}(A)
\end{array}$$

6.2 Idéaux

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

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

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

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

Dans l'autre direction on a l'application

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

induite par le morphisme de localisation $\iota_S : A \rightarrow S^{-1}A$.

— Pour $I \subset A$ un idéal, on a

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

Où $s \cdot$ est l'application de multiplication par s , pour tout s dans S . 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

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

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 :

Lemme 6.2.1. *L'application $S^{-1} : (\mathcal{I}_A, \subset) \rightarrow (\mathcal{I}_{S^{-1}A}, \subset)$ 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 $\iota_S^{-1} : (\mathcal{I}_{S^{-1}A}, \subset) \rightarrow (\mathcal{I}_A, \subset)$ est injective, croissante pour \subset et induit une bijection

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

Lemme 6.2.2. *Les applications $S^{-1} : \mathcal{I}_A \rightarrow \mathcal{I}_{S^{-1}A}$ et $\iota_S^{-1} : \mathcal{I}_{S^{-1}A} \rightarrow \mathcal{I}_A$ se restreignent en des bijections inverses l'une de l'autres*

$$\mathrm{Spec}(S^{-1}A) \xrightleftharpoons[\iota_S^{-1}]{S^{-1}} \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}$$

Démonstration. Si $\mathfrak{p} \in \mathrm{Spec}(A)$ 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 $S^{-1} \iota_S^{-1} = \mathrm{Id}$, et $\iota_S^{-1} \mathrm{Spec}(S^{-1}A) \subset \mathrm{Spec}(A)$, il reste seulement à montrer que si $\mathfrak{p} \in \mathrm{Spec}(A)$ est tel que $S \cap \mathfrak{p} = \emptyset$ alors $S^{-1} \mathfrak{p} \in \mathrm{Spec}(S^{-1}A)$. Soit donc $\mathfrak{p} \in \mathrm{Spec}(A)$ 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 $\mathfrak{p} \in \mathrm{Spec}(A)$ et $vu \notin \mathfrak{p}$, on a $ab \in \mathfrak{p}$ donc $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. \square

Exemple 6.2.3 (Corps résiduel). Si $\mathfrak{p} \in \mathrm{Spec}(A)$, $A_{\mathfrak{p}}$ 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 $\mathrm{Spec}(A)$ en \mathfrak{p} . Si on reprend les notations de l'Exemple 1, le morphisme $\phi : A_{\mathfrak{p}} \rightarrow B_{\mathfrak{q}}$ envoie \mathfrak{p} dans \mathfrak{q} donc induit par passage au quotient un morphisme de corps — nécessairement injectif — $\kappa(\mathfrak{p}) \hookrightarrow \kappa(\mathfrak{q})$.

Corollaire 6.2.4. *Si A est noethérien (resp. principal) alors $S^{-1}A$ l'est aussi.*

Exercices 6.2.5. 1. Soit $\mathfrak{p} \in \mathrm{Spec}(A)$. Montrer qu'on a un morphisme d'anneaux canonique injectif $A/\mathfrak{p} \rightarrow \kappa(\mathfrak{p})$. 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

$$S^{-1}I/S^{-1}J \xrightarrow{\sim} \overline{S}^{-1}(I/J).$$

Chapitre 7

Complétion (Hors programme)

7.1 Limites projectives

Un système projectif d'ensembles est une suite d'applications ensemblistes

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

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

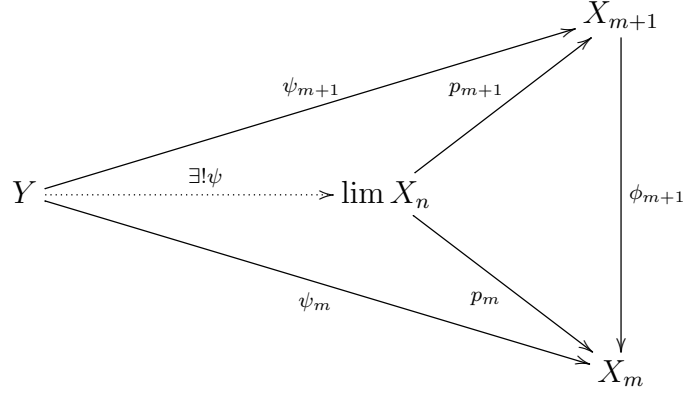
$$\lim X_n := \{ \underline{x} = (x_n)_{n \geq 0} \in \prod_{n \geq 0} X_n \mid \pi_{n+1}(x_{n+1}) = x_n, n \geq 0 \} \subset \prod_{n \geq 0} X_n$$

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

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 $p_m : P \rightarrow X_m$, $m \geq 0$ telles que pour toute famille d'applications ensemblistes $\psi_m : Y \rightarrow X_m$, $m \geq 0$ telles que $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, il existe une unique application ensembliste $\psi : Y \rightarrow \lim X_n$ telle que $p_m \circ \psi = \psi_m$, $m \geq 0$.*

Plus visuellement



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

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

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

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

Si les applications $\phi_{n+1} : X_{n+1} \rightarrow X_n$, $n \geq 0$ sont des morphismes de monoïdes (resp. de groupes, resp. d'anneaux), on vérifie immédiatement que $\lim X_n \subset \prod_{n \geq 0} X_n$ est un sous-monoïde (resp. un sous-groupe, resp. un sous-anneau) et que les projections $p_m : \prod_{n \geq 0} X_n \rightarrow X_m$, $m \geq 0$ sont des morphismes de monoïdes (resp. de groupes, resp. d'anneaux). Le Lemme 7.1.2 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) $p_m : P \rightarrow X_m$, $m \geq 0$ telles que pour toute famille de morphismes de monoïdes (resp. de groupes, resp. d'anneaux) $\psi_m : Y \rightarrow X_m$, $m \geq 0$ telles que $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, il existe un unique morphisme de monoïdes (resp. de groupes, resp. d'anneaux) $\psi : Y \rightarrow \lim X_n$ 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 $p_n : A \rightarrow A/I_n$ se factorise en

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

d'où un système projectif de morphismes d'anneaux

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

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

$$c_I : A \rightarrow \hat{A} := \lim A/I_n.$$

On note

$$\hat{I}_n := \{\underline{a} \in \hat{A} \mid a_m = 0, m \leq n\}$$

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, $+, \cdot : A \times A \rightarrow A$ 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 $c_I : A \rightarrow \hat{A}$ est continu (pour les topologies définies par les suites I_n , $n \geq 0$ et \hat{I}_n , $n \geq 0$). De plus, \hat{A} est

complet, séparé et $c_I : A \rightarrow \widehat{A}$ induit des isomorphismes canoniques $A/I_n \xrightarrow{\sim} \widehat{A}/\widehat{I}_n$.

On dit que $c_I : A \rightarrow \widehat{A}$ est ‘la’ complétion 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 complétion 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 $\mathbb{Z} \rightarrow \mathbb{Z}_p$ 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 $\mathbb{Z} \rightarrow \mathbb{Z}_p$ 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 et 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 $\widehat{\mathbb{Z}_{p\mathbb{Z}}} \xrightarrow{\sim} \mathbb{Z}_p$, où $\widehat{\mathbb{Z}_{p\mathbb{Z}}} \rightarrow \widehat{\mathbb{Z}_{p\mathbb{Z}}}$ est la complétion $p\mathbb{Z}$ -adique de $\mathbb{Z}_{p\mathbb{Z}}$.

2. Soit A un anneau commutatif intègre. $A = A[X]$, $I = XA[X]$. Plus précisément, reprenons les notations du paragraphe 1.3. On munit $A^\mathbb{N}$ des lois $+$, $\cdot : A^\mathbb{N} \times A^\mathbb{N} \rightarrow A^\mathbb{N}$ définies par

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

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 $\widehat{A[X]_{XA[X]}} \xrightarrow{\sim} A[[X]]$, où $A[X] \rightarrow A[[X]]$ est la complétion

$XA[X]_{XA[X]}$ -adique de $A[X]_{XA[X]}$.

Chapitre 8

Un peu de géométrie (Hors programme)

L'objectif¹ de ce chapitre est de fournir une motivation géométrique aux (nombreuses) définitions algébriques énoncées dans les chapitres précédents.

Définition 8.0.1 (variété algébrique affine). On appelle *variété algébrique (affine)* le lieu d'annulation de r polynômes à n indéterminées $P_1, \dots, P_r \in \mathbb{C}[X_1, \dots, X_n]$. On la note $V(P_1, \dots, P_r) := \{\underline{x} \in \mathbb{C}^n : \forall i \in \llbracket 1, \dots, n \rrbracket, P_i(\underline{x}) = 0\}$ ou encore $V(\langle P_1, \dots, P_r \rangle) := \{\underline{x} \in \mathbb{C}^n : \forall P \in \langle P_1, \dots, P_r \rangle, P(\underline{x}) = 0\}$.

Remarque 8.0.2. Les deux définitions sont bien équivalentes. Le lecteur est invité à le vérifier.

On peut vouloir munir une telle variété d'une topologie. La topologie de Zariski répond à cette volonté.

Définition 8.0.3 (topologie de Zariski). Soient $P_1, \dots, P_r \in \mathbb{C}[X_1, \dots, x_n]$. La topologie de Zariski sur la variété algébrique $V(P_1, \dots, P_r)$ est la topologie dont les fermés sont les idéaux $V(I)$ où I est un idéal de $\mathbb{C}[X_1, \dots, X_n]$ contenant l'idéal $\langle P_1, \dots, P_r \rangle$.

Nous allons maintenant donner un exemple fondamental de variétés algébriques que nous reprendrons tout au long du chapitre.

1. Chapitre rédigé par Quentin Dupré, à partir du cours dispensé en classe par Anna Cadoret

Exemple 8.0.4 (courbes planes dans \mathbb{C}^2). On considère ici des variétés $C = V(P)$ où $P \in \mathbb{C}[X, Y]$.

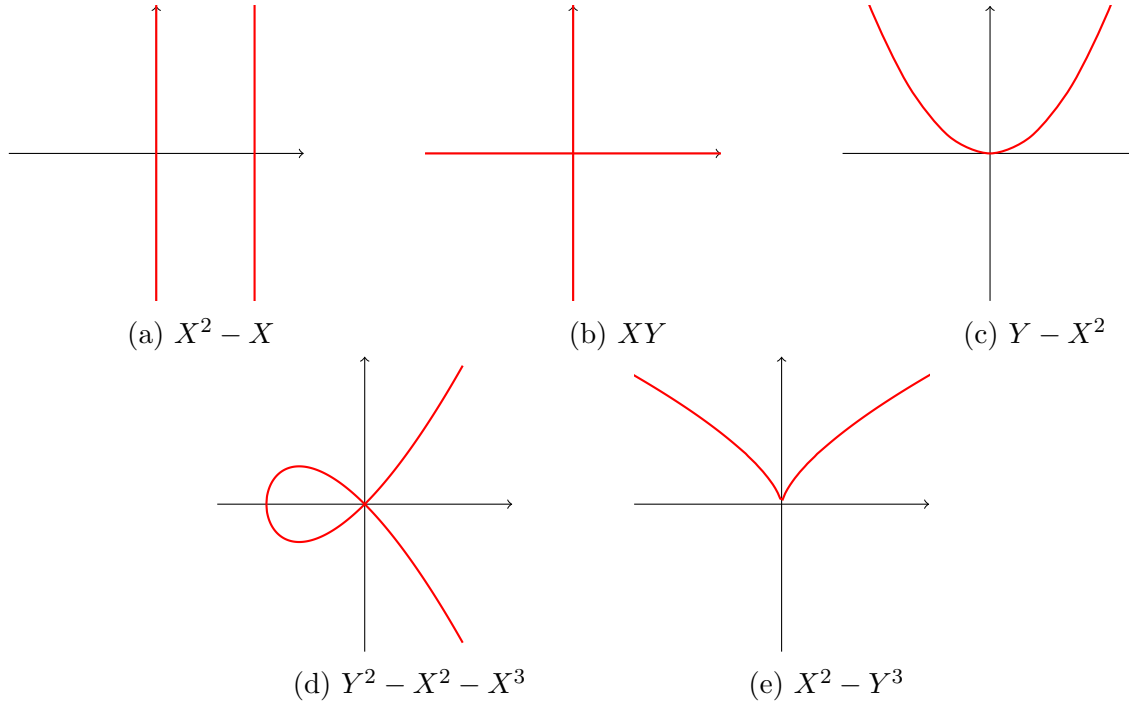


FIGURE 8.1 – Courbes algébriques dans \mathbb{C}^2

Remarque 8.0.5. En général, $V(P_1, \dots, P_r)$ est très difficile à comprendre. L'idée fondamentale est donc d'étudier $V := V(P_1, \dots, P_r)$ via les fonctions algébriques sur $V \subset \mathbb{C}^n$.

Définition 8.0.6. Soit $V := V(P_1, \dots, P_r)$ (où $P_1, \dots, P_r \in \mathbb{C}[X_1, \dots, X_r]$) une variété algébrique. On a alors un morphisme d'anneaux

$$I_v : \mathbb{C}[X_1, \dots, X_n] \rightarrow \mathbb{C}^V \quad (8.1)$$

$$F \mapsto \underline{x} \in V \mapsto \underline{F}(\underline{x}) \in \mathbb{C} \quad (8.2)$$

où la fonction \underline{F} est polynomiale. Ce morphisme se factorise en $\mathbb{C}[X_1, \dots, X_n] / \sqrt{\langle P_1, \dots, P_r \rangle} \rightarrow \mathbb{C}[V]$. On dit que $\mathbb{C}[V] \subset \mathbb{C}^V$ est l'anneau des fonctions algébriques sur V . $\sqrt{\langle P_1, \dots, P_r \rangle} \subset \text{Ker}(I_v : \mathbb{C}[X_1, \dots, X_n] \rightarrow \mathbb{C}[V])$ (théorème des zéros de Hilbert).

Remarque 8.0.7. Ce qui est remarquable en géométrie algébrique est l'existence d'une correspondance bijective (équivalence de catégories) entre deux mondes a priori distincts.

$$\begin{array}{ccc}
\begin{array}{c} \mathbb{C}\text{-algèbres de type fini} \\ \text{morphismes de } \mathbb{C}\text{-algèbres} \\ \mathbb{C}[V] \end{array} & \leftrightarrow & \begin{array}{c} \text{variétés algébriques affines} \\ \text{morphismes } F_{|V_1}^{V_2} \rightarrow V_2 \\ V \end{array}
\end{array}$$

On dispose ainsi d'un dictionnaire :

$$\begin{array}{ccc}
\text{propriétés algébriques de } \mathbb{C}[V] & & \text{propriétés géométriques de } V \\
\ll \text{preuve} \gg & \leftrightarrow & \ll \text{intuition} \gg
\end{array}$$

Exemple 8.0.8. Si l'on considère les courbes 8.1b et 8.1d, on semble y trouver en zéro les mêmes types de propriétés, alors que celles-ci paraissent différentes sur la courbe 8.1e. Cette intuition géométrique et visuelle se montre algébriquement.

Insérer ici le dictionnaire sur la topologie

Exemple 8.0.9. Courbe 8.1a $\mathbb{C}[V] = \mathbb{C}[X, Y]/(X^2 - X) \simeq \mathbb{C}[X, Y]/(X) \times \mathbb{C}[X, Y]/(X - 1)$ d'après le théorème chinois. V n'est pas connexe : il y a deux composantes connexes $V(X)$ et $V(X - 1)$.

Courbe 8.1b $\mathbb{C}[V] = \mathbb{C}[X, Y]/(XY)$ n'est pas intègre car $\overline{XY} = 0$ alors que $\overline{X} \neq 0$ et $\overline{Y} \neq 0$. Deux idéaux premiers minimaux $\langle X \rangle, \langle Y \rangle$ qui correspondent aux deux composantes irréductibles $V(X)$ et $V(Y)$.

En revanche, V est connexe. $\mathbb{C}[X, Y]/(XY) \not\simeq A_1 \times A_2$ car il n'existe pas d'idempotent.

$$e_1 = (1, 0), e_2 = (0, 1)$$

$$e_1^2 = e_1, e_2^2 = e_2, e_1 e_2 = 0, e_1, e_2 \notin \{0, 1\}$$

Soit $\overline{P} \in \mathbb{C}[X, Y]/(XY)$ tel que $\overline{P} \neq \overline{0}, \overline{1}$ et $\overline{P}^2 = \overline{P}$. Alors $\overline{P}^2 - \overline{P} = \overline{0}$ donc $XY \mid P(P-1)$.

En utilisant la factoriabilité de $\mathbb{C}[X, Y]$, on a $X \mid P$ ou $X \mid P - 1$ et $Y \mid P$ ou $Y \mid P - 1$.

Les différentes possibilités sont alors :

- $X, Y \mid P \implies XY \mid P \implies \overline{P} = \overline{0}$,
- $X, Y \mid P - 1 \implies XY \mid P - 1 \implies \overline{P} = \overline{1}$,
- $(X \mid P, Y \mid P - 1) \implies P = UX = 1 + VY$ contradictoire avec le choix d'irréductibles (on peut aussi évaluer ce polynôme en $(0, 0)$ pour obtenir une contradiction).

Dans tous les cas, on obtient une contradiction. Un tel \overline{P} n'existe donc pas.

Courbes 8.1c, 8.1d et 8.1e $Y - X^2, Y^2 - X^2 - X^3$ et $X^2 - Y^3$ sont irréductibles dans $\mathbb{C}[X, Y]$ donc premiers par factoriabilité de l'anneau, V est par conséquent irréductible et $\mathbb{C}[V]$ est intègre.

Ici le dictionnaire sur les singularités.

Exemple 8.0.10.

Remarque 8.0.11. Pour étudier plus finement les singularités, il faut en quelque sorte zoomer sur celles-ci. Algébriquement, cela correspond à localiser ou à compléter. Pour étudier V en $(0, 0)$, on localise $A/I = \mathbb{C}[V]$ en $\mathfrak{m}/I = \langle \bar{X}, \bar{Y} \rangle$ où \mathfrak{m}/I est un idéal maximal, $A = \mathbb{C}[X_1, \dots, X_n]$, $I = \langle P_1, \dots, P_r \rangle$ et $\mathfrak{m} = \langle X, Y \rangle$.

Définition 8.0.12. Une bonne définition de « être lisse » pour une courbe algébrique est :
 V est lisse $\iff \forall \mathfrak{m} \in \text{spm}(\mathbb{C}[V]), \mathbb{C}[V]_{\mathfrak{m}}$ est un anneau de valuation discrète.

Pour la complétion, on a :

$$\mathbb{C}[V]_{\mathfrak{m}} \leftrightarrow \text{Complétion par la topologie } \mathfrak{m}\text{-adique } \widehat{\mathbb{C}[V]_{\mathfrak{m}}}$$

Deuxième partie

Modules sur un anneaux

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

Chapitre 9

Premières définitions et constructions

9.1 Définitions

Définition 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 $\cdot : A \times M \rightarrow M$ - appelée 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

$$\begin{aligned} A &\rightarrow \text{End}_{Grp}(M) \\ a &\mapsto a.\text{Id} \end{aligned}$$

est un morphisme d'anneaux.

Définition 9.1.2. Étant donnés deux A -modules M, N , un morphisme de A -modules est un morphisme de groupes $f : (M, +) \rightarrow (N, +)$ 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 $\text{Id} : M \rightarrow M$ est un morphisme de A -modules et que si $f : M \rightarrow N$ et $g : N \rightarrow P$ sont des morphismes de A -modules alors $g \circ f : M \rightarrow P$ est un morphisme de A -modules.

Définition 9.1.3. On notera $\text{Hom}_A(M, N)$ l'ensemble des morphismes de A -modules $\phi : M \rightarrow N$ et, si $M = N$, $\text{End}_A(M) := \text{Hom}_A(M, M)$.

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

9.1.1 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 $\cdot : A \times A \rightarrow A$. 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 $\cdot : A \times I \rightarrow I$ induite par le produit de A est un A -module. On dit alors que A est le A -module régulier.
- Si M, N sont deux A -modules, $\text{Hom}_A(M, N)$ 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 $\phi : A \rightarrow B$ est un morphisme d'anneaux tout B -module M est naturellement un A -module pour la multiplication extérieure $A \times M \rightarrow M$, $(a, n) \rightarrow \phi(a) \cdot n$. On notera ϕ^*M ou $M|_A$ lorsqu'il n'y a pas d'ambiguïté sur $\phi : A \rightarrow B$ le A -module ainsi obtenu à partir du B -module M . On notera que tout morphisme de B -modules $f : M \rightarrow N$ est automatiquement un morphisme de A -modules $f|_A = f : M|_A \rightarrow N|_A$. En particulier, une structure de A -algèbre $\phi : A \rightarrow B$ sur un anneau B détermine une structure de A -module ϕ^*B sur B . Inversement, une structure de A -module $\cdot : A \times B \rightarrow B$ sur le groupe abélien sous-jacent $(B, +)$ d'un anneau B détermine une structure de A -algèbre $\phi : A \rightarrow B$ sur B en posant $\phi(a) = a \cdot 1_B$. En particulier, si M est un A -module, $\text{End}_A(M)$ est naturellement muni d'une structure de A -algèbre.
- Soit A un anneau commutatif. Par la propriété universelle de $\iota_A : A \rightarrow A[X_1, \dots, X_n]$,

la donnée d'un $A[X_1, \dots, X_n]$ -module est équivalente à la donnée d'un couple $(M, \underline{\phi})$, où M est un A -module et $\underline{\phi} := (\phi_1, \dots, \phi_n)$ 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 $u \in \text{End}_k(V)$, on peut munir V de la structure V_u de $k[X]$ -module définie par $P(X) \cdot v = P(u)(v)$. Si $u, u' \in \text{End}_k(V)$, on a

$$\text{Hom}_{k[X]}(V_u, V_{u'}) = \{\varphi : V \rightarrow V \mid \varphi \circ u = u' \circ \varphi\}.$$

Un certain nombre de résultats d'algèbre linéaire s'interprètent (et deviennent bien plus naturels!) en termes de $k[X]$ -modules.

Définition 9.1.4 (Sous-module). 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 9.1.5. — Les sous- A -modules du A -module régulier A sont les idéaux de A .

— Si $f : M \rightarrow N$ 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, $\text{im}(f) \subset N$ et $\text{ker}(f) \subset M$ sont des sous- A -modules.

— Si $I \subset A$ est un idéal et M un A -module,

$$IM := \left\{ \sum_{m \in M} a(m)m \mid a : M \rightarrow I \text{ à support fini} \right\} \subset M$$

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

$$\begin{aligned} A \times \prod_{i \in I} M_i &\rightarrow \prod_{i \in I} M_i \\ (a, \underline{m} = (m_i)_{i \in I}) &\rightarrow a \cdot \underline{m} = (a \cdot m_i)_{i \in I}. \end{aligned}$$

Avec cette structure de A -module, les projections canoniques $p_j : \prod_{i \in I} M_i \rightarrow M_j$, $j \in I$ deviennent des morphismes de A -modules.

Définition 9.2.1 (Somme directe). On appelle somme directe de la famille $M_i, i \in I$ et l'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 9.2.2 (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 $p_i : \Pi \rightarrow M_i$, $i \in I$ et $\iota_i : M_i \rightarrow \Sigma$, $i \in I$ tels que*

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

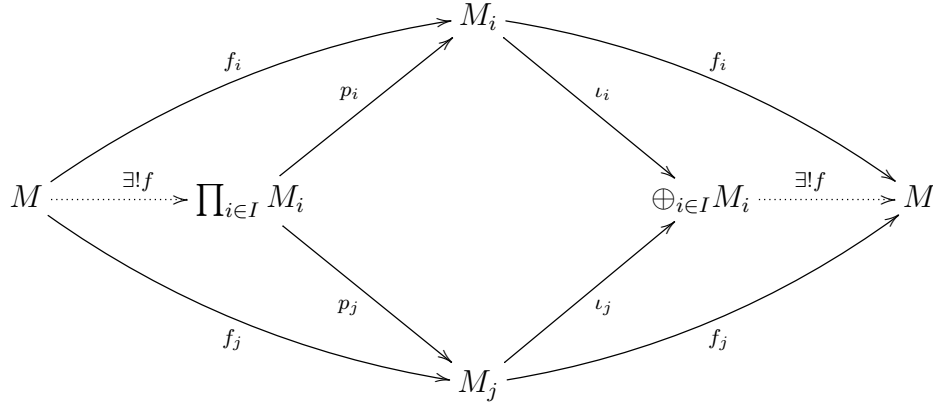
Démonstration. On vérifie comme d'habitude que les morphismes de A -modules $p_j : \prod_{i \in I} M_i \rightarrow M_j$, $j \in I$ et $\iota_j : M_j \hookrightarrow \bigoplus_{i \in I} M_i$, $j \in I$ construits ci-dessus conviennent. \square

Remarque 9.2.3. On peut aussi réécrire le lemme en disant que, pour tout A -module M les morphismes canoniques

$$\begin{aligned} \text{Hom}_A(M, \prod_{i \in I} M_i) &\rightarrow \prod_{i \in I} \text{Hom}_A(M, M_i) \\ f &\mapsto (p_i \circ f)_{i \in I} \end{aligned}$$

$$\begin{aligned} \text{Hom}_A(\bigoplus_{i \in I} M_i, M) &\rightarrow \prod_{i \in I} \text{Hom}_A(M_i, M) \\ f &\mapsto (f \circ \iota_i)_{i \in I} \end{aligned}$$

sont des isomorphismes ou encore, plus visuellement :



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

Remarque 9.2.4. Si $M_i = M$ pour tout $i \in I$, on notera $M^I := \prod_{i \in I} M_i$ et $M^{(I)} := \bigoplus_{i \in I} M_i$. Par construction, on a des isomorphismes canoniques

$$\text{Hom}(A^{(I)}, M) \simeq \prod_{i \in I} \text{Hom}(A, M) \simeq M^I$$

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

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

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

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

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

on obtient un unique morphisme de A -modules $f := \bigoplus_{i \in I} f_i : \bigoplus_{i \in I} M_i \rightarrow \bigoplus_{i \in I} N_i$ 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 .

Définition 9.3.1. 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 .

Remarque 9.3.2. On vérifie qu'il coïncide avec l'ensemble des éléments de la forme $\sum_{x \in X} a(x)x$, où $a : X \rightarrow A$ 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 $-x : A \rightarrow M, a \mapsto ax, x \in X$ nous donne un unique morphisme de A -modules $p_X : A^{(X)} \rightarrow M$ tel que $p_X \circ \iota_x(a) = ax, x \in X$. On vérifie immédiatement que les propriétés suivantes sont équivalentes :

1. $M = \langle X \rangle$;
2. Le morphisme de A -modules $p : A^{(X)} \rightarrow M$ 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*.

Exemple 9.3.3. — Si A est un corps, les A -modules de type fini sont les A -espaces vectoriels de dimension finie.

— Si A est noethérien, tout sous A -module de A (c'est à dire les idéaux de l'anneau A) est de type fini.

— Si $\text{card}(X) < +\infty$, $A^{(X)}$ est un A -module de type fini, engendré par les $e_x := (\delta_{xy})_{y \in X}$.

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

$$\sum_{i \in I} M_i = \left\langle \bigcup_{i \in I} M_i \right\rangle = \left\{ \sum_{i \in I} m_i : m_i \in M_i, \text{card}\{i \in I : m_i \neq 0\} < +\infty \right\} \subset M.$$

Là encore la propriété universelle de $\iota_i : M_i \hookrightarrow \bigoplus_{i \in I} M_i$, $i \in I$ 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 - $p : \bigoplus_{i \in I} M_i \twoheadrightarrow \sum_{i \in I} M_i (\subset M)$ 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 $p_{M'} : M \rightarrow M/M'$, $m \rightarrow p_{M'}(m) =: \overline{m}$ comme groupe abélien. On peut munir M/M' d'une structure de A -module comme suit. Pour tout $a \in A$, l'application

$$\begin{aligned} \mu_a : M &\rightarrow M/M' \\ m &\rightarrow \overline{a \cdot m} \end{aligned}$$

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

$$\begin{array}{ccc} M & \xrightarrow{\mu_a} & M/M' \\ p_{M'} \downarrow & \nearrow \overline{\mu}_a & \\ M/M' & & \end{array}$$

On pose alors

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

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 $p_{M'} : M \rightarrow M/M'$ un morphisme de A -modules. De plus,

Lemme 9.4.1 (Propriété universelle du quotient). *Pour tout sous- A -module $M' \subset M$ il existe*

un morphisme de A -modules $p : M \rightarrow Q$ tel que pour tout morphisme de A -modules $f : M \rightarrow N$ tels que $M' \subset \ker(f)$, il existe unique morphisme de A -modules $\bar{f} : Q \rightarrow N'$ tel que $\bar{f} \circ p = f$.

Démonstration. On vérifie comme d'habitude que le morphisme de A -modules $p'_M : M \rightarrow M/M'$ construit ci-dessus convient. \square

Remarque 9.4.2. On peut aussi réécrire 9.4 en disant que, pour tout A -module N le morphisme canonique

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

est un isomorphisme ou encore, plus visuellement :

$$\begin{array}{ccccc} & & 0 & & \\ & \curvearrowright & & \searrow & \\ M' & \xrightarrow{\quad} & M & \xrightarrow{f} & N \\ & & \downarrow \overline{(-)} & \nearrow \exists! \bar{f} & \\ & & M/M' & & \end{array}$$

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

$$\begin{array}{ccccccc} & & \ker(f) & & & & \\ & \swarrow \simeq & \downarrow & & & & \\ \ker(f) \hookrightarrow & M & \xrightarrow{f|_{\mathrm{im}(f)}} & \mathrm{im}(f) \hookrightarrow & N & \twoheadrightarrow & N/\mathrm{im}(f) =: \mathrm{coker}(f) \\ & \downarrow \overline{(-)} & & \nearrow \simeq & & & \\ & M/\ker(f) =: \mathrm{coim}(f) & & & & & \end{array}$$

Définition 9.4.3 (Coimage, conoyau). 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 $\text{im}(f)$ et $M/\ker(f)$ sont isomorphes, on notera parfois $\text{coim}(f) := M/\ker(f)$ (coimage). On note $\text{coker}(f) := M'/\text{im}(f)$ (conoyaux).

9.4.1 Suites exactes, lemme du serpent, lemme des cinq

Définition 9.4.4. On dit qu'une suite de morphismes de A -modules

$$\cdots M_{n-1} \xrightarrow{u_{n-1}} M_n \xrightarrow{u_n} M_{n+1} \xrightarrow{u_{n+1}} \cdots$$

est exacte si $\text{im}(u_n) = \ker(u_{n+1})$ pour tout n .

Définition 9.4.5. Une suite exacte courte est une suite exacte de la forme :

$$0 \rightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \rightarrow 0.$$

Autrement dit $\ker(v) = \text{im}(u)$; $\ker(u) = \{0\}$, i.e. u est injectif et $\text{im}(v) = M''$, i.e. v est surjectif.

Remarque 9.4.6. La notion de suite exacte est au coeur de l'étude de la structure des A -modules. 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'').

En général si $M' \subset M$ est un sous-module de M il n'existe pas forcément un sous A -module $M'' \subset M$ tel que $M \simeq M' \oplus M''$. Plus précisément :

Lemme 9.4.7. Soit

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

une suite exacte courte de A -modules. Les propriétés suivantes sont équivalentes :

1. il existe un morphisme de A -modules $s : M'' \rightarrow M$ tel que $v \circ s = \text{Id}_{M''}$;
2. il existe un morphisme de A -modules $r : M \rightarrow M'$ tel que $r \circ u = \text{Id}_{M'}$;
3. il existe un isomorphisme de A -modules $f : M \xrightarrow{\sim} M' \oplus M''$ tel que $\iota_{M'} = f \circ u$ et $p_{M''} \circ f = v$.

Définition 9.4.8. 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 $s : M'' \rightarrow M$ est un morphisme de A -modules tel que $vs = \text{Id}_{M''}$ on vérifie que le morphisme de A -modules $\text{Id} - sv : M \rightarrow M$ a son image contenue dans $\ker(v) = u(M')$ et que $t := (u|^{u(M')})^{-1} \circ (\text{Id} - sv) : M \rightarrow M'$ vérifie bien $tu = \text{Id}_{M'}$.

$(2) \Rightarrow (3)$: Si $r : M \rightarrow M'$ est un morphisme de A -modules tel que $r \circ u = \text{Id}_{M'}$, on peut considérer $f := s \oplus v : M \rightarrow M' \oplus M''$. Par construction, $p_{M''} \circ f = v$ et $f \circ u(s(m)) = s(m) = \iota_{M'}(s(m))$ donc, comme $s : M \rightarrow M'$ est surjective, $f \circ u = \iota_{M'}$. Enfin, $f : M \rightarrow M' \oplus M''$ 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 $m' = r \circ u(m') = 0$. Donc, en fait $m = 0$. Il est surjectif car pour tout $m' \in M'$, $m'' \in M''$, on peut écrire $m'' = v(m) = v(m - ur(m) + u(m'))$ et $m' = ru(m') = s(m - us(m) + u(m'))$.

$(3) \Rightarrow (1)$: Si $f : M \xrightarrow{\sim} M' \oplus M''$ est un isomorphisme de A -modules tel que $p_{M''} \circ f = v$ et $f \circ u = \iota_{M'}$, on peut considérer $s := f^{-1} \circ \iota_{M''} : M'' \rightarrow M$. Par construction $vs(m) = vf^{-1}\iota_{M''} = p_{M''}\iota_{M''} = \text{Id}_{M''}$. \square

9.4.1.2

Exercices 9.4.9. 1. Montrer que, si $n \geq 2$ est un entier, la suite exacte courte de \mathbb{Z} -modules $0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow \mathbb{Z}/n \rightarrow 0$ n'est pas scindée.

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

1. $X \cdot (a, b) = (a + b, b)$ et la suite exacte courte $0 \rightarrow \mathbb{Z} \xrightarrow{a \rightarrow (a, 0)} \mathbb{Z}^2 \rightarrow \mathbb{Z} \rightarrow 0$.

2. $X \cdot (a, b) = (b, a)$ et la suite exacte courte $0 \rightarrow \mathbb{Z} \xrightarrow{a \rightarrow (a, a)} \mathbb{Z}^2 \rightarrow \mathbb{Z} \rightarrow 0$

Déterminer si ces suites exactes courtes sont scindées. Même question si l'on remplace \mathbb{Z} par \mathbb{Q}

9.4.1.3 Exercice. (Lemme du serpent)

1. Soit

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

un diagramme commutatif de morphismes de A -modules. Montrer que $u' : M' \rightarrow M$ induit un morphisme canonique $\ker(\alpha') \rightarrow \ker(\alpha)$ et que $v' : N' \rightarrow N$ induit un morphisme canonique $\operatorname{coker}(\alpha') \rightarrow \operatorname{coker}(\alpha)$.

2. Soit

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

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

- (a) Construire un morphisme 'naturel' $\delta : \ker(\alpha'') \rightarrow \operatorname{coker}(\alpha')$;
- (b) Montrer que la suite de morphismes

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

est exacte.

- (c) Montrer que si α' , α'' sont injectives (resp. surjectives) alors α est injective (resp. surjective).
- (d) On suppose de plus que $u' : M' \rightarrow M$ est injective et $v : N \rightarrow N''$ est surjective. Montrer que si deux des trois morphismes α , α' , α'' sont des isomorphismes alors le troisième l'est aussi.
- (e) Soit $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ 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

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

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

3. (Lemme des cinq) Soit

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

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.

Chapitre 10

Conditions de finitude

Soit A un anneau commutatif.

10.1 Lemme

Lemme 10.1.1. *Soit M un A -module. Les conditions suivantes sont équivalentes.*

1. *Toute suite croissante de sous- A -modules de M est stationnaire.*
2. *Tout ensemble non vide de sous- A -modules de M admet un élément maximal pour l'inclusion.*
3. *Tout sous- A -module de M est de type fini.*

Définition 10.1.2. Un A -module M vérifiant les conditions équivalentes du lemme 10.1 est dit *noethérien*.

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, \dots, m_r une famille de générateurs de U . Chaque m_i est dans M_{n_i} pour un certain $n_i \geq 0$. Avec

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

on a $M_n = M_N$, $n \geq N$. □

Remarque. Un anneau A est en particulier noethérien au sens de 3 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

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

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 10.2 est dit *artinien*. On laisse en exercice la preuve du lemme 10.2, qui est exactement similaire à celle du lemme 10.1

10.3 Exemple

1. Le \mathbb{Z} -module \mathbb{Q} n'est ni noetherien ni artinien. En effet, on a la suite infinie de sous \mathbb{Z} -modules

$$\cdots \subsetneq p^{n+1}\mathbb{Z} \subsetneq p^n\mathbb{Z} \subsetneq \cdots \subsetneq p\mathbb{Z} \subsetneq \mathbb{Z} \subsetneq p^{-1}\mathbb{Z} \subsetneq \cdots \subsetneq p^{-n}\mathbb{Z} \subsetneq p^{-n-1}\mathbb{Z} \subsetneq \cdots$$

2. Le \mathbb{Z} -module régulier est noetherien mais pas artinien. Il est noetherien car \mathbb{Z} est principal donc tous ses idéaux sont de type fini (et même engendrés par un seul élément). Il n'est pas artinien car on a toujours la suite infinie

$$\cdots \subsetneq p^{n+1}\mathbb{Z} \subsetneq p^n\mathbb{Z} \subsetneq \cdots \subsetneq p\mathbb{Z} \subsetneq \mathbb{Z}$$

3. Le \mathbb{Z} -module $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ est artinien mais pas noetherien. En effet, les éléments de $M := \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ sont tous d'ordre fini, une puissance de p . Pour chaque $n \in \mathbb{Z}$, $n \geq 0$ notons $M_n := \mathbb{Z}\frac{1}{p^n} + \mathbb{Z}/\mathbb{Z} \subset \mathbb{Z}$. On a la suite strictement croissante de sous- \mathbb{Z} -modules

$$M_0 = \{0\} \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots M$$

donc M n'est pas noetherien. Soit maintenant $N \subset M$ un sous- \mathbb{Z} -module. Distinguons deux cas.

- (a) Le sup des ordres des éléments de N est fini, égal à p^n . Soit $a \in N$ d'ordre maximal p^n ; on peut donc écrire $a = \frac{b}{p^n} \in \mathbb{Z}[\frac{1}{p}] + \mathbb{Z}/\mathbb{Z}$ avec $1 \leq b \leq p^n - 1$, $p \nmid b$. Comme p est premier, il existe $u, v \in \mathbb{Z}$ tels que $ub + vp^n = 1$ donc $ua = \frac{1}{p^n} \in N$. Cela montre que $M_n \subset N$. Inversement, tout élément $a \in N$ s'écrit sous la forme $a = \frac{u}{p^m} \in \mathbb{Z}[\frac{1}{p}] + \mathbb{Z}/\mathbb{Z}$ avec $1 \leq b \leq p^m - 1$, $p \nmid b$ et $m \leq n$. Mais on peut aussi écrire $a = \frac{up^{n-m}}{p^n}$. Cela montre que $N \subset M_n$.
- (b) Il existe une application strictement croissante $\phi : \mathbb{N} \rightarrow \mathbb{N}$ tel que N contient un élément a_n d'ordre exactement $p^{\phi(n)}$, $n \geq 0$. L'argument précédent montre que $\mathbb{Z}a_n = M_{\phi(n)} \subset N$. Donc $M = \bigcup_{n \geq 0} M_n \subset N$.

Les seuls sous \mathbb{Z} -modules de M sont donc M et les M_n , $n \geq 0$. Comme ils sont strictement ordonnés pour l'inclusion $M_0 = \{0\} \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots M$, on en déduit que M est artinien.

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 $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ une suite exacte courte de A -modules. Alors M est noethérien (resp. artinien) si et seulement si M' et M'' sont noethériens (resp. artiniens).
2. Une somme directe finie de A -modules noethériens (resp. artiniens) est encore noethérien (resp. artinien).

3. Tout module de type fini sur un anneau noethérien (resp. artinien) est noethérien (resp. artinien). Montrer que tout module de type fini sur un anneau noethérien est de présentation finie.

Démonstration. 1. Supposons M noethérien (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'' noethériens (resp. artiniens). Soit $M_1 \subset \dots \subset M_n \subset M_{n+1} \subset \dots \subset M$ 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 $(M_N + M')/M' = (M_n + M')/M'$ $n \geq N$. La conclusion résulte du lemme du serpent appliqué à

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

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

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

3. D'après 1.3.4 (2) $A^{\oplus n}$ est noethérien (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 noethérien 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 $f : M \rightarrow M$ un endomorphisme de A -module.

1. Si M est noethérien 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 noethérien 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

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

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

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

3. (3) Comme M est artinien et noethérien, il existe un entier $N \geq 1$ tel que

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

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 $\text{im}(f^N) = \text{im}(f^{2N})$ 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.

□

Chapitre 11

Modules indécomposables, Krull-schmidt

11.1 Modules indécomposables

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

Un anneau E est dit *local* si $E \setminus E^\times$ est un idéal ; auquel cas, $E \setminus E^\times$ est l'unique idéal bilatère maximal de E .

11.2

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

Démonstration. Supposons E local et qu'on puisse écrire $M = M' \oplus M''$ avec $M', M'' \subset M$ deux sous A -modules non nuls. Notons $e := \iota_{M'} \circ p_{M'} \in E$ la projection de M sur M' parallèlement à M'' . On a $e, 1 - e \in E \setminus E^\times$. Mais si E est local, $E \setminus E^\times$ est un idéal donc $1 = e + (1 - e) \in E \setminus E^\times$: contradiction. Supposons maintenant que M est un A -module artinien et noethérien indécomposable, d'après l'Lemma 10.5 (3), tout élément non nul de E est soit inversible soit nilpotent. En particulier $J := E \setminus E^\times$ est l'ensemble des éléments nilpotents de E . Il suffit de montrer que J est un idéal bilatère. Soit donc $j \in J$ et $e \in E$. Comme j est nilpotent on a

$\ker(j) \neq 0$ et $\operatorname{im}(j) \neq M$ (Lemme 10.5 (1), (2)). Donc aussi $\ker(ej) \neq 0$ et $\operatorname{im}(je) \neq M$, ce qui montre que $ej, je \in E \setminus E^\times = J$. Donc $EJ = JE = J$. Il reste à voir que J est stable par addition. Soit $j, j' \in J$, si $j + j' \in E^\times$ il existerait $e \in E$ tel que $ej = 1 - ej'$. Comme $ej' \in J$, on a forcément $1 - ej' \in E^\times$ (d'inverse $\sum_{n \geq 0} (ej')^n$), ce qui contredit le fait que $j \in J$. \square

11.3 Théorème de Krull-Schmidt

Notons $\operatorname{Ind}(A)$ l'ensemble des classes d'isomorphismes de A -modules indécomposables.

11.3.1

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

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

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

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

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

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

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

...

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

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

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

$$M \supset M_1^{(0)} \supset M_1^{(0)} \supset \cdots \supset M_1^{(n)} \supset M_1^{(n+1)} \supset \cdots$$
$$M \oplus M' \simeq N_1 \oplus \cdots \oplus N_s =: N$$
$$\Psi = \begin{pmatrix} \psi \\ \psi' \end{pmatrix} : N \xrightarrow{\sim} M \oplus M'.$$
$$\text{Id}_M = \psi \circ \phi = \sum_{1 \leq i \leq s} \psi \circ \iota_i \circ p_i \circ \phi$$
$$0 \longrightarrow \ker(\psi \circ \iota_i) \longrightarrow N_i \xrightarrow{\psi \circ \iota_i} \operatorname{im}(\psi \circ \iota_i) \longrightarrow 0$$

$\quad\quad\quad \curvearrowright \quad\quad\quad$
 $\quad\quad\quad p_i \circ \phi \circ \chi_i^{-1}$

$$N_i = \ker(\psi \circ \iota_i) \oplus \operatorname{im}(p_i \circ \phi).$$
$$0 \rightarrow M \xrightarrow{\iota} M \oplus M' \xrightarrow{p} M' \rightarrow 0$$

$$0 \rightarrow \bigoplus_{i \neq j} N_j \xrightarrow{\Psi_{ol'_i}} M \oplus M' \xrightarrow{p_i \circ \Phi} N_i \rightarrow 0.$$

Sorbonne université

la preuve en exercice au lecteur. \square

11.3.2

Lemme.

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

Chapitre 12

Modules de type fini sur les anneaux principaux

12.1 Préambule

Supposons que A soit un anneau principal, et soit M un A -module. Un élément $m \in M$ est dit *de torsion* s'il existe $0 \neq a \in A$ tel que $am = 0$. On note $T_M \subset M$ l'ensemble des éléments de torsion de M . On vérifie immédiatement que c'est un sous A -module et que le A -module M/T_M est sans torsion. Le A -module M s'insère donc dans la suite exacte courte

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

où T_M est de torsion et M/T_M est sans torsion. Cela indique la voie pour classifier les A -modules de type fini : montrer que la suite exacte courte $(*)$ se scinde, ce qui par le Lemme 9.4.1.1 impliquera automatiquement que

$$M \xrightarrow{\sim} T_M \oplus M/T_M$$

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

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

En fait, on va plutôt procéder dans l'ordre suivant. Notons que comme A est noethérien (car principal) et M de type fini, M est noethérien. Donc T_M et M/T_M sont aussi noethériens donc de type fini.

1. Tout d'abord, la raison pour laquelle on se restreint aux A -modules de type fini provient du lemme suivant.

Lemme 12.1.1. *Un A -module de type fini est noethérien. Un A -module de type fini et de torsion est noethérien et artinien.*

Démonstration. Comme A est principal, tous ses sous A -modules (=idéaux) sont de type fini donc A est noethérien ; la première partie de l'énoncé résulte donc du Lemme 10.4. Supposons M de torsion. Soit $m_1, \dots, m_r \in M$ un système de générateurs. Pour chaque $i = 1, \dots, r$ on peut trouver un élément $0 \neq a_i \in A$ tel que $a_i m_i = 0$. On a donc une factorisation

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

D'après le Lemme 10.4, il suffit donc de montrer que les A -module de la forme A/Aa avec $0 \neq a \in A$ sont artiniens. Soit

$$A/Aa =: M_0 \supset M_1 \supset \dots \supset M_n \supset M_{n+1} \supset \dots$$

une suite décroissante de sous A -modules. Notons $\pi : A \rightarrow A/Aa$ la projection canonique et posons :

$$I_n := \pi^{-1}(M_n), \quad n \geq 0.$$

Par construction on obtient une suite décroissante d'idéaux

$$A = I_0 \supset I_1 \supset \dots \supset I_n \supset I_{n+1} \supset \dots Aa.$$

Chacun de ces idéaux est de la forme $I_n = Aa_n$ avec $0 \neq a_n \in A$ et $a_n | a$. Mais comme un anneau principal est factoriel, a n'a qu'un nombre fini de diviseurs deux à deux non associés. Il n'y a donc qu'un nombre fini d'idéaux dans la suite I_n , $n \geq 0$. \square

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

Lemme 12.1.2. *Si M'' est un A -module libre alors toute suite exacte courte de A -modules $0 \rightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \rightarrow 0$ est scindée.*

Démonstration. On construit une section en utilisant la propriété universelle de la somme directe. Plus précisément, quitte à composer v par un isomorphisme, on peut supposer que $M'' = A^{(I)}$. Pour chaque $i \in I$ notons $e_i = (\delta_{i,j})_{j \in I} \in A^{(I)}$ et choisissons $m_i \in I$ tel que $v(m_i) = e_i$. Le choix de m_i définit un morphisme de A -module $s_i : Ae_i \xrightarrow{e_i \mapsto m_i} Am_i \hookrightarrow M$. Par propriété universelle des $\iota_i : Ae_i \rightarrow A^{(I)}$, $i \in I$, on en déduit un unique morphisme $s : A^{(I)} \rightarrow M$ tel que $s \circ \iota_i = s_i$, $i \in I$. Par construction $v \circ s = \text{Id}$. On conclut par l'Exercice 9.4.1.1. \square

3. D'après le Lemme 12.1.1 et le Théorème de Krull-Schmidt 11.3.1, T_M est totalement décomposable ; le point sera donc de classier les modules indécomposables de torsion sur un anneau principal A . On montrera que ce sont exactement les A -modules de la forme A/\mathfrak{p}^n , où \mathfrak{p} est un idéal premier (=maximal) de A et $n \geq 0$.

12.2 Classification des A -modules de type fini sans torsion

Supposons d'abord que A est seulement un anneau commutatif intègre.

Lemme 12.2.1. *Un A -module de type fini sans torsion est isomorphe à un sous A -module d'un A -module libre de type fini.*

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

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

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

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

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

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

est injectif, puisque M est sans torsion. □

Lemme 12.2.2 (Classification des A -modules libres de type fini par le rang). *1. Le A -module libre $A^{(I)}$ est de type fini si et seulement si $|I| < +\infty$.*
2. Soit I, J deux ensembles finis. Alors $A^{(I)}$ et $A^{(J)}$ sont isomorphes comme A -modules si et seulement si $|I| = |J|$.

Démonstration. L'idée est de se ramener au cas des espaces vectoriels sur un corps pour lesquels le lemme est connu. Soit donc M un A -module libre de type fini et $\mathfrak{m} \subset A$ un idéal maximal. Comme M est de type fini, le $k := A/\mathfrak{m}$ espace vectoriel $M/\mathfrak{m}M$ est de dimension finie - disons r - sur k . Soit I un ensemble pour lequel on a un isomorphisme de A -modules

$$f : A^{(I)} \xrightarrow{\sim} M.$$

Posons $m_i := f(e_i)$, où e_i est le ' i -ème vecteur de la base canonique', $i \in I$. On va montrer que $|I| = r$. Pour cela, il suffit de montrer que les images \overline{m}_i , $i \in I$ des m_i , $i \in I$ dans $M/\mathfrak{m}M$ forment une k -base de $M/\mathfrak{m}M$. Puisque f est surjective, les \overline{m}_i , $i \in I$ forment une famille génératrice. Montrons qu'elle est libre. Soit $a : I \rightarrow A$ à support fini telle que

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

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

Le Lemme 12.2.2 montre en particulier que si M est un A -module libre de type fini il existe un unique entier $r \geq 1$ tel que $M \simeq A^{\oplus r}$. On appelle cet entier le *rang* du A -module libre M . C'est également la dimension du A/\mathfrak{m} -espace vectoriel $M/\mathfrak{m}M$, pour \mathfrak{m} un idéal maximal de 1.

Supposons maintenant que A est *principal*.

Lemme 12.2.3. *Un sous A -module d'un A -module libre de rang fini r est un A -module libre de rang $\leq r$.*

Démonstration. On procède par récurrence sur r . Si $r = 1$, cela résulte du fait que A est principal. Supposons que l'énoncé du Lemme 12.2.3 est vérifié pour tout A -module libre de rang $\leq r$. Soit $M \subset A^{\oplus(r+1)}$ un sous A -module. Notons $p_{r+1} : A^{\oplus(r+1)} \rightarrow A$ la $r + 1$ -ième projection canonique. Comme $\ker(p_{r+1}) \simeq A^{\oplus r} \subset A^{\oplus(r+1)}$ est un A -module libre de rang r , par hypothèse de récurrence, le sous A -module $M \cap \ker(p_{r+1}) \subset \ker(p_{r+1})$ est un A -module libre de rang $s \leq r$. Comme $p_{r+1}(M) \subset A$ est un idéal et que A est principal, il existe $d_0 \in A$ et $m_0 \in M$ tel que $p_{r+1}(M) = Ad_0 \xleftarrow{d_0} A$ et on conclut par le Lemme 12.1.2. \square

On vient donc de montrer

Corollaire 12.2.4. *Un A -module de type fini sans torsion est libre de rang fini. Plus précisément, l'application $\mathbb{Z}_{\geq 0} \rightarrow \text{Mod}_A$, $r \rightarrow A^{\oplus r}$ induit une bijection de $\mathbb{Z}_{\geq 0}$ sur l'ensemble des classes d'isomorphismes de A -modules de type fini sans torsion.*

En particulier, M/T_M est un A -module libre de rang fini - disons r - donc, par le Lemme 12.1.2 on a

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

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

12.3 Classification des A -modules de type fini de torsion

Soit A un anneau principal.

Théorème 12.3.1. *Les A -modules de type fini de torsion qui sont indécomposables sont exactement les A -modules de la forme A/\mathfrak{p}^n , où $\mathfrak{p} \subset A$ est un idéal premier non nul et $n \in \mathbb{Z}_{\geq 0}$.*

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

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

a un unique idéal maximal (c'est par exemple la factorialité de A) - $\mathfrak{p}/\mathfrak{p}^n$, donc est local (ici A/\mathfrak{p}^n est commutatif). Le fait que A/\mathfrak{p}^n est indécomposable résulte alors du lemme 11.2.

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

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

l'idéal annulateur de m et on se fixe un générateur $a_m \in \text{Ann}_A(m)$. On note également

$$\text{Ann}_A(M) := \bigcap_{m \in M} \text{Ann}_A(m) \subset A$$

l'idéal annulateur de M .

12.3.1.1.

Lemme 12.3.2. *Il existe $m \in M$ tel que $\text{Ann}_A(m) = \text{Ann}_A(M)$.*

Notons $B := A/\text{Ann}_A(m) = A/\text{Ann}_A(M)$ et considérons la suite exacte courte

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

On notera que comme $\text{Ann}_A(M)$ annule M , cette suite est également une suite de B -modules.

Lemme 12.3.3. *La suite exacte courte de B -modules*

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

est scindée.

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

$$M \simeq A/\text{Ann}_A(M) \oplus M/Am$$

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

Preuve du lemme 12.3.3 Soit m_1, \dots, m_r un système de générateurs de M comme A -module.

On a

$$\text{Ann}_A(M) = \cap_{1 \leq i \leq r} \text{Ann}_A(m_i).$$

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

$$\text{Ann}_A(m_1) \cap \text{Ann}_A(m_2) = \text{Ann}_A(m_3).$$

Ecrivons $\text{Ann}_A(m_i) = Aa_i$, $i = 1, 2$. Comme A est factoriel, en utilisant la décomposition en produit de facteurs irréductibles de a_1 et a_2 , on peut écrire $a_1 = \alpha_1\beta_1$ et $a_2 = \alpha_2\beta_2$ avec α_1, α_2 premier entre eux de produit 'le' plus petit commun multiple de a_1 et a_2 . Posons $m_3 := \beta_1m_1 + \beta_2m_2$ et vérifions que m_3 convient. On a clairement $\text{Ann}_A(m_1) \cap \text{Ann}_A(m_2) \subset \text{Ann}_A(m_3)$. Pour l'inclusion réciproque, soit $a \in \text{Ann}_A(m_3)$. On a $a\beta_1m_1 = -a\beta_2m_2$. Par Bézout, il existe $u, v \in A$ tels que $u\alpha_1 + v\alpha_2 = 1$. On a donc

$$a\beta_1m_1 = (u\alpha_1 + v\alpha_2)a\beta_1m_1 = \underbrace{aua_1m_1}_{=0} + v\alpha_2a\beta_1m_1 = -\underbrace{av\alpha_2m_2}_{=0} = 0.$$

Donc $a\beta_1 \in \text{Ann}_A(m_1) = Aa_1$ et $a\beta_2 \in \text{Ann}_A(m_2) = Aa_2$ en particulier a est un multiple commun de α_1 et α_2 donc de $\alpha_1\alpha_2 = \text{ppcm}(a_1, a_2)$. Donc $a \in \text{Ann}_A(m_1) \cap \text{Ann}_A(m_2)$. \square

Preuve du Lemme 12.3.1.2. Introduisons l'ensemble \mathcal{E} des couples (u, N) où $m \in N \subset M$ est un sous- B -module et $u : N \rightarrow B$ un morphisme de B -modules tel que $u(m) = 1$. On munit \mathcal{E} de la relation d'ordre \leq définie par $(u_1, N_1) \leq (u_2, N_2)$ si $N_1 \subset N_2$ et $u_2|_{N_1} = u_1$. \mathcal{E} est non-vidé : par définition $B = A/\text{Ann}_A(m)$ donc on a un isomorphisme $v : B \xrightarrow{\sim} Bm$ et $(Am, v^{-1}) \in \mathcal{E}$. Par définition, \mathcal{E} est un ensemble ordonné inductif donc admet un élément maximal (u, N) (en fait, ici, on peut invoquer le fait que M est noethérien, ce qui permet d'éviter le Lemme de Zorn). Montrons que $N = M$. Sinon, soit $\mu \in M \setminus N$ et montrons qu'on peut étendre $u : N \rightarrow B$ en $u_1 : N + B\mu \rightarrow B$. Pour cela, il faut 'deviner' la bonne valeur de $u_1(\mu)$. Introduisons l'idéal

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

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

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

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

12.3.1

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

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

telle que

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

Démonstration. Comme M est artinien et noethérien, d'après le Théorème de Krull-Schmidt 11.3.1, M se décompose de façon unique comme somme directe de modules indécomposables. D'après le Théorème 12.3.1, cette décomposition s'écrit

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

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

$$\alpha_{M,-} : \text{Spec}(A) \rightarrow \mathbb{Z}_{\geq 0}^{(\mathbb{Z}_{\geq 0})}$$

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

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

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

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

12.4 Applications

12.4.1 Classification des groupes abéliens de type fini

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

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

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

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

12.4.2

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

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

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

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

1. Soit $u, u' : V \rightarrow V$ deux endomorphismes. Montrer qu'il existe $\phi \in \text{Aut}_k(V)$ tel que $u = \phi \circ u' \circ \phi^{-1}$ si et seulement si u et u' ont mêmes invariants de similitude.
2. Calculer le polynôme minimal et le polynôme caractéristique de u en fonction de sa suite d'invariants de similitude. Montrer plus précisément qu'il existe une base du k -espace

vectorel V dans laquelle u a pour matrice la matrice diagonale par blocs dont les blocs diagonaux sont les matrices compagnons des $P_{u,i}$.

3. Calculer le nombre de classes de conjugaison (sous $\mathrm{GL}_n(\mathbb{F}_q)$) dans $M_n(\mathbb{F}_q)$, dans $\mathrm{GL}_n(\mathbb{F}_q)$.

Au lieu d'appliquer le Corollaire 12.3.1 sous la forme énoncée, on peut l'appliquer avec la décomposition donnée par Krull-Schmidt (*cf.* preuve) *i.e.* il existe une unique famille de polynômes irréductibles P_1, \dots, P_s et des familles d'entiers $n_{i,1} \geq \dots \geq n_{i,r_i} > 0$, $i = 1, \dots, s$ tels que

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

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

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

où U est ma matrice carrée de taille $d_i \times d_i$ avec $u_{1,d_i} = 1$ et $u_{i,j} = 0$ sinon.

12.4.3

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

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

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

Démonstration. L'unicité de s et de la suite $Ad_1 \supset Ad_2 \supset \dots \supset Ad_s$ résulte du Corollaire 12.3.1 car $r - s$ est le rang de la partie libre de M/N et $Ad_1 \supset Ad_2 \supset \dots \supset Ad_s$ est la suite des invariants de la partie de torsion de M/N . L'existence est un peu plus délicate. On procède par récurrence sur r . Si $r = 1$, c'est la traduction du fait que A est principal. Si $r \geq 1$, l'idée

est de construire d_1, e_1 à partir de l'inclusion $N \hookrightarrow M$. Pour cela, on introduit l'ensemble \mathcal{E} des idéaux de la forme $f(N) \subset A$, où $f : M \rightarrow A$ est un morphisme de A -module. Comme A est noethérien, \mathcal{E} contient au moins un élément maximal $f(N) = Ad = Af(n)$.

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

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

Par maximalité de $f(N)$, cela implique $f(N) = Ad = A\delta = (uf + vg)(N)$. En particulier, pour tout $n' \in N$, d divise $(uf + vg)(n')$. Mais $f(N) = Ad$, donc d divise aussi $f(n')$. On en déduit que d divise $vg(n')$ et comme d est premier avec v , que d divise $g(n')$. *In fine*, on a $g(N) \subset Ad = f(N)$ comme annoncé.

2. Il existe $\mu \in M$ tel que $d\mu = n$. Choisissons une A -base quelconque e_1, \dots, e_r de M et notons $p_i : M \rightarrow Am_i \simeq A$ la projection correspondante sur la i -ème coordonnée. On a, dans cette base, $n = \sum_{1 \leq i \leq r} a_i e_i$ et en appliquant (1) aux p_i , on obtient que d divise a_i , $i = 1, \dots, r$. Donc en écrivant $a_i = db_i$ pour un certain $b_i \in A$, $i = 1, \dots, r$, on peut prendre $\mu = \sum_{1 \leq i \leq r} b_i e_i$.
3. De $d\mu = n$, on déduit $f(d\mu) = df(\mu) = f(n) = d$ donc comme A est intègre, $f(\mu) = 1$. Cela donne une décomposition $M \simeq \ker(f) \oplus A\mu$ ($m = (m - f(m)\mu) + f(m)\mu$) telle que $N = \ker(f) \cap N \oplus Ad\mu$. On peut donc appliquer l'hypothèse de récurrence à $\ker(f) \cap N \subset \ker(f)$ puisqu'on sait que $\ker(f)$ est un A -module libre de rang r pour obtenir une suite $A \supsetneq Ad_2 \supset \dots \supset Ad_s \supsetneq 0$ d'idéaux de A et $m_2, \dots, m_r \in \ker(f)$ tels que

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

Enfin, en appliquant à nouveau (1) à la projection $M = A\mu \oplus \bigoplus_{2 \leq i \leq r} Am_i \rightarrow Am_2 \simeq A$, on voit que d divise d_2 .

□

12.4.3.0.2 Corollaire. (Classes d'équivalence) *On considère l'action de $\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ sur $M_{n,m}(A)$ donnée par $(P, Q) \cdot M = PMQ^{-1}$. L'ensemble des classes d'équivalence $M_{n,m}(A) / \mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ est canoniquement en bijection avec les suites $Ad_1 \supset Ad_2 \supset \dots \supset Ad_n$ d'idéaux de A .*

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

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

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

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

est scindée. Notons $s : f(M) \rightarrow M$ un scindage. On a alors $M \simeq \ker(f) \oplus s(f(M))$. Comme A est principal et M est un A -module libre, $\ker(f) \subset M$ est encore un A -module libre. En concaténant une A -base de $\ker(f)$ et la A -base $s(\nu_1), \dots, s(\nu_n)$ de $f(M)$, on obtient une A -base μ_1, \dots, μ_m de M . La matrice de f dans les bases μ_1, \dots, μ_m et ν_1, \dots, ν_n est de la forme

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

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

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

12.4.3.0.3 Exercice. Soit M un \mathbb{Z} -module libre de rang fini m et $\phi \in \text{End}_{\mathbb{Z}}(M)$ tel que $\phi \otimes \mathbb{Q} \in \text{Aut}_{\mathbb{Q}}(M \otimes \mathbb{Q})$ est inversible. Montrer que $\phi(M) \subset M$ est d'indice fini et calculer $[M : \phi(M)]$.

Chapitre 13

Produit tensoriel

13.1 Construction

Soit M_1, \dots, M_r et M des A -modules. Notons

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

l'ensemble des applications $f : M_1 \times \dots \times M_r \rightarrow M$ qui sont r - A -linéaires *i.e.* telles que $f \circ \iota_i : M_i \rightarrow M$ est un morphisme de A -modules, $i = 1, \dots, r$.

Notons

$$\Sigma := A^{(M_1 \times \dots \times M_r)},$$

le A -module libre engendré par $M_1 \times \dots \times M_r$, $(m_1, \dots, m_r) \in M_0$ l'élément correspondant au terme avec des 0 partout sauf en l'indice (m_1, \dots, m_r) et $R \subset \Sigma$ le sous A -module engendré par les éléments de la forme

$$(m_1, \dots, a_i m_i + a'_i m'_i, \dots, m_r) - a_i(m_1, \dots, m_i, \dots, m_r) - a'_i(m_1, \dots, m'_i, \dots, m_r).$$

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

$$\begin{array}{llll} p : M_1 \times \dots \times M_r & \rightarrow & A^{(M_1 \times \dots \times M_r)} & \rightarrow M_1 \otimes_A \dots \otimes_A M_r \\ (m_1, \dots, m_r) & \rightarrow & 1 \cdot (m_1, \dots, m_r) & \rightarrow (m_1, \dots, m_r) \bmod M_{00} =: m_1 \otimes \dots \otimes m_r \end{array}$$

on vérifie facilement que $p : M_1 \times \dots \times M_r \rightarrow M_1 \otimes_A \dots \otimes_A M_r$ est une application A - r -linéaire. On prendra garde que $p : M_1 \times \dots \times M_r \rightarrow M_1 \otimes_A \dots \otimes_A M_r$ n'est pas surjective en général mais que, $M_1 \otimes_A \dots \otimes_A M_r$ est engendré comme A -module par les éléments de la forme $m_1 \otimes \dots \otimes m_r$.

13.1.1

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

Démonstration. Vérifions que $T := M_1 \otimes_A \dots \otimes_A M_r$ et l'application r - A -linéaire $p : M_1 \times \dots \times M_r \rightarrow M_1 \otimes_A \dots \otimes_A M_r$ conviennent. Si $\bar{f} : M_1 \otimes_A \dots \otimes_A M_r \rightarrow M$, la condition $p \circ \bar{f} = f$ impose $\bar{f}(m_1 \otimes \dots \otimes m_r) = f(m_1, \dots, m_r)$. Comme $M_1 \otimes_A \dots \otimes_A M_r$ est engendré, comme A -module, par les éléments de la forme $m_1 \otimes \dots \otimes m_r$, cela montre l'unicité de \bar{f} sous réserve de son existence. Par propriété universelle des $\iota_{\underline{m}} : A \hookrightarrow A^{(M_1 \times \dots \times M_r)}$, $\underline{m} = (m_1, \dots, m_r) \in M_1 \times \dots \times M_r$, il existe un unique morphisme de A -modules $F : M_0 = A^{(M_1 \times \dots \times M_r)} \rightarrow M$ tel que $F \circ \iota_{\underline{m}} : A \rightarrow M$ est le morphisme qui envoie 1 sur $f(m_1, \dots, m_r)$. Comme $f : M_1 \times \dots \times M_r \rightarrow M$ est r - A -linéaire, $M_{00} \subset \ker(F)$ donc $F : M_0 \rightarrow M$ se factorise en un morphisme de A -modules $\bar{f} : M_1 \otimes_A \dots \otimes_A M_r \rightarrow M$ tel que $p \circ \bar{f} = F$; en particulier

$$p \circ \bar{f}(m_1, \dots, m_r) = F(m_1, \dots, m_r) = f(m_1, \dots, m_r), \quad (m_1, \dots, m_r) \in M_1 \times \dots \times M_r.$$

□

Comme d'habitude, $p : M_1 \times \dots \times M_r \rightarrow M_1 \otimes_A \dots \otimes_A M_r$ est unique à unique isomorphisme près.

On peut aussi réécrire 13.1.1 en disant que pour tout A -module M l'application canonique

$$\mathrm{Hom}_A(M_1 \times \dots \times M_r, M) \rightarrow L_{r,A}(M_1 \times \dots \times M_r, M), \quad f \rightarrow p \circ f$$

est bijective ou encore, plus visuellement,

$$\begin{array}{ccc} M_1 \times \dots \times M_r & \xrightarrow{\forall f} & M \\ \downarrow p & \nearrow \exists! \bar{f} & \\ M_1 \otimes_A \dots \otimes_A M_r & & \end{array}$$

Si $f_i : M_i \rightarrow N_i$, $i = 1, \dots, r$ sont r morphismes de A -modules, l'application

$$\begin{aligned} (f_1, \dots, f_r) \quad M_1 \times \dots \times M_r &\rightarrow N_1 \otimes_A \dots \otimes_A N_r \\ (m_1, \dots, m_r) &\rightarrow f_1(m_1) \otimes \dots \otimes f_r(m_r) \end{aligned}$$

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

13.2 Propriétés élémentaires

13.2.1

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

$$\begin{aligned} M \otimes_A (\bigoplus_{i \in I} M_i) &\xrightarrow{\sim} \bigoplus_{i \in I} (M \otimes_A M_i) \\ m \otimes (m_i)_{i \in I} &\rightarrow (m \otimes m_i)_{i \in I} \end{aligned}$$

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

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

13.2.2

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

$$\begin{aligned} L \otimes_A (M \otimes_A N) &\xrightarrow{\sim} (L \otimes_A M) \otimes_A N \\ l \otimes (m \otimes n) &\rightarrow (l \otimes m) \otimes n \end{aligned}$$

$$\begin{aligned} M \otimes_A N &\xrightarrow{\sim} N \otimes_A M \\ m \otimes n &\rightarrow n \otimes m \end{aligned}$$

13.2.3

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

$$\begin{aligned} A \otimes_A M &\xrightarrow{\sim} M \\ a \otimes m &\rightarrow am \end{aligned}$$

13.2.4

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

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

$$A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_r)} \xrightarrow{\sim} A^{(I_1 \times \dots \times I_r)}$$

qui envoie $e_{i_1} \otimes \dots \otimes e_{i_r}$ sur $e_{(i_1, \dots, i_r)}$, $(i_1, \dots, i_r) \in I_1 \times \dots \times I_r$.

Démonstration. On peut le déduire formellement des Lemmes 13.2.1, 13.2.2, 13.2.3 :

$$\begin{aligned} A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_r)} &\xrightarrow{\sim} (A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_{r-1})}) \otimes_A A^{(I_r)} \\ &\xrightarrow{\sim} ((A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_{r-1})}) \otimes_A A)^{(I_r)} \\ &\xrightarrow{\sim} (A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_{r-1})})^{(I_r)} \\ &\xrightarrow{\sim} \dots \xrightarrow{\sim} A^{(I_1 \times \dots \times I_r)}. \end{aligned}$$

On peut aussi donner un argument direct. En effet, l'application $A^{(I_1)} \times \dots \times A^{(I_r)} \xrightarrow{\sim} A^{(I_1 \times \dots \times I_r)}$, $((a_{i_1})_{i_1 \in I_1}, \dots, (a_{i_r})_{i_r \in I_r}) \rightarrow (a_{i_1} \dots a_{i_r})_{(i_1, \dots, i_r) \in I_1 \times \dots \times I_r}$ est r - A -linéaire donc se factorise en un morphisme de A -modules $\phi : A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_r)} \rightarrow A^{(I_1 \times \dots \times I_r)}$ tel que $\phi((a_{i_1})_{i_1 \in I_1} \otimes \dots \otimes (a_{i_r})_{i_r \in I_r}) = (a_{i_1} \dots a_{i_r})_{(i_1, \dots, i_r) \in I_1 \times \dots \times I_r}$. Inversement, pour chaque $(i_1, \dots, i_r) \in I_1 \times \dots \times I_r$ on dispose du morphisme de A -modules $\psi_{(i_1, \dots, i_r)} : A \rightarrow A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_r)} \xrightarrow{\sim} A^{(I_1 \times \dots \times I_r)}$, $a \rightarrow ae_{i_1} \otimes \dots \otimes e_{i_r}$ donc, par propriété universelle de la somme directe, d'un morphisme de A -modules $\psi = \bigoplus_{(i_1, \dots, i_r) \in I_1 \times \dots \times I_r} \psi_{(i_1, \dots, i_r)} : A^{(I_1 \times \dots \times I_r)} \rightarrow A^{(I_1)} \otimes_A \dots \otimes_A A^{(I_r)}$ tel que $\psi \circ \iota_{(i_1, \dots, i_r)} = \psi_{(i_1, \dots, i_r)}$, $(i_1, \dots, i_r) \in I_1 \times \dots \times I_r$. On vérifie sur les définitions que ϕ et ψ sont inverses l'une de l'autre. \square

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

13.2.5

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

$$\begin{array}{llll} M^\vee \otimes_A N & \rightarrow & \text{Hom}_A(M, N) & , \quad M^\vee \otimes_A N^\vee \rightarrow (M \otimes_A N)^\vee \\ f \otimes n & \rightarrow & f(-)n; & \quad f \otimes g \rightarrow m \otimes n \rightarrow f(m)g(n). \end{array}$$

et

$$\begin{array}{ll} \text{End}_A(M) \otimes_A \text{End}_A(N) & \rightarrow \text{End}_A(M \otimes_A N) \\ f \otimes g & \rightarrow m \otimes n \rightarrow f(m) \otimes g(n); \end{array}$$

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

Démonstration. Les morphismes se construisent en utilisant la propriété universelle du produit tensoriel. En général, il n'y a par contre pas de façon canonique de construire des inverses de ces morphismes (et d'ailleurs, ce ne sont pas toujours des isomorphismes). Mais si M et N sont libres de rang fini, on peut vérifier que ces trois morphismes envoient à chaque fois une base sur une base. \square

13.3 Adjonctions

13.3.1

$- \otimes_A M$ **versus** $\text{Hom}_A(M, -)$

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

$$\begin{array}{llll} \text{Hom}_A(L, \text{Hom}_A(M, N)) & \xrightarrow{\sim} & L_{r,A}(L \times M, N) & \xrightarrow{\sim} \text{Hom}_A(L \otimes_A M, N) \\ f & \rightarrow & (l, m) \rightarrow f(l)(m) & \\ l \rightarrow \beta(l, -) & \leftarrow & \beta & \end{array}$$

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

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

$$0 \rightarrow N' \xrightarrow{u} N \xrightarrow{v} N'' \rightarrow 0$$

1. La suite

$$0 \rightarrow \operatorname{Hom}_A(M, N') \xrightarrow{u \circ} \operatorname{Hom}_A(M, N) \xrightarrow{v \circ} \operatorname{Hom}_A(M, N'')$$

est exacte.

2. La suite

$$M \otimes_A N' \xrightarrow{\operatorname{Id} \otimes u} M \otimes_A N \xrightarrow{\operatorname{Id} \otimes v} M \otimes_A N'' \rightarrow 0$$

est exacte.

13.3.2

Extension/Restriction des scalaires. Soit $\phi : A \rightarrow B$ une A -algèbre. À tout B -module M on peut associer un A -module noté $M|_A$ (ou $\phi_* M$) dont le groupe abélien sous-jacent est encore M et dont la structure de A -module est définie par $a \cdot m = \phi(a)m$, $a \in A$, $m \in M$. Tout morphisme de B -modules $f : M \rightarrow N$ induit alors tautologiquement un morphisme de A -modules $f|_A : M|_A \rightarrow N|_A$. On voudrait, inversement, associer à tout A -module M un B -module $\phi^* M$ et à tout morphisme de A -modules $f : M \rightarrow N$ un morphisme de B -modules $\phi^* f : \phi^* M \rightarrow \phi^* N$.

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

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

est 2 - A -linéaire donc se factorise en un morphisme de A -module $b_0 \cdot : M \otimes_A N \rightarrow M \otimes_A N$, $m \otimes n \rightarrow b_0 \cdot (m \otimes n) := (b_0 m) \otimes n$. On vérifie que cela définit une structure de B -module sur $M \otimes_A N$. Tout morphisme de A -modules $f : N \rightarrow N'$ induit alors un morphisme de B -modules $\operatorname{Id}_M \otimes f : M \otimes_A N \rightarrow M \otimes_A N'$. Si $M = B$ muni de la structure de A -module donnée par $\phi : A \rightarrow B$ ($a \cdot b = \phi(a)b$, $a \in A$, $b \in B$), on note parfois $\phi^* N := B \otimes_A N$ et $\phi^* f := \operatorname{Id}_B \otimes f : \phi^* N \rightarrow \phi^* N'$.

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

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

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

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

1. Soit M, M' des B -modules et N un A -module. Montrer qu'on a un isomorphisme canonique de B -modules

$$M' \otimes_B (M \otimes_A N) \xrightarrow{\sim} (M' \otimes_B M) \otimes_A N.$$

En déduire qu'on a un isomorphisme canonique de B -modules $M \otimes_B (B \otimes_A N) \xrightarrow{\sim} M \otimes_A N$;

2. Soit $A \rightarrow B \rightarrow C$ des morphismes d'anneaux et M un A -module. Montrer qu'on a un isomorphisme canonique

$$C \otimes_B (B \otimes_A M) \xrightarrow{\sim} C \otimes_A M.$$

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

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

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

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

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

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

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

est bijective. Or 13.3.2.0.1 dit que le morphisme de A -module $p : M \rightarrow A/I \otimes_A M, m \rightarrow \bar{1} \otimes m$ vérifie la même propriété. Par unicité des objets universels, on a donc un unique morphisme de A/I -modules $\phi : A/I \otimes M \rightarrow M/IM$ tel que $\phi \circ p = p_{IM}$. On peut aussi démontrer cela 'à la main', comme suit.

L'application canonique

$$\begin{aligned} A \times M &\rightarrow M/IM \\ (a, m) &\rightarrow \overline{am} \end{aligned}$$

est 2- A -linéaire et passe au quotient en une application 2- A -linéaire $A/I \times M \rightarrow M/IM$ donc se factorise en un morphisme de A -modules $f : (A/I) \otimes_A M \rightarrow M/IM$. Inversement, l'application $M \rightarrow (A/I) \otimes_A M, m \rightarrow 1 \otimes m$ est un morphisme de A -modules dont le noyau contient IM donc se factorise en un morphisme de A -modules $M/IM \rightarrow (A/I) \otimes_A M$. Par construction, f et g sont inverses l'une de l'autre. On a donc montré qu'on avait un isomorphisme de A -modules canoniques

$$(A/I) \otimes_A M \xrightarrow{\sim} M/IM.$$

Exemple. Soit A un anneau principal, $a, b \in A$ des éléments premiers entre eux et M un A -module tel que $aM = 0$. Par Bézout on a alors $bM = M$ donc $(A/b) \otimes_A M = 0$. Par exemple si $p \neq q$ sont deux nombres premiers, $\mathbb{Z}/p \otimes_{\mathbb{Z}} \mathbb{Z}/q = 0$.

13.3.2.0.4 Extension des scalaires par une localisation. Soit $S \subset A$ une partie multiplicative et M un A -module. Munissons le produit cartésien $S \times M$ de la relation \sim définie par $(s, m) \sim (s', m')$ s'il existe $s'' \in S$ tel que $s''(s'm - sm') = 0$.

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

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

$$\begin{aligned} -/- : S \times M &\rightarrow S^{-1}M \\ (s, m) &\rightarrow m/s \end{aligned}$$

la projection canonique.

On vérifie que les applications

$$\begin{aligned} + : S^{-1}M \times S^{-1}M &\rightarrow S^{-1}M, & \cdot : S^{-1}A \times S^{-1}M &\rightarrow S^{-1}A \\ (m/s, n/t) &\rightarrow (tm + sn)/(st) & (a/s, n/t) &\rightarrow (an)/(st) \end{aligned}$$

munissent $S^{-1}A$ d'une structure de $S^{-1}A$ -module et que l'application canonique $\iota_S := -/1 : M \rightarrow (\iota_S)_*S^{-1}M$ est un morphisme de A -modules de noyau $\ker(\iota_S) = \{m \in M \mid \exists s \in S \text{ tel que } sm = 0\}$.

Lemme. (Propriété universelle de la localisation des A -modules) *Pour toute partie multiplicative $S \subset A \setminus \{0\}$ et pour tout A -module M il existe un $S^{-1}A$ -module L et un morphisme de A -modules $\iota_S : M \rightarrow (\iota_S)_*L$ tel que pour tout $S^{-1}A$ -module N et pour tout morphisme de A -module $f : M \rightarrow N$, il existe un unique morphisme de $S^{-1}A$ -modules $\tilde{f} : L \rightarrow N$ tel que $f = \tilde{f} \circ \iota_S$.*

Démonstration. On vérifie que $\iota_S := -/1 : M \rightarrow (\iota_S)_*S^{-1}M$ convient... □

En particulier, pour tout morphisme de A -modules $f : M \rightarrow N$, en appliquant la propriété universelle de $\iota_S : M \rightarrow S^{-1}M$ au morphisme de A -modules $M \xrightarrow{f} N \xrightarrow{\iota_S} S^{-1}N$ on obtient un morphisme de $S^{-1}A$ -modules $S^{-1}f : S^{-1}M \rightarrow S^{-1}N$ donné explicitement par $f(m/s) = f(m)/s$, $s \in S$, $m \in M$.

On peut réécrire le Lemme en disant que pour tout $S^{-1}A$ -module N l'application canonique

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, (\iota_S)_*N) \rightarrow \mathrm{Hom}_A(M, N), \phi \rightarrow (\phi \circ \iota_S)$$

est bijective. Or 13.3.2.0.1 dit que le morphisme de A -modules $\iota : M \rightarrow (\iota_S)_*(S^{-1}A \otimes_A M)$, $m \rightarrow 1/1 \otimes m$ vérifie la même propriété. Par unicité des objets universels, on a donc un unique morphisme de $S^{-1}A$ -modules $\phi : S^{-1}A \otimes_A M \rightarrow S^{-1}M$ tel que $\phi \circ \iota = \iota_S$. Là encore, on peut aussi démontrer cela 'à la main'.

L'application canonique

$$\begin{aligned} S^{-1}A \times M &\rightarrow S^{-1}M \\ (a/s, m) &\rightarrow (am)/s (= a(m/s)) \end{aligned}$$

est bien définie et 2- A -linéaire donc se factorise en un morphisme de A -modules $f : S^{-1}A \otimes_A M \rightarrow S^{-1}M$ qui est, automatiquement, un morphisme de $S^{-1}A$ -modules. Inversement, l'application $S \times M \rightarrow S^{-1}A \otimes_A M$, $(s, m) \rightarrow (1/s) \otimes m$ se factorise en un morphisme de $S^{-1}A$ -modules $g : S^{-1}M \rightarrow S^{-1}A \otimes_A M$. Par construction, f et g sont inverses l'une de l'autre. On a donc montré qu'on avait un isomorphisme de $S^{-1}A$ -modules canonique

$$S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M.$$

Exemple. Si pour tout $m \in M$ il existe $s \in S$ tel que $sm = 0$, $S^{-1}M = 0$. Si pour tout $s \in S$ l'application $s \cdot - : M \rightarrow M$ de multiplication par s est bijective, $\iota_S : M \rightarrow S^{-1}M$ est un isomorphisme de A -modules. En particulier, si A est un anneau principal de corps des fractions K et M est un A -module de type fini, $K \otimes_A M = K^{\oplus r}$ et pour tout $\mathfrak{p} \in \text{Spec}(A) \setminus \{0\}$, $A_{\mathfrak{p}} \otimes_A M = A_{\mathfrak{p}}^{\oplus r} \oplus M(\mathfrak{p})$, où on a noté $M(\mathfrak{p})$ la \mathfrak{p} -partie de M et r le rang de M . Par exemple $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = 0$, $\mathbb{Z}_{2\mathbb{Z}} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, $\mathbb{Z}_{3\mathbb{Z}} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = \mathbb{Z}/3 \times \mathbb{Z}/3$, $\mathbb{Z}_{p\mathbb{Z}} \otimes_{\mathbb{Z}} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = 0$ pour $p \neq 2, 3$.

13.4 Produit tensoriel de A -algèbres

Soit $\phi : A \rightarrow B$ et $\psi : A \rightarrow C$ deux A -algèbres. Les applications produits $B \times B \rightarrow B$ et $C \times C \rightarrow C$ sont 2- A -bilinéaires donc se factorisent en des morphismes de A -modules $\mu_B : B \otimes_A B \rightarrow B$ et $\mu_C : C \otimes_A C \rightarrow C$. On en déduit une application

$$(B \otimes_A C) \otimes_A (B \otimes_A C) \xrightarrow{\sim} (B \otimes_A B) \otimes_A (C \otimes_A C) \xrightarrow{\mu_B \otimes \mu_C} B \otimes_A C$$

dont on vérifie qu'elle munit le A -module $B \otimes_A C$ d'une structure de A -algèbre telle que les applications $\iota_B : B \rightarrow B \otimes_A C$, $b \rightarrow b \otimes 1$ et $\iota_C : C \rightarrow B \otimes_A C$, $c \rightarrow 1 \otimes c$ sont des morphismes de A -algèbres.

13.4.1

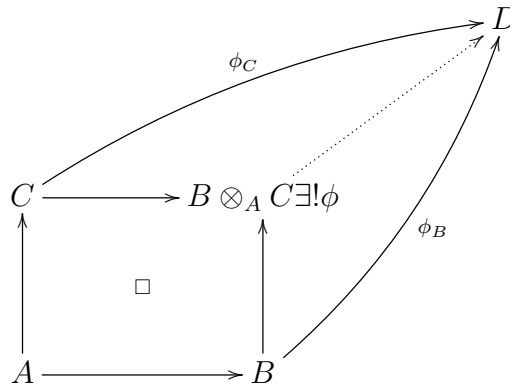
Lemme. (Propriété universelle du produit tensoriel de A -algèbres) *Pour toutes A -algèbres $A \rightarrow B$ et $A \rightarrow C$, il existe une A -algèbre T et des morphismes de A -algèbres $\iota_B : B \rightarrow T$, $\iota_C : C \rightarrow T$ tels que pour toute A -algèbre $A \rightarrow D$ et morphismes de A -algèbres $\phi_B : B \rightarrow D$, $\phi_C : C \rightarrow D$ il existe un unique morphisme de A -algèbres $\phi : T \rightarrow D$ tel que $\phi \circ \iota_B = \phi_B$ et $\phi \circ \iota_C = \phi_C$*

Démonstration. On vérifie comme d'habitude que $B \otimes_A C$ et $\iota_B : B \rightarrow B \otimes_A C$, $\iota_C : C \rightarrow B \otimes_A C$ conviennent. Si $\phi : B \otimes_A C \rightarrow D$ existe les conditions $\phi \circ \iota_B = \phi_B$ et $\phi \circ \iota_C = \phi_C$ forcent $\phi(b \otimes c) = \phi_B(b)\phi_C(c)$, d'où l'unicité de ϕ sous réserve de son existence. Considérons l'application $B \times C \rightarrow D$, $(b, c) \rightarrow \phi_B(b)\phi_C(c)$. Elle est 2- A -bilinéaire donc se factorise en un morphisme de A -modules $\phi : B \otimes_A C \rightarrow D$ tel que $\phi(b \otimes c) = \phi_B(b)\phi_C(c)$ et on vérifie sur la construction que c'est automatiquement un morphisme de A -algèbres. \square

On peut aussi réécrire 13.4.1 en disant que pour toutes A -algèbres $A \rightarrow B$, $A \rightarrow C$ et $A \rightarrow D$ l'application canonique

$$\mathrm{Hom}_{\mathrm{Alg}/A}(B \otimes_A C, D) \rightarrow \mathrm{Hom}_{\mathrm{Alg}/A}(B, D) \times \mathrm{Hom}_{\mathrm{Alg}/A}(C, D), \quad \phi \mapsto (\phi \circ \iota_B, \phi \circ \iota_C)$$

est bijective ou encore, plus visuellement,



13.4.2

Exercice.

1. Soit $I, J \subset A$ deux idéaux. Montrer qu'on a un isomorphisme canonique de A -algèbres

$$(A/I) \otimes_A (A/J) \xrightarrow{\sim} A/(I+J).$$

Si A est un anneau principal et $a, b \in A$, calculer $(A/a) \otimes_A (A/b)$.

2. Montrer qu'on a un isomorphisme canonique de A -algèbres $A[X_1] \otimes_A \cdots \otimes_A A[X_n] \xrightarrow{\sim} A[X_1, \dots, X_n]$.
3. Si $\varphi : A \rightarrow B$ est un morphisme d'anneaux et $P \in A[X]$, montrer qu'on a un isomorphisme canonique de B -algèbres

$$B \otimes_A (A[X]/P) \xrightarrow{\sim} B[X]/\varphi(P)$$

(on note encore $\varphi : A[X] \rightarrow B[X]$ le morphisme obtenu en appliquant φ aux coefficients).

Calculer $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Est-ce un corps ? Même question avec $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.

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

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

* * *

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