Algèbre commutative

N. Perrin

Université de Versailles Saint-Quentin-en-Yvelines
Année 2017-2018

Table des matières

Première partie .

Algèbre Commutative

1. Anneaux et idéaux

1.1. Anneaux

Définition 1.1.1 1. **Un anneau** $(A, +, \times)$ est un triplet formé d'un ensemble A et de deux lois de composition $+ : A \times A \to A, (x, y) \mapsto x+y$ et $\times : A \times A \to A, (x, y) \mapsto xy$ telles que :

1. $(A, +)$ est un groupe abélien d'élément neutre 0 ;
2. la multiplication est associative : on a $x(yz) = (xy)z$ pour tout $x, y, z \in A$.
3. la multiplication est bilinéaire : on a $x(y + z) = xy + xz$ et $(x + y)z = xz + yz$ pour tout $x, y, z \in A$.
4. Unité : il existe un élément $1 \in A$ tel que $x1 = x = 1x$ pour tout $x \in A$.

2. Un anneau $(A, +, \times)$ est dit **commutatif** si on a $xy = yx$ pour tout $x, y \in A$.

Dans ce cours tous les anneaux seront commutatifs.

Remarque 1. Dans un anneau, on a toujours $0x = 0 = x0$: en effet, on a $0x = (0 + 0)x = 0x + 0x$ et donc $x0 = 0x = 0$.

2. On peut avoir l'égalité $1 = 0$. Dans ce cas, on a

$$x = 1x = 0x = 0$$

pour tout $x \in A$. L'anneau A n'a donc qu'un élément, l'élément nul : $A = \{0\}$. Par abus de notation, on écrit alors $A = 0$. Cet anneau est appelé **l'anneau nul**.

3. Les éléments 0 et 1 sont uniques.

Définition 1.1.3 Un morphisme d'anneaux (ou encore morphisme dans la catégorie des aneaux, on en reparlera plus tard) est une application $f : A \to B$, où A et B sont des anneaux telle que

1. $f(x + y) = f(x) + f(y)$ pour tout $x, y \in A$
2. $f(xy) = f(x)f(y)$ pour tout $x, y \in A$
3. $f(1) = 1$.

Remarque Soient $f : A \to B$ et $g : B \to C$ des morphismes d'anneaux. Alors $g \circ f$ est un morphisme d'anneaux.

Définition 1.1.5 Un sous-anneau B de A (ou sous-objet dans la catégorie des anneaux) est un sous-ensemble $B \subset A$ tel que

1. $x - y \in B$ pour tout $x, y \in B$
2. $xy \in B$ pour tout $x, y \in B$
3. $1 \in B$.

Remarque Soit $f : A \to B$ un morphisme d'anneaux. Alors $\mathrm{Im}f = f(A)$ est un sous-anneau de B.

Définition 1.1.7 Soit $(A_i)_{i\in I}$ une famille d'anneaux. Alors le produit

$$\prod_{i\in I} A_i = \{(x_i)_{i\in I} \ | x_i \in A_i \text{ pour tout } i \in I\}$$

muni des opérations $(x_i) + (y_i) = (x_i + y_i)$ et $(x_i)(y_i) = (x_i y_i)$ est un anneau avec $0 = (0_i)$ et $1 = (1_i)$ comme élément nul et unité et s'appelle **l'anneau produit**.

1.2. Idéaux

Définition 1.2.1 Soit A un anneau. **Un idéal** $\mathfrak{a}$ de A est un sous-ensemble $\mathfrak{a} \subset A$ tel que

1. $0 \in \mathfrak{a}$;
2. $x - y \in \mathfrak{a}$ pour tout $x, y \in \mathfrak{a}$;
3. $xy \in \mathfrak{a}$ pour tout $x \in \mathfrak{a}$ et $y \in A$.

Exemple Le sous-ensemble $\{0\}$ est un idéal appelé **l'idéal nul**. On le note simplemant 0.

Remarque Soit $f : A \to B$ un morphisme d'anneaux. Alors $\mathrm{Ker}f$ est un idéal de A. Comme le montre la proposition suivante, tous les idéaux sont de cette forme.

Plus généralement, si $\mathfrak{b} \subset B$ est un idéal de B, alors $f^{-1}(\mathfrak{b}) \subset A$ est un idéal de A.

Proposition 1.2.4 Soit A un anneau et $\mathfrak{a}$ un idéal.

1. L'addition $[x] + [y] = [x + y]$ et la multiplication $[x][y] = [xy]$ sont bien définies et munissent $A/\mathfrak{a}$ d'une structure d'anneau d'élément nul $[0]$ et d'unité $[1]$.

2. La projection canonique $\pi : A \to A/\mathfrak{a}, x \mapsto [x]$ est un morphisme d'anneau surjectif.

Preuve. Exercice. ∎

Théorème 1.2.5 Soit $f : A \to B$ un morphisme d'anneau et $\mathfrak{a}$ un idéal de A.

1. Il existe un morphisme d'anneau $\bar{f} : A/\mathfrak{a} \to B$ tel que $f = \bar{f} \circ \pi$ si et seulement si $\mathfrak{a} \subset \mathrm{Ker} f$.

2. L'application $\bar{f}$ est injective si et seulement si $\mathrm{Ker} f = \mathfrak{a}$.

3. L'application $\bar{f}$ est surjective si et seulement si f l'est. □

Preuve. Exercice. ■

Proposition 1.2.6 Soit $\mathfrak{a} \subset A$ un idéal. On a une bijection entre l'ensemble des idéaux $\mathfrak{b} \subset A$ tels que $\mathfrak{a} \subset \mathfrak{b}$ et l'ensemble des idéaux $\overline{\mathfrak{b}} \subset A/\mathfrak{a}$:

$$\{\mathfrak{b} \text{ idéal de } A \text{ tel que } \mathfrak{a} \subset \mathfrak{b}\} \to \{\overline{\mathfrak{b}} \text{ idéal de } A/\mathfrak{a}\},$$

avec $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ et $\overline{\mathfrak{b}} \mapsto \pi^{-1}(\overline{\mathfrak{b}})$.

Preuve. Exercice. ■

1.3. Opérations sur les idéaux

Définition 1.3.1 Soit A un anneau.

1. Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux de A. La **somme de $\mathfrak{a}$ et $\mathfrak{b}$** est définie par $\mathfrak{a}+\mathfrak{b} = \{x+y \in A \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$. C'est encore un idéal (exercice).

2. Plus généralement, soit $(\mathfrak{a}_i)_{i\in I}$ une famille d'idéaux. Alors la somme $\sum_i \mathfrak{a}_i = \{\sum_i x_i \in A \mid x_i \in \mathfrak{a}_i, x_i \neq 0 \text{ pour un nombre fini de } i \in I\}$ est un idéal appelé **la somme des idéaux** $(\mathfrak{a}_i)_{i\in I}$.

Remarque 1. La somme $\mathfrak{a} + \mathfrak{b}$ (resp. $\sum_i \mathfrak{a}_i$) est aussi appelé idéal engendré par $\mathfrak{a}$ et $\mathfrak{b}$ (resp. $(\mathfrak{a}_i)_{i\in I}$). C'est le plus petit idéal contenant $\mathfrak{a}$ et $\mathfrak{a}$ (resp. $(\mathfrak{a}_i)_{i\in I}$).

2. Si $\mathfrak{a} = (x)$ et $\mathfrak{b} = (y)$, on écrit $\mathfrak{a} + \mathfrak{b} = (x) + (y) = (x, y)$. Plus généralement, si $\mathfrak{a}_i = (x_i)$ pour tout $i \in I$, on écrit $\sum_i \mathfrak{a}_i = \sum_i (x_i) = (x_i \mid i \in I)$. Pour $I = [1, n]$, on écrit $(x_i \mid i \in I) = (x_1, \cdots, x_n)$.

Remarque Soit A un anneau.

1. Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux. Alors l'intersection $\mathfrak{a} \cap \mathfrak{b}$ est un idéal.

2. Plus généralement, soit $(\mathfrak{a}_i)_{i\in I}$ une famille d'idéaux. Alors l'intersection $\cap_i \mathfrak{a}_i$ est un idéal (exercice).

Exemple Soient $n, m \in \mathbb{Z}$. On a $(n)+(m) = (\mathrm{pgcd}(n, m))$ et $(n)\cap(m) = (\mathrm{ppcm}(n, m))$.

Définition 1.3.5 Soit A un anneau.

1. Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux. **L'idéal produit** $\mathfrak{ab}$ est l'idéal

$$\mathfrak{ab} = (xy | x \in \mathfrak{a}, y \in \mathfrak{b})$$

(l'idéal engendré par tous les produits xy avec $x \in \mathfrak{a}$ et $y \in \mathfrak{b}$).

2. Plus généralement, soit $(\mathfrak{a}_i)_{i[1,n]}$ une famille finie d'idéaux. On définit l'idéal produit par récurrence : $\mathfrak{a}_1 \cdots \mathfrak{a}_n = (\cdots((\mathfrak{a}_1\mathfrak{a}_2)\mathfrak{a}_3)\cdots\mathfrak{a}_n)$. C'est l'idéal engendré par les éléments de la forme $x_1 \cdots x_n$ où $x_i \in \mathfrak{a}_i$ pour tout $i \in [1, n]$:

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n = (x_1 \cdots x_n \mid x_i \in \mathfrak{a}_i \text{ pour tout } i \in [1, n]).$$

3. En particulier, si $\mathfrak{a}$ est un idéal, on définit $\mathfrak{a}^n$ comme l'idéal engendré par les éléments de la forme $x_1 \cdots x_n$ avec $x_i \in \mathfrak{a}$ pour tout $i \in [1, n]$:

$$\mathfrak{a}^n = (x_1 \cdots x_n \mid x_i \in \mathfrak{a} \text{ pour tout } i \in [1, n]).$$

Remarque On a l'inclusion $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.

Exemple Pour $\mathfrak{a} = (2) = \mathfrak{b} \subset \mathbb{Z}$, on a $\mathfrak{ab} \subsetneq \mathfrak{a} \cap \mathfrak{b}$. En effet, on a $\mathfrak{ab} = (2)(2) = (4) \subsetneq (2) = (2) \cap (2) = \mathfrak{a} \cap \mathfrak{b}$.

Proposition 1.3.8 On a (distributivité : $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$.

Preuve. Exercice. ∎

1.4. Diviseurs de zéro, éléments nilpotents, éléments inversibles

Définition 1.4.1 Soit A un anneau.

1. Un élément $x \in A$ est dit **diviseur de zéro** s'il existe $y \in A$ tel que $y \neq 0$ et $xy = 0$. Un anneau $A \neq 0$ dont le seul diviseur de zéro est 0 est appelé **anneau intègre**.

2. Un élément $x \in A$ est dit **nilpotent** s'il existe un entier $n \geq 1$ tel que $x^n = 0$. Un anneau dont le seul élément nilpotent est 0 est appelé **réduit**.

3. Un élément $x \in A$ est dit **inversible** s'il existe un $y \in A$ tel que $xy = 1$. L'élément y est uniquement déterminé et est appelé **inverse de** x. On le note x^{-1}. On note par $A^\times$ l'ensemble des éléments inversibles de A.

Remarque 1. Un élément nilpotent est toujours diviseur de zéro (sauf dans le cas où $A = 0$). Par contre, les diviseurs de zéros ne sont pas toujours nilpotents. Par exemple, dans $\mathbb{Z}/6\mathbb{Z}$, les élément 2 et 3 sont diviseurs de zéro mais pas nilpotents.

2. L'ensemble $(A^\times, \times)$ est un groupe commutatif.

3. Un sous-anneau d'un anneau intègre est encore un anneau intègre (exercice).

Définition 1.4.3 Soit $x \in A$. L'ensemble $(x) = \{xy \in A \,|y \in A\}$ est un idéal. C'est l'idéal engendré par x. Un idéal de cet forme s'appelle **idéal principal**. Un anneau dont tous les idéaux sont principaux est appelé **anneau principal**.

Remarque Soit $x \in A$. On a $x \in A^\times \Leftrightarrow (x) = A$.

Définition 1.4.5 Un corps est un anneau $(A, +, \times)$ tel que $1 \neq 0$ et $A^\times = A \setminus \{0\}$ (c'est-à-dire que tout élément non nul est inversible).

Proposition 1.4.6 Soit A un anneau. Les propositions suivantes sont équivalentes :

1. A est un corps ;
2. Les seuls idéaux de A sont 0 et A ;
3. tous les morphismes d'anneaux $f : A \to B$ avec $B \neq 0$ sont injectifs.

Preuve. (1. $\Rightarrow$ 2.) Soit $0 \neq \mathfrak{a} \subset A$ un idéal. Il existe alors un x dans $\mathfrak{a}$ tel que $x \neq 0$. Alors x est inversible et on a $A = (x) \subset \mathfrak{a} \subset A$ donc $\mathfrak{a} = A$.

(2. $\Rightarrow$ 3.) Le noyau $\mathrm{Ker} f$ est un idéal et on a $f(1) = 1 \neq 0$ donc $\mathrm{Ker} f \neq A$. On en déduit $\mathrm{Ker} f = 0$ et f est injective.

(3. $\Rightarrow$ 1.) Soit $x \in A$ non inversible. Posons $\mathfrak{a} = (x)$. On a $(x) \subsetneq A$ donc $A/\mathfrak{a} \neq 0$. Par hypothèse, on doit avoir que $\pi : A \to A/\mathfrak{a}$ est injective donc $\mathfrak{a} = \mathrm{Ker}\pi = 0$. On en déduit $x = 0$. ∎

1.5. Idéaux premiers et maximaux

Définition 1.5.1 Soit A un anneau.

1. Un idéal $\mathfrak{p} \subset A$ est dit **premier** si $\mathfrak{p} \neq A$ et si l'implication suivante est vraie : $(xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ ou $y \in \mathfrak{p})$ pour tout $x, y \in A$.

2. Un idéal $\mathfrak{m} \subset A$ est dit **maximal** si $\mathfrak{m} \neq A$ et si on a l'implication $(\mathfrak{m} \subset \mathfrak{a} \subset A \Rightarrow$ $\mathfrak{a} = \mathfrak{m}$ ou $\mathfrak{a} = A)$ pour tout idéal $\mathfrak{a} \subset A$.

Proposition 1.5.2 Soit A un anneau et soient $\mathfrak{p}, \mathfrak{m} \subset A$ des idéaux.

1. L'idéal $\mathfrak{p}$ est premier si et seulement si $A/\mathfrak{p}$ est intègre.

2. L'idéal $\mathfrak{m}$ est maximal si et seulement si $A/\mathfrak{m}$ est un corps.

Preuve. 1. Supposons $\mathfrak{p}$ premier. Tout d'abord, comme $\mathfrak{p} \neq A$, on a $A/\mathfrak{p} \neq 0$. Soit maintenant $[x]$ un diviseur de zéro dans $A/\mathfrak{p}$. Il existe donc $[y] \in A/\mathfrak{p}$ avec $[y] \neq 0$ tel que $[x][y] = 0$. Sur les éléments $x, y \in A$ ceci se traduit par : $y \notin \mathfrak{p}$ et $xy \in \mathfrak{p}$. Comme l'idéal est premier ceci impose $x \in \mathfrak{p}$ et donc $[x] = 0$. L'anneau quotient est intègre.

Réciproquement, supposons que $A/\mathfrak{p}$ est intègre. En particulier $A/\mathfrak{p} \neq 0$ et donc $\mathfrak{p} \neq A$. Soient $x, y \in A$ tels que $xy \in \mathfrak{p}$. Alors on a $[x][y] = [xy] = 0$ et donc $[x] = 0$ ou $[y] = 0$ (l'aneau $A/\mathfrak{p}$ est intègre) ce qui se traduit par $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$ et donc l'idéal $\mathfrak{p}$ est permier.

2. On a une bijection entre les idéaux de $A/\mathfrak{m}$ et les idéaux de A contenant $\mathfrak{m}$. On en déduit les équivalences : $A/\mathfrak{m}$ est un corps $\Leftrightarrow$ les seuls idéaux de $A/\mathfrak{m}$ sont 0 et $A/\mathfrak{m}$ $\Leftrightarrow$ les idéaux de A contenant $\mathfrak{m}$ sont $\mathfrak{m}$ et A ce qui est équivalent au fait que $\mathfrak{m}$ est maximal. ∎

Remarque On voit que tout idéal maximal est premier mais que la réciproque est fausse. Par exemple, 0 est un idéal premier de $\mathbb{Z}$ mais n'est pas maximal (on a $0 \subsetneq (2)$).

Corollaire Soit $f : A \to B$ un morphisme d'anneau et soit $\mathfrak{b}$ un idéal premier de B. Alors $f^{-1}(\mathfrak{b})$ est un idéal premier de A.

Preuve. Soit $g : A \to B/\mathfrak{b}$ avec $g = \pi \circ f$. On a $\mathrm{Ker} g = f^{-1}(\mathfrak{b})$. On a donc un morphisme d'anneaux injectif $\bar{g} : A/f^{-1}(\mathfrak{b}) \to B/\mathfrak{b}$ et donc $A/f^{-1}(\mathfrak{b})$ est isomorphe à un sous-anneau de $B/\mathfrak{b}$. Ce dernier est intègre donc $A/f^{-1}(\mathfrak{b})$ aussi. ∎

Remarque L'assertion ci-dessus est fausse si on remplace "idéal premier" par "idéal maximal". Ainsi par exemple, pour $f : \mathbb{Z} \to \mathbb{Q}, x \mapsto x$ l'inclusion, on a $f^{-1}(0) = 0$ qui n'est pas maximal dans $\mathbb{Z}$ alors que (0) est maximal dans $\mathbb{Q}$. C'est par contre toujours un idéal premier.

Proposition 1.5.6 Soit $f : A \to B$ surjectif et $\mathfrak{b} \subset B$ maximal, alors $f^{-1}(\mathfrak{b})$ est maximal dans A.

Preuve. Soit $\mathfrak{a} = \mathrm{Ker} f$. On a $B \simeq A/\mathfrak{a}$. On peut donc supposer que f est la projection canonique $\pi : A \to A/\mathfrak{a}$. L'assertion découle maintenant de la Proposition 1.2.4. ∎

L'énoncé suivant est équivalent à l'axiome du choix. Nous l'utiliserons sans preuve.

Lemme 1.5.7 (Lemme de Zorn) Soit S un ensemble non vide muni d'une relation d'ordre $\leq$ (une relation d'ordre est une relation R telle que R est reflexive : on a xRx pour tout $x \in S$, R est transitive : (xRy et $yRz \Rightarrow xRz$) pour tout $x, y, z \in S$ et (xRy et $yRx \Rightarrow x = y$).

Une chaine T d'éléments de S est un sous-ensemble de S vérifiant la condition suivante : $x \leq y$ ou $y \leq x$ pour tout $x, y \in T$.

Si toute chaine a une borne supérieure (*i.e.* il existe $x \in S$ tel que $y \leq x$ pour tout $y \in T$), alors a S un élément maximal.

Remarque Un ensemble ordonné non vide tel que toute chaine a une borne supérieure s'appelle **ensemble inductif**.

Un corollaire du lemme de Zorn est le résultat bien utile suivant.

Théorème 1.5.9 Tout anneau non nul a un idéal maximal. □

Preuve. Soit A un anneau non nul et soit S l'ensemble des idéaux propres de A c'est-à-dire

$$S = \{I \subsetneq A \mid I \text{ idéal de } A\}.$$

L'ensemble S est non vide (il contient l'idéal nul) et ordonné par la relation $\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow \mathfrak{a} \subset \mathfrak{b}$. L'ensemble S est inductif : soit T une chaine, alors

$$\mathfrak{b} = \bigcup_{\mathfrak{a} \in T} \mathfrak{a}$$

est un idéal : si $x, y \in \mathfrak{b}$, alors il existe $\mathfrak{a}, \mathfrak{a}' \in T$ tels que $x \in \mathfrak{a}$ et $y \in \mathfrak{a}'$. Mais on a $\mathfrak{a} \subset \mathfrak{a}'$ ou $\mathfrak{a}' \subset \mathfrak{a}$. On peut donc supposer $\mathfrak{a}' \subset \mathfrak{a}$. On a alors $x + y, xy \in \mathfrak{a} \subset \mathfrak{b}$. On a aussi $\mathfrak{b} \subsetneq A$: sinon $1 \in \mathfrak{b}$ donc il existe $\mathfrak{a} \in T$ tel que $1 \in \mathfrak{a}$ et donc $\mathfrak{a} = A$, une contradiction. L'nsemble S est donc inductif et a un élément maximal qui est un idéal maximal de A. ■

Corollaire Soit $\mathfrak{a} \subsetneq A$ un idéal, alors il existe un idéal maximal $\mathfrak{m}$ de A tel que $\mathfrak{a} \subset \mathfrak{m}$.

Preuve. Posons $\mathfrak{m} = \pi^{-1}(\overline{\mathfrak{m}})$, avec $\pi : A \to A/\mathfrak{a}$ la projection canonique et $\overline{\mathfrak{m}}$ un idéal maximal de $A/\mathfrak{a}$. ■

Corollaire Soit $x \in A$ un élément non inversible, alors il existe un idéal maximal $\mathfrak{m}$ de A avec $x \in \mathfrak{m}$.

Preuve. Soit $\mathfrak{a} = (x)$. On a $\mathfrak{a} \subsetneq A$. L'assertion découle du corollaire précédent. ■

1.6. Anneaux locaux

Définition 1.6.1 Un anneau A est dit **local** si A contient un unique idéal maximal $\mathfrak{m}$. Le corps $A/\mathfrak{m}$ s'appelle **le corps résiduel de** A

Proposition 1.6.2 Soit A un anneau et $\mathfrak{m} \subsetneq A$ un idéal.

1. Si $A \setminus \mathfrak{m} = A^\times$, alors A est un anneau local d'idéal maximal $\mathfrak{m}$.

2. Si $\mathfrak{m}$ est maximal et tout élément de la forme $1 + x$ avec $x \in \mathfrak{m}$ est inversible, alors A est local d'idéal maximal $\mathfrak{m}$.

Preuve. 1. Soit $\mathfrak{m}'$ un idéal maximal. On a $\mathfrak{m}' \subset A \setminus A^\times = \mathfrak{m}$ donc $\mathfrak{m}' = \mathfrak{m}$.

2. Soit $x \in A \setminus \mathfrak{m}$. On a $(x) + \mathfrak{m} = A$. On a donc des éléments $y \in \mathfrak{m}$ et $z \in A$ tels que $1 = y + xz$. On a donc $xz = 1 - y$. Soit $u = (1-y)^{-1}$ (par hypothèse $1 - y$ est inversible). On a $xzu = 1$ et $x \in A^\times$. On en déduit $A \setminus \mathfrak{m} \subset A^\times$. L'inclusion réciproque est toujours vraie (les éléments de $\mathfrak{m}$ ne peuvent être inversibles), on a donc $A \setminus \mathfrak{m} = A^\times$ et l'assertion découle de 1. ∎

1.7. Radical

Lemme 1.7.1 L'ensemble $\mathfrak{n}(A) = \sqrt{0} = \{x \in A \mid x \text{ nilpotent}\}$ est un idéal de A appelé **nilradical de** A.

Le quotient $A/\mathfrak{n}(A)$ n'a pas d'élément nilpotent non nul et est donc réduit.

Preuve. Exercice. ∎

Proposition 1.7.2 Le nilradical $\mathfrak{n}(A)$ est l'intersection de tous les idéaux premiers de A :

$$\mathfrak{n}(A) = \bigcap_{\mathfrak{p} \subset A \text{ idéal premier}} \mathfrak{p}.$$

Preuve. Soit $\mathfrak{n}'$ l'intersection ci-dessus et soit $x \in \mathfrak{n}(A)$. On a $x^n = 0 \in \mathfrak{p}$ pour tout idéal premier $\mathfrak{p}$ et donc $x \in \mathfrak{p}$. On en déduit $x \in \mathfrak{n}'$.

Réciproquement, soit $x \in A \setminus \mathfrak{n}(A)$ et soit

$$S = \{\mathfrak{a} \mid \mathfrak{a} \subset A \text{ idéal et } x^n \notin \mathfrak{a} \text{ pour tout } n \geq 1\}.$$

L'ensemble S ordonné par $\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow \mathfrak{a} \subset \mathfrak{b}$ est inductif : il est non vide car $\mathfrak{n}(A) \in S$ et si T est une chaine de S, alors

$$\mathfrak{b} = \bigcup_{\mathfrak{a} \in T} \mathfrak{a}$$

est un idéal. S'il existe $n \geq 1$ tel que $x^n \in \mathfrak{b}$ alors il existe $\mathfrak{a} \in T$ tel que $x^n \in \mathfrak{a}$, une contradiction au fait que $\mathfrak{a} \in T \subset S$. On a donc que $\mathfrak{b}$ est une borne supérieure de T et que S est inductif donc a un élément maximal $\mathfrak{p}$.

Nous montrons maintenant que $\mathfrak{p}$ est premier. Soient $y, z \in A \setminus \mathfrak{p}$, alors on a $\mathfrak{p} \subsetneq (y) + \mathfrak{p}$ et $\mathfrak{p} \subsetneq (z) + \mathfrak{p}$. On en déduit $(y) + \mathfrak{p} \notin S$ et $(z) + \mathfrak{p} \notin S$. Il existe donc $n, m \geq 1$ tels que $x^n \in (y) + \mathfrak{p}$ et $x^m \in (z) + \mathfrak{p}$. On a alors $x^{n+m} \in (yz) + \mathfrak{p}$ et $(yz) + \mathfrak{p} \notin S$. En particulier, on a $yz \notin \mathfrak{p}$ et $\mathfrak{p}$ est un idéal premier.

Nous en déduisons que $x \notin \mathfrak{p}$ avec $\mathfrak{p}$ un idéal premier et donc $x \notin \mathfrak{n}'$. On a donc $A \setminus \mathfrak{n}(A) \subset A \setminus \mathfrak{n}'$ et donc $\mathfrak{n}' \subset \mathfrak{n}(A)$. ∎

Définition 1.7.3 Soit $\mathfrak{a} \subset A$ un idéal, **le radical de** $\mathfrak{a}$ est l'ensemble

$$\sqrt{\mathfrak{a}} = \{x \in A \mid \text{il existe } n \geq 1 \text{ tel que } x^n \in \mathfrak{a}\}.$$

Proposition 1.7.4 Soit $\mathfrak{a} \subset A$ un idéal.

1. Alors $\sqrt{\mathfrak{a}}$ est un idéal.

2. Alors $A/\sqrt{\mathfrak{a}}$ est réduit.

3. On a $\mathfrak{a} = \sqrt{\mathfrak{a}} \Leftrightarrow A/\mathfrak{a}$ est réduit.

4. Le radical $\sqrt{\mathfrak{a}}$ est l'intersection des idéaux premiers contenant $\mathfrak{a}$:

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subset \mathfrak{p}, \text{ idéal premier}} \mathfrak{p}.$$

Preuve. 1. Soit $\pi : A \to A/\mathfrak{a}$, on a $\sqrt{\mathfrak{a}} = \pi^{-1}(\mathfrak{n}(A/\mathfrak{a}))$.

2. On a $A/\sqrt{\mathfrak{a}} \simeq (A/\mathfrak{a})/(\sqrt{\mathfrak{a}}/\mathfrak{a}) = (A/\mathfrak{a})/\mathfrak{n}(A/\mathfrak{a})$ qui est donc réduit.

3. On a $A/\mathfrak{a}$ réduit $\Leftrightarrow \mathfrak{n}(A/\mathfrak{a}) = 0 \Leftrightarrow A/\sqrt{\mathfrak{a}} = A/\mathfrak{a} \Leftrightarrow \sqrt{\mathfrak{a}} = \mathfrak{a}$.

4. Vient de l'égalité $\sqrt{\mathfrak{a}} = \pi^{-1}(\mathfrak{n}(A/\mathfrak{a}))$ avec $\pi : A \to A/\mathfrak{a}$ la projection canonique et de la proposition précédente pour $A/\mathfrak{a}$. ∎

Définition 1.7.5 Le radical de Jacobson $\mathfrak{R}(A)$ est l'intersection des idéaux maximaux de A :

$$\mathfrak{R}(A) = \bigcap_{\mathfrak{m} \subset A \text{ idéal maximal}} \mathfrak{m}.$$

Proposition 1.7.6 Soit $x \in A$, on a l'équivalence

$$x \in \mathfrak{R}(A) \Leftrightarrow 1 - xy \in A^\times \text{ pour tout } y \in A.$$

Preuve. ($\Rightarrow$) Soit $x \in \mathfrak{R}(A)$ et $y \in A$. Si $1 - xy$ n'est pas inversible, alors il existe un idéal maximal $\mathfrak{m}$ tel que $1 - xy \in \mathfrak{m}$. On a donc $1 = 1 - xy + xy \in \mathfrak{m}$, une contradiction.

($\Leftarrow$) Soit $x \notin \mathfrak{R}(A)$. Il existe alors un idéal maximal $\mathfrak{m}$ tel que $x \notin \mathfrak{m}$. On a alors $\mathfrak{m} \subsetneq (x) + \mathfrak{m}$ et donc $(x) + \mathfrak{m} = A$. On a donc un $y \in A$ et un $z \in \mathfrak{m}$ tels que $1 = xy + z$ *i.e.* $1 - xy = z \in \mathfrak{m}$. On en déduit que $1 - xy$ n'est pas inversible. ∎

1.8. Lemme chinois

Définition 1.8.1 Deux idéaux $\mathfrak{a}, \mathfrak{b} \subset A$ sont dis **premiers entre eux** si on a $\mathfrak{a} + \mathfrak{b} = A$.

Soit A un anneau et soient $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ des idéaux. On définit le morphisme d'anneaux suivant $f : A \to \prod_{i=1}^n A/\mathfrak{a}_i$ par $f(x) = ([x]_{\mathfrak{a}_1}, \cdots, [x]_{\mathfrak{a}_n})$, où $[x]_{\mathfrak{a}_i}$ est la classe de x dans $A/\mathfrak{a}_i$.

Proposition 1.8.2 (Lemme Chinois) Soit A un anneau et $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ des idéaux de A.

1.Si les idéaux $(\mathfrak{a}_i)_{i\in[1,n]}$ sont deux à deux premiers entre eux, alors on a $\prod_i \mathfrak{a}_i = \cap_i \mathfrak{a}_i$.

2. Le morphisme f est surjectif si et seulement si les idéaux $(\mathfrak{a}_i)_{i\in[1,n]}$ sont deux à deux premiers entre eux.

3. Le morphisme f est injectif si et seulement si $\cap_i \mathfrak{a}_i = 0$.

Preuve. 1. On procède par récurrence sur n. Le cas $n = 2$ est laissé en exercice (voir feuille 1). Supposons donc $n > 2$. Posons $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \cap_{i=1}^{n-1} \mathfrak{a}_i$. On a $\mathfrak{a}_i + \mathfrak{a}_n = A$ et donc des éléments $x_i \in \mathfrak{a}_i$, $y_i \in \mathfrak{a}_n$ tels que $x_i + y_i = 1$. On en déduit

$$\mathfrak{b} \ni x_1 \cdots x_{n-1} = (1 - y_1) \cdots (1 - y_{n-1}) \equiv 1 \pmod{\mathfrak{a}_n}.$$

On a donc $\mathfrak{b} + \mathfrak{a}_n = A$ puis $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} \cap \mathfrak{a}_n$.

2. ($\Rightarrow$) Nous montrons que $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont premiers entre eux (et de même on aura que $\mathfrak{a}_i$ et $\mathfrak{a}_j$ sont premiers entre eux pour tout $i \neq j$). Comme f est surjective, il existe $x \in A$ tel que $f(x) = (1, 0, \cdots, 0)$. On en déduit $x \equiv 1 \pmod{\mathfrak{a}_1}$ et donc $1 - x \in \mathfrak{a}_1$. On a alors $1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2$ et $A = \mathfrak{a}_1 + \mathfrak{a}_2$.

($\Leftarrow$) Il suffit de montrer qu'il existe $x \in A$ tel que $f(x) = (1, 0, \cdots, 0)$ (de même on aura $(0, \cdots, 0, 1, 0 \cdots, 0) \in \mathrm{Im}f$). Pour $i \geq 2$, on a des éléments $x_i \in \mathfrak{a}_1$ et $y_i \in \mathfrak{a}_i$ tels que $x_i + y_i = 1$. Soit $x = y_2 \cdots y_n$. On a alors $x = (1 - x_2) \cdots (1 - x_n) \equiv 1 \pmod{\mathfrak{a}_1}$ et $x \in \mathfrak{a}_i$ pour tout $i \geq 2$. On en déduit $f(x) = (1, 0, \cdots, 0)$.

3. On a $\mathrm{Ker}f = \cap_i \mathfrak{a}_i$. ∎

1.9. Lemme d'évitement

Proposition 1.9.1 Soit A un anneau.

1. Soient $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ des idéaux premiers et soit $\mathfrak{a}$ un idéal tel que

$$\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Alors il existe un indice i tel que $\mathfrak{a} \subset \mathfrak{p}_i$.

2. Soient $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ des idéaux et $\mathfrak{p}$ un idéal premier tel que

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \subset \mathfrak{p} \text{ (resp. } \bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p}).$$

Alors il existe un indice i tel que $\mathfrak{a}_i \subset \mathfrak{p}$ (resp. $\mathfrak{a}_i = \mathfrak{p}$).

Preuve. 1. Sans restriction, on peut supposer que n est minimal tel que $\mathfrak{a} \subset \cup_{i=1}^{n} \mathfrak{p}_i$. On montre que $n = 1$. Supposons donc que $n \geq 2$. Pour tout $j \in [1, n]$, on a

$$\mathfrak{a} \not\subset \bigcup_{i=1, i\neq j}^{n} \mathfrak{p}_i.$$

On peut donc choisir $x_j \in \mathfrak{a} \setminus \cup_{i=1, i\neq j}^{n} \mathfrak{p}_i$. On a alors $x_j \in \mathfrak{p}_j$ et $x = x_1 + x_2 \cdots x_n \in \mathfrak{a}$. Il existe donc un indice i tel que $x \in \mathfrak{p}_i$. Si $i \geq 2$, on a $x_1 = x - x_2 \cdots x_i \cdots x_k \in \mathfrak{p}_i$, une contradiction. Si $x \in \mathfrak{p}_1$, alors $x_2 \cdots x_k = x - x_1 \in \mathfrak{p}_1$. Comme $\mathfrak{p}_1$ est premier, on a un $j \geq 2$ tel que $x_j \in \mathfrak{p}_1$, une contradiction.

2. Si $\mathfrak{a}_i \not\subset \mathfrak{p}$ pour tout $i \in [1, n]$, on peut alors choisir $x_i \in \mathfrak{a}_i$ tel que $x_i \notin \mathfrak{p}$ pour tout $i \in [1, n]$ et on pose $x = x_1 \cdots x_n$. On a $x \in \mathfrak{a}_i$ pour tout i donc $x \in \mathfrak{p}$. On en déduit qu'il existe un i tel que $x_i \in \mathfrak{p}$, une contradiction. ∎

1.10. Conducteur

Définition 1.10.1 Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux de A. **Le conducteur de $\mathfrak{b}$ vers $\mathfrak{a}$** est l'ensemble

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subset \mathfrak{a}\}.$$

Si $\mathfrak{a} = 0$, le conducteur $(0 : \mathfrak{b})$ s'appelle aussi **l'annulateur de $\mathfrak{b}$**. On écrit alors $\mathrm{Ann}(\mathfrak{b}) = (0 : \mathfrak{b})$. Si $\mathfrak{b} = (x)$ est principal, on écrit $\mathrm{Ann}(\mathfrak{b}) = \mathrm{Ann}(x)$.

Remarque 1. Let conducteur est un idéal (exercice).

2. On a $\mathrm{Ann}(0) = A$.

3. L'ensemble des éléments diviseurs de zéro peut s'ecrire : $\bigcup_{x\neq 0} \mathrm{Ann}(x)$.

2. Modules

2.1. Definition

Définition 2.1.1 Soit A un anneau. Un **A-module** est un groupe abélien $(M, +)$ muni d'une multiplication scalaire $A \times M \to M$, $(a, m) \mapsto am$ telle que

1. $a(m + m') = am + am'$ pour $a \in A$ et $m, m' \in M$,
2. $(a + b)m = am + bm$ pour $a, b \in A$ et $m \in M$,
3. $a(bm) = (ab)m$ pour $a, b \in A$ et $m \in M$,
4. $1m = m$ pour $m \in M$.

Remarque Cette définition est équivalente à la donnée d'un groupe abélien M et d'un morphisme d'anneaux $A \to \mathrm{End}(M)$, où $\mathrm{End}(M)$ désigne l'anneau des morphismes de groupes de M dans lui même.

Remarque Le groupe trivial $M = \{0\}$ est un A-module pour tout anneau A avec $a0 = 0$. Ce module s'appelle **module trivial ou module nul**.

Exemple 1. L'anneau A est un A-module avec pour multiplication $A \times A \to A$, $(a, m) \mapsto am$.

2. Si $A = \mathsf{k}$ est un corps, on retrouve la notion d'espace vectoriel : (A-module) = (k-espace vectoriel).

3. Si $A = \mathbb{Z}$, on a (A-module) = (groupe abélien), avec $nm = \underbrace{m + \cdots + m}_{n \text{ fois}}$.

4. Pour $A = \mathsf{k}[X]$ avec k un corps, on a (A-module) = (k-espace vectoriel muni d'un endomorphisme f), avec pour multiplication $Xm = f(m)$.

Définition 2.1.5 Soit A un anneau.

1. **Un morphisme de A-modules** est une application $f : M \to N$, où M et N sont des A-modules telle que

1. $f(m + m') = f(m) + f(m')$ pour $m, m' \in M$ et
2. $f(am) = af(m)$ pour $a \in A$ et $m \in M$.

L'ensemble des morphismes de A-modules de M dans N se note $\mathrm{Hom}_A(M,N)$ (ou encore $\mathrm{Hom}(M,N)$).

2. Un isomorphisme de A-modules est un morphisme de A-modules bijectif.

Remarque 1. La composition de deux morphismes de A-modules est encore un morphisme de A-modules.

2. Un isomorphisme de A-module $f : M \to N$ peut aussi être caractérisé de la manière suivante : $f : M \to N$ est un isomorphisme si et seulement s'il existe $g : N \to M$ tel que $f \circ g = \mathrm{Id}_N$ et $g \circ f = \mathrm{Id}_M$.

3. L'ensemble $\mathrm{Hom}(M,N)$ est encore un A-module pour les opérations $(f+g)(m) = f(m) + g(m)$ et $(af)(m) = af(m)$.

4. Soient $g : M' \to M$ et $h : N \to N'$ deux morphismes de A-modules. Alors on a des morphismes de A-modules induits par la composition :

$$\mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N) \text{ und } \mathrm{Hom}(M,N) \to \mathrm{Hom}(M,N')$$

définis par $f \mapsto f \circ g$ et $f \mapsto h \circ f$.

5. On a un isomorphisme de A-modules $\mathrm{Hom}(A,M) \simeq M$ dont les bijections réciproques sont données par $f \mapsto f(1)$ et $m \mapsto (E_m : A \to M)$, avec $E_m(a) = am$.

2.2. Sous-modules

Définition 2.2.1 Soit M un A-modules. Un **sous-A-module ou sous-module** N de M est un sous-groupe N de M tel que $an \in N$ pour $a \in A$ et $n \in N$.

Remarque Les sous-A-modules de l'anneau A vu comme A-module sont les idéaux.

Lemme 2.2.3 Soit $f : M \to N$ un morphisme de A-modules. Alors $\mathrm{Ker} f$ et $\mathrm{Im} f$ sont des sous-A-modules.

Plus généralement, soient $M' \subset M$ et $N' \subset N$ des sous-A-modules, alors $f^{-1}(N')$ et $f(M')$ sont des sous-modules de M et N respectivement.

Preuve. Exercice. ∎

Tous les sous-modules peuvent être réalisés comme noyau d'un morphisme de modules.

Lemme 2.2.4 Soit $N \subset M$ un sous-A-module. Alors le quotient M/N du groupe M par son sous-groupe N peut-être muni d'une structure de A-module en posant $[m] + [m'] = [m + m']$ et $a[m] = [am]$.

La projection canonique $\pi : M \to M/N$ est alors un morphisme de A-modules et on a $\mathrm{Ker}\pi = N$.

Preuve. Exercice. ∎

Proposition 2.2.5 Soit $f : M \to N$ un morphisme de A-modules et $M' \subset M$ un sous-A-module et soit $\pi : M \to M/M'$ la projection canonique.

1. Il existe un morphisme de A-modules $\bar{f} : M/M' \to N$ tel que $f = \bar{f} \circ \pi$ si et seulement si $M' \subset \mathrm{Ker}f$.

Si un tel morphisme existe, alors on a

2. $\mathrm{Ker}\bar{f} = \mathrm{Ker}f/M'$.

3. L'application $\bar{f}$ est injective (resp. surjective) si et seulement si $\mathrm{Ker}f = M'$ (resp. f est surjective).

Preuve. Exercice. ∎

Corollaire Soit $f : M \to N$ un morphisme de modules, alors on a un isomorphisme $M/\mathrm{Ker}f \simeq \mathrm{Im}f$.

Définition 2.2.7 Soit $f : M \to N$ un morphisme de modules. **Le conoyau** $\mathrm{Coker}f$ **de** f est le quotient $\mathrm{Coker}f = N/\mathrm{Im}f$. Il mesure la (non)surjectivité de f

Définition 2.2.8 Une suite exacte de modules est une chaine de morphisme de modules

$$\cdots \to M_{i-1} \overset{f_{i-1}}{\to} M_i \overset{f_i}{\to} M_{i+1} \to \cdot$$

telle que $\mathrm{Im}f_{i-1} = \mathrm{Ker}f_i$ pour tout i.

Remarque 1. Une chaine $0 \to M \overset{f}{\to} N$ est exacte si et seulement si f est injective : $\mathrm{Ker}f = \mathrm{Im}0 = 0$.

2. Une chaine $M \overset{f}{\to} N \to 0$ est exacte si et seulement si f est surjective : $N = \mathrm{Ker}0 = \mathrm{Im}f$.

Proposition 2.2.10 Soit $f : M \to N$ un morphisme de A-modules. On a alors des suites exactes

$$0 \to \mathrm{Ker}f \to M \to \mathrm{Im}f \to 0$$
$$0 \to \mathrm{Im}f \to N \to \mathrm{Coker}f \to 0$$
$$0 \to \mathrm{Ker}f \to M \to N \to \mathrm{Coker}f \to 0.$$

Preuve. Nous montrons la dernière et laissons les deux premières en exercice. L'application $\mathrm{Ker}f \to M$ est injective et l'application $N \to N/\mathrm{Im}f = \mathrm{Coker}f$ est surjective. Il suffit donc de montrer que $\mathrm{Ker}(N \to \mathrm{Coker}f) = \mathrm{Im}(M \to N) = \mathrm{Im}f$ et $\mathrm{Ker}(M \to N) = \mathrm{Im}(\mathrm{Ker}f \to M)$. Les deux premiers sont égaux à $\mathrm{Im}f$ et les deux derniers à $\mathrm{Ker}f$. ∎

2.3. Operations sur les modules

Lemme 2.3.1 Soit $(M_i)_{i\in I}$ une famille de sous-A-modules de M. Alors $\cap_{i\in I}M_i$ est un sous-A-module.

Soit $E \subset M$ un sous-ensemble de M. Alors il existe un plus petit sous-module contenant E.

Preuve. Exercice. ∎

Définition 2.3.2 Soit M un A-module et $E \subset M$ un sous-ensemble. Le plus petit sous-module de M contenant E est appelé **le sous-module engendré par** E.

Remarque 1. Si $E = \cup_{i\in I}M_i$ avec $(M_i)_{i\in I}$ une famille de sous-modules, alors le sous-module engendré par E est **la somme**

$$\sum_{i\in I} M_i = \left\{ \sum_{i\in I} x_i \mid x_i \in M_i \text{ et } x_i \neq 0 \text{ pour un nombre fini de } i \in I \right\}.$$

2. Si $E = \{m_1, \cdots, m_n\}$, alors le sous-module engendré par E est de la forme

$$Am_1 + \cdots + Am_n = \left\{ \sum_{i=1}^{n} a_i m_i \mid a_i \in A \text{ pour tout } i \in I \right\}.$$

Proposition 2.3.4 Soit M un module.

1. Soient $P \subset N \subset M$ des sous-modules. On a un isomorphisme

$$(M/P)/(N/P) \simeq M/N.$$

2. Soient $P, N \subset M$ des sous-modules. On a un isomorphisme

$$(N+P)/N \simeq P/(N \cap P).$$

Preuve. 1. Soient $\pi_{M/N} : M \to M/N$ et $\pi_{M/P} : M \to M/P$ les projections canoniques. Comme $P \subset N = \mathrm{Ker}\pi_{M/N}$, il existe un morphisme $\bar{\pi}_{M/N} : M/P \to M/N$ tel que $\pi_{M/N} = \bar{\pi}_{M/N} \circ \pi_{M/P}$. Ce morphisme est surjectif (car $\pi_{M/N}$ est surjectif) et on a $\mathrm{Ker}\bar{\pi}_{M/N} = N/P$ d'où le 1.

2. Soit $f : P \to (N+P)/N$ définit par $f(p) = [p]$. Alors on a f surjectif. En effet, soit $[n+p] \in (N+P)/N$, avec $n \in N$ et $p \in P$. Alors on a $f(p) = [p] = [n+p]$. De plus on a $\mathrm{Ker}f = N \cap P$. On en déduit le résultat. ∎

Définition 2.3.5 Soit M un A-module et soit $\mathfrak{a} \subset A$ un idéal. **Le produit** $\mathfrak{a}M$ est l'ensemble

$$\mathfrak{a}M = \left\{ \sum_{i=1}^{n} a_i m_i \mid n \geq 1, a_i \in \mathfrak{a}, m_i \in M \right\}.$$

Remarque Le produit $\mathfrak{a}M$ est un sous-module de M. C'est le sous-module engendré par les éléments de la forme am avec $a \in \mathfrak{a}$ et $m \in M$.

Définition 2.3.7 Soit M un A-module et soient $N, P \subset M$ des sous-modules.

1. **Le conducteur** $(N : P)$ de P dans N est l'ensemble

$$(N : P) = \{a \in A \mid aP \subset N\}.$$

Si $N = 0$, le conducteur $(0 : M)$ s'appelle **l'annulateur de** M, on le note $\mathrm{Ann}(M)$.

2. Un module M est dit **fidèle** si $\mathrm{Ann}(M) = 0$.

Remarque 1. Le conducteur et l'annulateur sont des idéaux.

2. Le module M est fidèle si et seulement si l'application $A \to \mathrm{End}(M)$ associée est injective. Le noyau de cette application est l'annulateur :

$$\mathrm{Ann}(M) = \mathrm{Ker}(A \to \mathrm{End}(M)).$$

Exemple 1. Soit $A = \mathbb{Z}$ et $M = \mathbb{Z}/n\mathbb{Z}$. On a alors $\mathrm{Ann}(M) = n\mathbb{Z}$.

2. Soit $A = \mathbb{Z}$ et $M = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Alors on a $\mathrm{Ann}(M) = n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{ppcm}(n, m)\mathbb{Z}$.

Lemme 2.3.10 Soit M un A-module et soit $\mathfrak{a} \subset \mathrm{Ann}(M) \subset A$ un idéal. Alors M est un $A/\mathfrak{a}$-module pour la multiplication $[a]m = am$.

Preuve. Il suffit de monter que cette multiplication est bien définie. Soit $a' \in \mathfrak{a}$, on a $(a + a')m = am + a'm = am$ car $a' \in \mathfrak{a} \subset \mathrm{Ann}(M)$. ∎

Corollaire Soit M un A-module. Alors M est un $A/\mathrm{Ann}(M)$-module fidèle.

Exemple Soit $A = \mathbb{Z}$ et $M = \mathbb{Z}/n\mathbb{Z}$. Alors M est un $\mathbb{Z}/n\mathbb{Z}$-module fidèle.

2.4. Somme directe et produit

Définition 2.4.1 Soit A un anneau.

1. Soient M et N deux A-modules. **La somme directe** $M \oplus N$ **de** M **et** N est l'ensemble $M \times N$ muni de l'addition $(m, n) + (m', n') = (m + m', n + n')$ et de la multiplication $a(m, n) = (am, an)$.

2. Plus généralement, soit $(M_i)_{i \in I}$ une famille de A-modules. **La somme directe** $\oplus_{i \in I} M_i$ **de la famille** $(M_i)_{i \in I}$ est l'ensemble

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i \text{ et } m_i = 0 \text{ sauf pour un nombre fini d'indices } i \in I\}$$

muni de l'addition $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$ et de la multiplication $a(m_i)_{i\in I} = (am_i)_{i\in I}$.

3. Soit $(M_i)_{i\in I}$ une famille de A-modules. **Le produit $\prod_{i\in I} M_i$ de la famille** $(M_i)_{i\in I}$ est l'ensemble

$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i\}$$

muni de l'addition $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$ et de la multiplication $a(m_i)_{i\in I} = (am_i)_{i\in I}$.

Remarque 1. La somme directe et le produit sont des A-modules.

2. Si I est fini, alors $\oplus_{i\in I} M_i$ et $\prod_{i\in I} M_i$ sont isomorphies. En général, la somme directe $\oplus_{i\in I} M_i$ est un sous-module du produit $\prod_{i\in I} M_i$ et on a

$$\bigoplus_{i\in I} M_i \subsetneq \prod_{i\in I} M_i.$$

Exemple L'ensemble A^n avec l'addition composante par composante et la multiplication diagonale par un scalaire est un A-module. C'est la somme directe (et le produit) de la famille de modules suivante : $(M_i)_{i\in I}$, avec $I = [1, n]$ et $M_i = A$ pour tout $i \in [1, n]$.

Plus généralement, si I est un ensemble, l'ensemble

$$A^{(I)} = \{(x_i)_{i\in I} \mid x_i \in A \text{ et } x_i = 0 \text{ sauf pour un nombre fini d'indices } i \in I\}$$

est la somme directe de la famille $(M_i)_{i\in I}$, avec $M_i = A$ pour tout $i \in [1, n]$. De même

$$A^I = \{(x_i)_{i\in I} \mid x_i \in A\}$$

est le produit de la famille $(M_i)_{i\in I}$, avec $M_i = A$ pour tout $i \in [1, n]$.

Définition 2.4.4 Un module est dit **libre**, s'il existe un ensemble I tel que M est isomorphe à $A^{(I)}$.

Un module s'appelle **libre de type fini**, s'il existe un entier n tel que M est isomorphe à A^n.

2.5. Modules finiment engendrés

Définition 2.5.1 Un module M est dit **finiment engendré ou de type fini** s'il existe un nombre fini d'éléments $m_1, \cdots, m_n \in M$ tels que $M = Am_1 + \cdots + Am_n$.

Proposition 2.5.2 Un module M est de type fini si et seulement s'il existe un morphisme surjectif $f : A^n \to M$.

Preuve. Soit x_i le i-ème élément de la base canbonique de A^n *i.e.* $x_i = (0, \cdots, 0, 1, 0,)$ où le 1 est à la i-ème place. On a $A^n = Ax_1 + \cdots + Ax_n$. On en déduit $M = f(A) = Af(x_1) + \cdots + Af(x_n)$ et donc la famille $(f(x_1), \cdots, f(x_n))$ engendre M.

Réciproquement, soit $(m_1, \cdots, m_n) \in M$ une famille génératrice de M. Soit alors $f : A^n \to M$ l'application définie par $f(a_1, \cdots, a_n) = a_1m_1 + \cdots a_nm_n$. On vérifie aisément que f est un morphisme de A-modules et par définition, il est surjectif d'où le résultat. ∎

Exemple Le A-module A est libre et de type fini.

Remarque Un sous-module d'un module de type fini n'est pas toujours de type fini.

Par exemple, soit $A = \mathsf{k}[X_1, \cdots, X_n, \cdots]$ l'anneau des polynômes en une infinité d'indéterminées. Alors le A-module $M = A$ est de type fini (1 est un générateur). Soit maintenant $N = (X_1, \cdots, X_n, \cdots)$ l'idéal engendré par les variables. C'est un sous-module de $M = A$ mais il n'est pas de type fini. En effet, s'il était de type fini, on aurait besoin d'un nombre fini de variables pour décrire tous ses éléments ce qui n'est pas le cas.

2.6. Suite exactes I

Proposition 2.6.1 Soit N un A-module.

1. Soit $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ une suite exacte. Alors il existe une suite exacte $0 \to \mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M) \xrightarrow{\bar{v}} \mathrm{Hom}(N, M'')$.

2. Soit $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ une suite exacte. Alors il existe une suite exacte $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$.

Preuve. 1. Les applications $\bar{u}$ et $\bar{v}$ sont définies de la façon suivante : $\bar{u}(f) = u \circ f$ et $\bar{v}(f) = v \circ f$.

Soit $f' : N \to M'$ tel que $f' \in \mathrm{Ker}\bar{u}$. On a $\bar{u}(f') = u \circ f' = 0$ et comme u est injective, on a en déduit $f' = 0$.

Soit $f' : N \to M'$. On a $\bar{v}(\bar{u}(f')) = v \circ u \circ f' = 0$ (on a $v \circ u = 0$, car $\mathrm{Im}u \subset \mathrm{Ker}v$).

Soit $f : N \to M$ tel que $f \in \mathrm{Ker}\bar{v}$. On a $\bar{v}(f) = v \circ f = 0$. Soit $n \in N$, on a $v(f(n)) = 0$ donc $f(n) \in \mathrm{Ker}v = \mathrm{Im}u$. Il existe donc un unique élément $m' \in M'$ tel que $f(n) = u(m')$. On pose $f' : N \to M'$, $n \mapsto m'$. On vérifie (exercice) que f' est linéaire. Par ailleurs, on a $\bar{u}(f')(n) = u \circ f'(n) = u(m') = f(n)$. On en déduit $f = \bar{u}(f') \in \mathrm{Im}\bar{u}$.

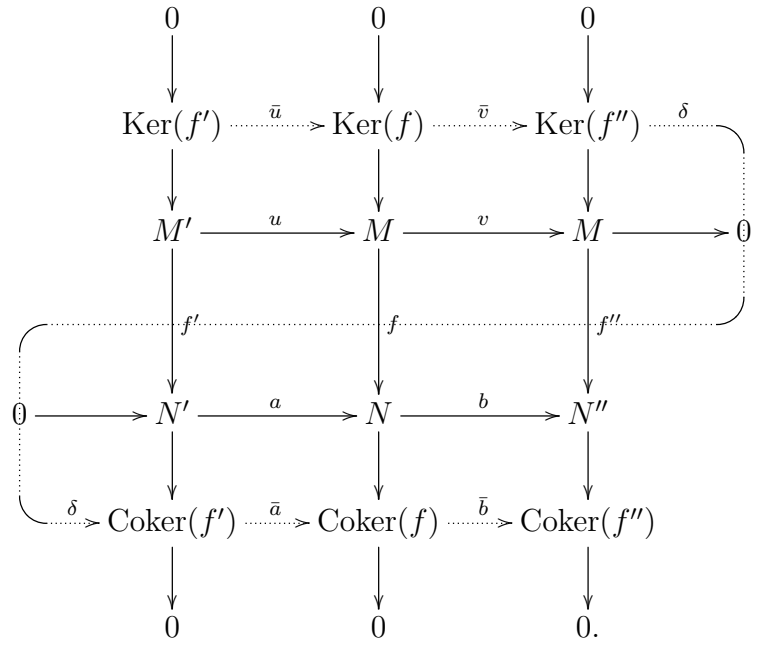
2. Les applications $\bar{u}$ et $\bar{v}$ sont définies comme suit : $\bar{u}(f) = f \circ u$ et $\bar{v}(f) = f \circ v$.

Soit $f'' : M'' \to N$ tel que $f'' \in \mathrm{Ker}\bar{v}$. On a $\bar{v}(f'') = f'' \circ v = 0$ et comme v est surjective, on en déduit $f'' = 0$.

Soit $f'' : M'' \to N$. On a $\bar{u}(\bar{v}(f'')) = f'' \circ u \circ v = 0$ (on a $v \circ u = 0$, car $\mathrm{Im}u \subset \mathrm{Ker}v$).

Soit $f : M \to N$ tel que $f \in \mathrm{Ker}\bar{u}$. On a $f(\mathrm{Im}u) = 0$. Soit $m'' \in M''$. Choisissons $m \in M$ tel que $v(m) = m''$. Nous montrons que $f(m)$ ne dépend pas du choix de ce m. En effet, soit $m_1 \in M$ tel que $v(m_1) = m''$. On a $v(m_1) = v(m)$ et donc $m_1 - m \in \mathrm{Ker}v = \mathrm{Im}u$. On a donc $f(m_1 - m) = 0$ et $f(m_1) = f(m)$. L'application $f'' : M'' \to N$, $m'' \mapsto f(m)$ est ainsi bien définie et linéaire (exercice). On a par ailleurs $\bar{v}(f'')(m) = f'' \circ v(m) = f''(m'') = f(m)$. On en déduit $f = \bar{v}(f'') \in \mathrm{Im}\bar{v}$. ∎

Proposition 2.6.2 (Lemme du serpent) Soient $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ et $0 \to N' \xrightarrow{a} N \xrightarrow{b} N''$ deux suites exactes et soient $f' : M' \to N'$, $f : M \to N$ et $f'' : M'' \to N''$ tels que les deux lignes du milieu du diagramme suivant forment un diagramme commutatif :



1. Alors il existe une application $\delta : \mathrm{Ker}(f'') \to \mathrm{Coker}(f')$ telle que la suite suivante soit exacte :

$$\mathrm{Ker}(f') \xrightarrow{\bar{u}} \mathrm{Ker}(f) \xrightarrow{\bar{v}} \mathrm{Ker}(f'') \xrightarrow{\delta} \mathrm{Coker}(f') \xrightarrow{\bar{a}} \mathrm{Coker}(f) \xrightarrow{\bar{b}} \mathrm{Coker}(f'').$$

2. On a l'équivalence ($\bar{u} : \mathrm{Ker}(f') \to \mathrm{Ker}(f)$ injective $\Leftrightarrow$ u injective).

3. On a l'équivalence ($\bar{b} : \mathrm{Coker}(f) \to \mathrm{Coker}(f'')$ surjective $\Leftrightarrow$ v surjective).

Preuve. 1. Soit $m' \in \mathrm{Ker}f'$. On pose $\bar{u}(m') = u(m')$. On a $f(u(m')) = a(f'(m')) = a(0) = 0$. On en déduit $u(m) \in \mathrm{Ker}(f)$ et $\bar{u} : \mathrm{Ker}(f') \to \mathrm{Ker}(f)$ est bien défini.

De même on a $v(m) \in \mathrm{Ker}(f'')$ pour tout $m \in \mathrm{Ker}(f)$ et $\bar{v} : \mathrm{Ker}(f) \to \mathrm{Ker}(f'')$, $\bar{v}(m) = v(m)$ est bien défini.k

Soient $\pi' : N' \to \mathrm{Coker}(f')$, $\pi : N \to \mathrm{Coker}(f)$ et $\pi'' : N'' \to \mathrm{Coker}(f'')$ les projections canoniques. Soit $\pi'(n') \in \mathrm{Coker}(f') = N/\mathrm{Im}(f')$. On pose $\bar{a}(\pi'(n')) = \pi(a(n'))$ et on montre que ceci ne dépend que de $\pi'(n')$ (et pas de n'). Soit $n'_1 \in N'$ tel que $\pi'(n'_1) = \pi'(n')$. On a $n'_1 - n \in \mathrm{Im}(f')$: il existe donc $m' \in M'$ tel que $n'_1 = n' + f'(m')$. On en déduit $\pi(a(n'_1)) = \pi(a(n')) + \pi(a(f'(m'))) = a(n') + \pi(f(u(m')))$. Comme $\pi(\mathrm{Im}(f) = 0$, on a $\pi(a(n'_1)) = \pi(a(n'))$ et $\bar{a} : \mathrm{Coker}(f') \to \mathrm{Coker}(f)$ est bien défini. De même, on définit $\bar{b} : \mathrm{Coker}(f) \to \mathrm{Coker}(f'')$.

On définit maintenant δ. Soit $m'' \in \mathrm{Ker}(f'')$. Soit $m \in M$ tel que $v(m) = m''$. On a alors $b(f(m)) = f''(v(m)) = f''(m'') = 0$ et donc $f(m) \in \mathrm{Ker}b = \mathrm{Im}a$. Il existe donc un unique élément $n' \in N'$ tel que $a(n') = f(m)$. On pose $\delta(m'') = \pi'(n')$. On montre que $\delta(m'')$ ne dépend pas du choix de m : soit $m_1 \in M$ tel que $v(m_1) = m'' = v(m)$. On a $v(m_1 - m) = 0$ donc $m_1 - m \in \mathrm{Ker}v = \mathrm{Im}u$. Il existe donc $m' \in M'$ tel que $m_1 = m + u(m')$. On a donc $f(m_1) = f(m) + f(u(m')) = f(m) + a(f'(m'))$. On en déduit $f(m_1) = a(n') + a(f'(m')) = a(n' + f'(m'))$ et $n' + f'(m'))$ est l'unique élément vérifiant cette relation (car a est injectif). On a donc $\pi'(n' + f'(m')) = \pi'(n')$ (car $\pi'(\mathrm{Im}f') = 0$). On en déduit que $\delta(m'')$ est bien défini.

On vérifie (exercice) que $\bar{u}$, $\bar{v}$, $\bar{a}$, $\bar{b}$ et δ sont linéaires.

Montrons maintenant que la suite est exacte.

En $\mathrm{Ker}(f)$**.** Soit $m' \in \mathrm{Ker}(f')$. On a $\bar{v}(\bar{u}(m')) = v(u(m')) = 0$ car $\mathrm{Im}u = \mathrm{Ker}v$. Soit $m \in \mathrm{Ker}(f)$ tel que $\bar{v}(m) = 0$. On a alors $v(m) = 0$. On en déduit qu'il existe un $m' \in M'$ tel que $u(m') = m$. On a $a(f'(m')) = f(u(m')) = f(m) = 0$. Comme a est injective, on a $f'(m') = 0$ et $m' \in \mathrm{Ker}(f')$. On a donc $\bar{u}(m') = u(m') = m$.

En $\mathrm{Ker}(f'')$**.** Soit $m \in \mathrm{Ker}(f)$ et posons $m'' = \bar{v}(m) = v(m) \in \mathrm{Ker}(f'')$. On a $f(m) = 0$ et il existe donc un unique élément $0 = n' \in N'$ tel que $a(n') = f(m) = 0$. On a $\delta(m'') = \pi'(n') = \pi'(0) = 0$.

Soit $m'' \in \mathrm{Ker}(f'')$ tel que $\delta(m'') = 0$. Soit $m \in M$ avec $v(m) = m''$. On a $f(m) \in \mathrm{Ker}b$ et il existe donc un $n' \in N'$ tel que $a(n') = f(m)$. Par définition, on a $\delta(m'') = \pi'(n')$. On en déduit $\pi'(n') = 0$ donc $n' \in \mathrm{Im}(f')$. Il existe donc $m' \in M'$ tel que $f'(m') = n'$. Ona alors $f(u(m')) = a(f'(m)) = a(n') = f(m)$ et donc $m - u(m') = m_1 \in \mathrm{Ker}(f)$. On en déduit $m = u(m') + m_1$ et $m'' = v(u(m')) + v(m_1) = v(m_1) = \bar{v}(m_1)$.

En $\mathrm{Coker}(f')$**.** Soit $m'' \in \mathrm{Ker}(f'')$. On prend $m \in M$ tel que $v(m) = m''$. On a $f(m) \in \mathrm{Ker}b$ et il existe un $n' \in N'$ tel que $a(n') = f(m)$. Par définition, on a $\delta(m'') = \pi'(n')$. On a aussi $\bar{a}(\delta(m'')) = \bar{a}(\pi'(n')) = \pi(a(n')) = \pi(f(m)) = 0$.

Soit $\pi'(n') \in \mathrm{Ker}\bar{a}$. On a $0 = \bar{a}(\pi'(n')) = \pi(a(n'))$. On en déduit $a(n') \in \mathrm{Im}f$. Prenons $m \in M$ tel que $f(m) = a(n')$ et soit $m'' = v(m)$. On a $f''(m'') = f''(v(m)) = b(f(m)) = b(a(n')) = 0$. On a alors $m'' \in \mathrm{Ker}(f'')$ et par définition de δ on a $\delta(m'') = \pi'(n')$.

En Coker(f)**.** Soit $\pi'(n') \in \text{Coker}(f')$ avec $n' \in N'$. On a $\bar{b}(\bar{a}(\pi'(n'))) = \pi''(b(a(n'))) = \pi''(0) = 0$.

Soit $\pi(n) \in \text{Ker}\bar{b}$ tel que $n \in N$. On a $0 = \bar{b}(\pi(n)) = \pi''(b(n))$. On a donc $b(n) \in \text{Im}f''$. Prenons $m'' \in M''$ tel que $f''(m'') = b(n)$ et prenons $m \in M$ tel que $v(m) = m''$. On a $b(f(m)) = f''(v(m)) = f''(m'') = b(n)$. On a donc $n - f(m) \in \text{Ker}b = \text{Im}a$. Prenons $n' \in N'$ tel que $a(n') = n - f(m)$. On a $\bar{a}(\pi'(n')) = \pi(a(n')) = \pi(n - f(m)) = \pi(n) - \pi(f(m)) = \pi(n)$.

2. ($\Leftarrow$) Soit $m' \in \text{Ker}(f')$ tel que $\bar{u}(m') = 0$. On a alors $u(m') = 0$ et comme u est injective, on a $m' = 0$.

($\Rightarrow$) Soit $m' \in M'$ tel que $u(m') = 0$. On a $0 = f(u(m') = a(f'(m'))$ et comme a est injective, on a $f'(m') = 0$. On a a donc $m' \in \text{Ker}f'$ et $\bar{u}(m') = u(m') = 0$. Comme $\bar{u}$ est injective, on en déduit $m' = 0$.

3. ($\Leftarrow$) Soit $\pi''(n'') \in \text{Coker}(f'')$ avec $n'' \in N''$. Soit $n \in N$ tel que $b(n) = n''$. On a $\bar{b}(\pi(n)) = \pi''(b(n)) = \pi''(n'')$.

($\Rightarrow$) Soit $n'' \in N''$. Alors on a $\pi''(n'') \in \text{Coker}(f'')$. Soit $\pi(n) \in \text{Coker}(f)$ avec $n \in N$ tel que $\bar{b}(\pi(n)) = \pi''(n'')$. On a alors $\pi''(b(n)) = \bar{b}(\pi(n)) = \pi''(n'')$. On en déduit $b(n) - n'' \in \text{Ker}\pi'' = \text{Im}f''$. Soit $m'' \in M''$ tel que $f''(m'') = n'' - b(n)$ et soit $m \in M$ tel que $v(m) = m''$. On a $b(n + f(m)) = b(n) + b(f(m)) = b(n) + f''(v(m)) = b(n) + f''(m'') = b(n) + n'' - b(n) = n''$. ∎

Définition 2.6.3 Une fonction $\ell : \{A\text{-modules}\} \to \mathbb{Z}$ s'appelle **additive**, si on a $\ell(M) = \ell(M') + \ell(M'')$ pour tout suite exacte courte $0 \to M' \to M \to M'' \to 0$.

Exemple Soit $A = \mathsf{k}$ un corps, alors la fonction $\ell(M) = \dim_{\mathsf{k}} M$ est une fonction additive : pour toute suite exacte $0 \to M' \to M \to M'' \to 0$, on a $M'' \simeq M/M'$ on a $\dim M'' = \dim M - \dim M'$ (en effet $M'' \simeq M/M'$).

Remarque Si ℓ est une fonction additive, on a toujours $\ell(0) = 0$: en effet, on a la suite exacte courte "triviale" suivante : $0 \to M' = 0 \to M = 0 \to M'' = 0 \to 0$. On doit donc avoir $\ell(0) = \ell(0) + \ell(0)$ et donc $\ell(0) = 0$.

Lemme 2.6.6 Soit

$$0 \xrightarrow{u_{-1}} M_0 \xrightarrow{u_0} M_1 \xrightarrow{u_1} \cdots \xrightarrow{u_{n-1}} M_n \xrightarrow{u_n} 0$$

une suite exacte. Alors pour tout $i \in [0, n-1]$, on a une suite exacte courte

$$0 \to \text{Im}u_{i-1} \to M_i \to \text{Ker}u_{i+1} \to 0.$$

Preuve. Comme $\text{Im}u_i = \text{Ker}u_{i+1}$, on a un morphisme surjectif $M_i \to \text{Ker}u_{i+1}$ défini par $m_i \mapsto u_i(m_i)$. Le noyau est $\text{Ker}u_i = \text{Im}u_{i-1}$. ∎

Corollaire Soit ℓ une fonction additive et soit

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

une suite exacte. Alors on a

$$\sum_{i=0}^{n}(-1)^i \ell(M_i) = 0.$$

Preuve. Par le lemme précédent, on a $\ell(M_i) = \ell(\mathrm{Im}u_{i-1}) + \ell(\mathrm{Ker}u_{i+1}) = \ell(\mathrm{Ker}u_i) + \ell(\mathrm{Ker}(u_{i+1})$ pour tout $i \in [0, n-1]$. On en déduit

$$\sum_{i=0}^{n}(-1)^i \ell(M_i) = \sum_{i=0}^{n-1}(-1)^i \ell(\mathrm{Ker}u_i) + \ell(\mathrm{Ker}(u_{i+1}) + (-1)^n \ell(M_n) = \ell(\mathrm{Ker}u_0).$$

Comme u_0 est injective, on a $\mathrm{Ker}u_0 = 0$ et $\ell(\mathrm{Ker}u_0) = 0$. ∎

2.7. Lemme de Nakayama

Proposition 2.7.1 Soit M un module de type fini et soit $\mathfrak{a} \subset A$ un idéal. Soit $f \in \mathrm{End}(M)$ tel que $f(M) \subset \mathfrak{a}M$.

Alors il xiste des éléments $a_1, \cdots, a_n \in \mathfrak{a}$ tels que

$$f^n + a_1 f^{n-1} + \cdots + a_n \mathrm{Id}_M = 0.$$

Preuve. Si $M = A^n$ et $\mathfrak{a} = A$, alors c'est le théorème de Cayley-Hamilton. On va s'en inspirer.

Soient $m_1, \cdots, m_n$ des générateurs de M. On a $f(m_i) \in \mathfrak{a}M$ donc il existe des éléments $a_{i,j} \in \mathfrak{a}$ tels que $f(m_i) = \sum_{j=1}^n a_{i,j} m_j$. On a donc $\sum_{j=1}^n (\delta_{i,j} f(m_j) - a_{i,j} m_j) = 0$ et donc

$$\sum_{j=1}^{n}(\delta_{i,j} f - a_{i,j}\mathrm{Id}_M)(m_j).$$

On considère maintenant la matrice $P = (P_{i,j})_{i,j\in[1,n]} \in M_n(\mathrm{End}(M))$ définie par

$$P_{i,j} = \delta_{i,j} f - a_{i,j}\mathrm{Id}_M.$$

Soit $\mathrm{Com}(P)$ sa comatrice. On a $\mathrm{Com}(P)^T P = \det(P) I_n \in \mathrm{End}(M)$. Soit $(m_1, \cdots, m_n) \in M^n$. On a $P(m_1, \cdots, m_n)^T = 0$ ce qui nous donne

$$\det(P) I_n (m_1, \cdots, m_n)^T = \mathrm{Com}(P)^T P (m_1, \cdots, m_n)^T = 0$$

et donc

$$\det(P) m_i = 0 \text{ pour tout } i \in [1, n].$$

Comme $m_1, \cdots, m_n$ est génératrice, on a $\det(P) = 0$ comme élément de $\mathrm{End}(M)$. Mais la matrice P est de la forme

$$\begin{pmatrix} f - a_{1,1}\mathrm{Id}_M & -a_{1,2}\mathrm{Id}_M & \cdots & -a_{1,n}\mathrm{Id}_M \\ -a_{2,1}\mathrm{Id}_M & f - a_{2,2}\mathrm{Id}_M & \ddots & -a_{2,n}\mathrm{Id}_M \\ \vdots & \ddots & \ddots & \vdots \\ -a_{n,1}\mathrm{Id}_M & \cdots & -a_{n,n-1}\mathrm{Id}_M & f - a_{n,n}\mathrm{Id}_M \end{pmatrix}$$

donc l'équation $\det(P) = 0$ est de la forme $f^n + a_1 f^{n-1} + \cdots + a_n \mathrm{Id}_M = 0$ ce que l'on cherchait à démontrer. ∎

Corollaire Soit M un A-module de type fini et $\mathfrak{a}$ un idéal tel que $\mathfrak{a}M = M$. Alors il existe un élément $x \in A$ tel que $x \equiv 1 \pmod{\mathfrak{a}}$ et $xM = 0$.

Preuve. Soit $f = \mathrm{Id}_M$ et $x = 1 + a_1 + \cdots + a_n$ avec $a_i \in \mathfrak{a}$ donné par la proposition précédente. On a $x \equiv 1 \pmod{\mathfrak{a}}$ et $x\mathrm{Id}_M = 0$ donc $xM = 0$. ∎

Corollaire (Lemme de Nakayama) Soit M un A-module de type fini et $\mathfrak{a} \subset A$ un idéal tel que $\mathfrak{a} \subset \mathfrak{R}(A)$ et $\mathfrak{a}M = M$. Alors $M = 0$.

Preuve. D'après le corollaire précédent, il existe un $x \equiv 1 \pmod{\mathfrak{a}}$ tel que $xM = 0$. On a aussi $x = 1 - y$ avec $y \in \mathfrak{R}(A)$. On en déduit (cf. Lemme 1.7.6) que x est inversible et donc $M = x^{-1}xM = x^{-1}0 = 0$. ∎

Corollaire Soit M un A-module de type fini et N un sous-module de M. Soit $\mathfrak{a} \subset \mathfrak{R}(A)$ un idéal tel que $M = \mathfrak{a}M + N$. Alors $M = N$.

Preuve. On a $\mathfrak{a}(M/N) = M/N$. D'après le Lemme de Nakayama on a $M/N = 0$ et donc $M = N$. ∎

Corollaire Soit A un anneau local d'idéal maximal $\mathfrak{m}$ et soit M un A-module de type fini. Soient $m_1, \cdots, m_n \in M$ tel que $[m_1], \cdots, [m_n]$ est une famille génératrice de $M/\mathfrak{m}M$.

Alors $(m_1, \cdots, m_n)$ est génératrice pour M.

Preuve. Soit $N = Am_1 + \cdots + Am_n$. L'application $N \to M \to M/\mathfrak{m}M$ est surjective. On a donc $N + \mathfrak{m}M = M$. Comme $\mathfrak{m} \subset \mathfrak{R}(A)$, on a par le résultat précédent l'égalité $M = N$. ∎

2.8. Produit tensoriel

Nous construisons à partir de deux A-modules M et N un nouvel A-module $M \otimes_A N$.

Définition 2.8.1 Soient M, N et P des A-modules. Une application $f : M \times N \to P$ est dite **A-bilinéaire** si pour tout $a, b \in A$, tout $m, m' \in M$ et tout $n, n' \in N$ on a :

— $f(am + bm', n) = af(m, n) + bf(m', n)$

— $f(m, an + bn') = af(m, n) + bf(m, n')$.

Lemme 2.8.2 Soit $f : M \times N \to P$ une application bilinéaire et soit $g : P \to Q$ un morphisme de A-modules. Alors la composée $g \circ f$ est bilinéaire.

Preuve. Exercice. ∎

Définition 2.8.3 Un A-module E s'appelle **produit tensoriel** de M et N si les propositions suivantes sont vérifiées :

1. Il existe une application bilinéaire $\pi_E : M \times N \to E$ et
2. pour toute application bilinéaire $f : M \times N \to P$, il existe une unique application linéaire $L_f^E : E \to P$ telle que $L_f^E \circ \pi_E = f$.

Proposition 2.8.4 Soient E et F deux produits tensoriels de M et N. Alors E et F sont isomorphes.

Preuve. Par le premier point de la définition, il existe des applications bilinéaires $\pi_E : M \times N \to E$ et $\pi_F : M \times N \to F$. Par le second point de la définition, il existe des morphismes uniques $L_{\pi_F}^E : E \to F$ et $L_{\pi_E}^F : F \to E$ tels que $\pi_F = L_{\pi_F}^E \circ \pi_E$ et $\pi_E = L_{\pi_E}^F \circ \pi_F$. Nous montrons que $L_{\pi_E}^F$ et $L_{\pi_F}^E$ sont inverses l'un de l'autre.

Nous avons une application bilinéaire $f = L_{\pi_E}^F \circ L_{\pi_F}^E \circ \pi_E : M \times N \to E$ telle que $f = L_{\pi_E}^F \circ L_{\pi_F}^E \circ \pi_E = L_{\pi_E}^F \circ \pi_F = \pi_E$. Par le second point de la définition, il existe un seul morphisme L_f^E tel que $L_f^E \circ \pi_E = f = \pi_E$. Mais $\mathrm{Id}_E \circ \pi_E = \pi_E$ donc $L_f^E = \mathrm{Id}_E$. On a aussi $f = L_{\pi_E}^F \circ L_{\pi_F}^E \circ \pi_E$ et $L_f^E = L_{\pi_E}^F \circ L_{\pi_F}^E$ et de la même manière, on a $L_{\pi_E}^F \circ L_{\pi_F}^E = \mathrm{Id}_E$.

De même $L_{\pi_F}^E \circ L_{\pi_E}^F = \mathrm{Id}_F$. On en déduit que $L_{\pi_E}^F$ et $L_{\pi_F}^E$ sont inverses l'un de l'autre. ∎

Ainsi, s'il existe, le produit tensoriel est unique à isomorphisme près. Nous montrons maintenant qu'il existe un produit tensoriel. Pour celà considérons le module libre

$$A^{(M\times N)} = \left\{ \varphi : M \times N \to A \;\middle|\; \varphi(m,n) = 0 \quad \begin{array}{c}\text{sauf pour un nombre fini}\\ \text{d'éléments } (m,n) \in M \times N\end{array} \right\}.$$

Pour $(m, n) \in M \times N$, il existe une application $\varphi_{(m,n)}$ telle que

$$\varphi_{(m,n)}(m, n') = \begin{cases} 1 & \text{pour } (m', n') = (m, n) \\ 0 & \text{sinon.} \end{cases}$$

Lemme 2.8.5 Le système $(\varphi_{(m,n)})_{(m,n)\in M\times N}$ forme une base de $A^{(M\times N)}$. Plus précisément, le système $(\varphi_{(m,n)})_{(m,n)\in M\times N}$ est linéairement indépendant et pour $\varphi \in A^{(M\times N)}$, on a

$$\varphi = \sum_{(m,n)\in M\times N} \varphi(m,n)\varphi_{(m,n)}.$$

Dans la somme ci-dessus, n'apparait qu'un nombre fini de termes $\varphi(m,n)\varphi_{(m,n)}$ non nuls.

Preuve. Exercice. ∎

Les applications

$$\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)} \text{ et } \varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')}$$

sont des éléments de $A^{(M\times N)}$. On considère le sous-module suivant de $A^{(M\times N)}$:

$$L = \langle \varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}, \varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')} \rangle.$$

Définition 2.8.6 On pose $M \otimes_A N = A^{(M\times N)}/L$ et notons $p : A^{(M\times N)} \to M \otimes_A N$ la projection canonique. Pour $(m,n) \in M \times N$, on note $m \otimes n = p(\varphi_{(m,n)})$ l'image de $\varphi_{(m,n)}$ dans $M \otimes_A N$.

Lemme 2.8.7 On a

1. $(am + bm') \otimes n = a(m \otimes n) + b(m' \otimes n)$.
2. $m \otimes (an + bn') = a(m \otimes n) + b(m \otimes n')$.

Preuve. Exercice. ∎

Lemme 2.8.8 La famille $(m \otimes n)_{(m,n)\in M\times N}$ est une famille génératrice du A-module $M \otimes_A N$.

Preuve. C'est l'image de la base $(\varphi_{(m,n)})_{(m,n)\in M\times N}$. ∎

Soit $\pi : M\times N \to M\otimes_A N$ l'application définie par $\pi(m,n) = m\otimes n$.

Proposition 2.8.9 La paire $(M \otimes_A N, \pi)$ est un (le) produit tensoriel de M et N.

Preuve. Par le Lemme 2.8.7, l'application π est bilinéaire ce qui montre le premier point de la définition.

Soit maintenant $f : M \times N \to P$ une application bilinéaire. Nous montrons qu'il existe une application linéaire $L_f : M \otimes_A N \to P$ telle que $f = L_f \circ \pi$.

Commençons par définir une application linéaire $g : A^{(M\times N)} \to P$. Comme la famille $(\varphi_{(m,n)})_{(m,n)\in M\times N}$ est une base, il suffit de définir $g(\varphi_{(m,n)})$. On pose $g(\varphi_{(m,n)}) =$

$f(m,n)$. Montrons que $g|_L = 0$. Comme $(\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}, \varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')})$ est une famille génératrice de L, il suffit de montrer que

$$g(\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}) = g(\varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')}) = 0.$$

Mais g est linéaire et f bilinéaire donc

$$\begin{aligned} g(\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}) &= g(\varphi_{(am+bm',n)}) - ag(\varphi_{(m,n)}) - bg(\varphi_{(m',n)})) \\ &= f(am+bm',n) - af(m,n) - bf(m',n) \\ &= 0. \end{aligned}$$

De même, on montre que $g(\varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')}) = 0$.

On peut donc factoriser g par le quotient et on obtient un morphisme de A-modules $L_f : M \otimes_A N \to P$, tel que le diagramme suivant est commutatif :

$$\begin{array}{ccc} A^{(M\times N)} & \xrightarrow{\quad g \quad} & P \\ {\scriptstyle p}\downarrow & \nearrow_{L_f} & \\ A^{(M\times N)}/L = M \otimes_A N. & & \end{array}$$

Nous montrons que $L_f \circ \pi = f$, en effet on a

$$L_f \circ \pi(m,n) = L_f(m \otimes n) = L_f(p(\varphi_{(m,n)})) = g(\varphi_{(m,n)}) = f(m,n).$$

Comme $m \otimes n$ est génértrice, l'application L_f est déterminée par $L_f(m \otimes n) = f(m,n)$ et donc par f. Elle est unique. ∎

Définition 2.8.10 Soit $M_1, \cdots, M_n$ une famille de A-modules. Une application $f : M_1 \times \cdots \times M_n \to P$ s'appelle **n-linéaire** si pour tout $i \in [1,n]$ et tout $m_j \in M_j$ tel que $j \neq i$,l'application $f_i : M_i \to P$ définie par $f_i(m_i) = f(m_1, \cdots, m_n)$ est linéaire.

Définition 2.8.11 Un A-module E s'appelle **produit tensoriel** de $M_1, \cdots, M_n$ si les proposition suivantes sont vérifées :

1. Il existe une application n-linéaire $\pi_E : M_1 \times \cdots \times M_n \to P$ et
2. pour tout application n-linéaire $f : M_1 \times \cdots \times M_n \to P$, il existe un unique morphisme $L_f^E : E \to P$ tel que $L_f^E \circ \pi_E = f$.

Proposition 2.8.12 Soit $M_1, \cdots, M_n$ une famille de A-modules.

1. Soient E et F deux produits tensoriels de $M_1, \cdots, M_n$. Alors E et F sont isomorphes.

2. Il existe un produit tensoriel $(M_1 \otimes_A \cdots \otimes_A M_n, \pi)$ de $M_1, \cdots, M_n$.

Preuve. Exercice. ∎

Proposition 2.8.13 Soient M, N, P trois A-modules. Alors il existe des isomorphismes uniques

1. $M \otimes_A N \simeq N \otimes_A M$
2. $(M \otimes_A N) \otimes_A P \simeq M \otimes_A N \otimes_A P \simeq M \otimes_A (N \otimes_A P)$
3. $(M \oplus N) \otimes_A P \simeq (M \otimes_A P) \oplus (N \otimes_A P)$
4. $A \otimes_A M \simeq M$

tels que

1. $m \otimes n \mapsto n \otimes m$
2. $(m \otimes n) \otimes p \mapsto m \otimes n \otimes p \mapsto m \otimes (n \otimes p)$
3. $(m, n) \otimes p \mapsto (m \otimes p, n \otimes p)$
4. $a \otimes m \mapsto am$.

Preuve. Exercice. ∎

2.9. Suites exactes II

Proposition 2.9.1 Soient $f : M \to M'$ et $g : N \to N'$ des morphismes. Alors il existe un unique morphisme $f \otimes g : M \otimes_A N \to M' \otimes_A N'$ tel que $f \otimes g(m \otimes n) = f(m) \otimes g(n)$.

Preuve. Exercice. ∎

Proposition 2.9.2 Soit $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ une suite exacte et N un A-module. On a alors une suite exacte

$$M' \otimes_A N \xrightarrow{u \otimes \mathrm{Id}_N} M \otimes_A N \xrightarrow{v \otimes \mathrm{Id}_N} M'' \otimes_A N \to 0.$$

Preuve. Soit $\sum_i m_i'' \otimes n_i \in M'' \otimes_A N$, tel que $m_i'' \in M''$ et $n_i \in N$. Soit $m_i \in M$ tel que $v(m_i) = m_i''$. Alors on a $(v \otimes \mathrm{Id}_N)(\sum_i m_i \otimes n_i) = \sum_i v(m_i) \otimes n_i = \sum_i m_i'' \otimes n_i$ et donc $v \otimes \mathrm{Id}_N$ est surjective.

Soit $m' \otimes n \in M' \otimes_A N$, tel que $m' \in M'$ et $n \in N$. Alors on a $(u \otimes \mathrm{Id}_N)(m' \otimes n) = u(m') \otimes n$. On en déduit $(v \otimes \mathrm{Id}_N)(u \otimes \mathrm{Id}_N)(m' \otimes n) = v(u(m')) \otimes n = 0 \otimes n = 0$. Comme $m' \otimes n$ est génératrice de $M' \otimes_A N$, on en déduit que $\mathrm{Im}(u \otimes \mathrm{Id}_N) \subset \mathrm{Ker}(v \otimes \mathrm{Id}_N)$.

Soit $P = \mathrm{Im}(u \otimes \mathrm{Id}_N) \subset M \otimes_A N$. Comme $P \subset \mathrm{Ker}(v \otimes \mathrm{Id}_N)$ et comme $v \otimes \mathrm{Id}_N$ est surjective, il existe un morphisme surjectif $f : M \otimes_A N/P \to M'' \otimes_A N$ tel que $f([m \otimes n]) = v(m) \otimes n$.

Montrons que ce morphisme est un isomorphisme. Soit $G : M'' \times N \to M \otimes_A N/P$ défini par $G(m'', n) = [m \otimes n]$, où $m \in M$ est tel que $v(m) = m''$. Cette application

n'est *a priori* pas bien définie car elle dépend du choix de l'élément $m \in M$ tel que $v(m) = m''$. Soit $m_1 \in M$ un qutre élément tel que $v(m_1) = m'' = v(m)$. On a $v(m_1 - m) = 0$ donc $m_1 - m \in \mathrm{Ker}v = \mathrm{Im}u$. On en déduit $(m_1 - m) \otimes n \in P$ donc $[m_1 \otimes n] = [m \otimes n]$. L'application G est donc bien définie et on v{erifie (exercice) qu'elle est bilinéaire. On a donc un morhisme $g : M'' \otimes_A N \to M \otimes_A N/P$ tel que $g(m'' \otimes n) = [m \otimes n]$, où $m \in M$ est tel que $v(m) = m''$. Nous montrons que g et f sont inverses l'une de l'autre. On a $f(g(m'' \otimes n)) = f(m \otimes n) = v(m) \otimes n = m'' \otimes n$ et $g(f([m \otimes n])) = g(v(m) \otimes n) = [m \otimes n]$. ∎

Nous allons donner une seconde preuve plus conceptuelle de la proposition précédente en utilisant les catégories.

2.10. Catégories

Nous introduisons dans ce paragraphe le langage des catégories de manières informelles. Une **catégorie** est formé de ses **objets** et de ses **morphismes** qui doivent satisfaire un certain nombre d'axiomes. Plus précisément, une catégorie $\mathcal{C}$ a un "ensemble" $\mathrm{Obj}(\mathcal{C})$ d'objets (ce n'est pas nécessairement un ensemble en fait) et pour toute paire d'objets (A, B) un ensemble de morphismes de A vers B dans la catégories, noté $\mathrm{Hom}_{\mathcal{C}}(A, B)$. Les morphismes vérifient les trois conditions suivantes :

Composition Pour $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ et $g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, il existe un morphisme obtenu par "composition" $g \circ f \in \mathrm{Hom}_{\mathcal{C}}(A, C)$

Identité Pour tout objet A, il existe un morphisme $\mathrm{Id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ tel que $f \circ \mathrm{Id}_A = f$ et $\mathrm{Id}_A \circ g = g$ pour tout f et g composables.

Associativité La composition est associative c'est-à-dire $(f \circ g) \circ h = f \circ (g \circ h)$.

Un morphisme $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ dans la catégorie $\mathcal{C}$ est appelé **isomorphisme** s'il existe $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ tel que $g \circ f = \mathrm{Id}_A$ et $f \circ g = \mathrm{Id}_B$.

Exemple Voici quelques catégories bien connues (k un corps et A un anneau) :

Categorie	Objets	Morphismes
des ensembles	ensembles	applications
des groupes	groupes	morphismes de groupes
des anneaux	anneaux	morphismes d'anneaux
des corps	corps	morphismes de corps
des k-espaces vectoriels	k-espaces vectoriels	applications k-linéaires
des A-modules	A-modules	applications A-linéaires
des espaces topologiques	ensembles munis d'une topologie	applications continues

Les **foncteurs** sont les "morphismes" entre catégories. Plus précisément, un foncteur $F : C \to D$ de la catégorie C vers la catégorie D est la donnée d'une "correspondance"

$$F_{\mathrm{Obj}} : \mathrm{Obj}(C) \to \mathrm{Obj}(D)$$

et pour chaque couple d'objets A, A' de C d'une application

$F_{\mathrm{Mor}} : \mathrm{Mor}_C(A, A') \to \mathrm{Mor}_D(F_{\mathrm{Obj}}(A), F_{\mathrm{Obj}}(A'))$ cas d'un foncteur covariant ou
$F_{\mathrm{Mor}} : \mathrm{Mor}_C(A, A') \to \mathrm{Mor}_D(F_{\mathrm{Obj}}(A'), F_{\mathrm{Obj}}(A))$ cas d'un foncteur contravariant

qui vérifie les conditions suivantes :

$$F_{\mathrm{Mor}}(\mathrm{Id}_A) = \mathrm{Id}_{F_{\mathrm{Obj}}(A)} \text{ pour tout } A \text{ objet de } C$$

Pour $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ et $g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ on a

$$\begin{array}{ll} F_{\mathrm{Mor}}(g \circ f) = F_{\mathrm{Mor}}(g) \circ F_{\mathrm{Mor}}(f) & \text{pour un foncteur covariant ou} \\ F_{\mathrm{Mor}}(g \circ f) = F_{\mathrm{Mor}}(f) \circ F_{\mathrm{Mor}}(g) & \text{pour un foncteur contravariant.} \end{array}$$

Par exemple, pour un A-module N, on a le foncteur suivant de la catégorie A-**mod** des A-modules dans elle même : $\mathrm{Hom}_A(N, -) : A\text{-}\mathbf{mod} \to A\text{-}\mathbf{mod}$ défini par $\mathrm{Hom}_A(N, -)(M) = \mathrm{Hom}_A(N, M)$. On a vu que c'est un foncteur covariant. On a aussi le foncteur $\mathrm{Hom}_A(-, N) : A\text{-}\mathbf{mod} \to A\text{-}\mathbf{mod}$ défini par $\mathrm{Hom}_A(-, N)(M) = \mathrm{Hom}_A(M, N)$. C'est un foncteur contravariant.

Définition 2.10.2 Soit A un anneau.

1. **Un foncteur covariant F de la catégorie des A-modules** associe à chaque objet (A-module) M l'objet (A-module) $F(M)$ de telle sorte que
   a. pour $f \in \mathrm{Hom}(M, N)$, il existe un $F(f) \in \mathrm{Hom}(F(M), F(N))$,
   b. pour tout $f : M \to N$ et tout $g : N \to P$, on a $F(g) \circ F(f) = F(g \circ f)$ et
   c. on a $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$ pour tout objet M.
2. **Un foncteur contravariant dela catégorie des A-modules** associe à chaque objet (A-module) M l'objet (A-module) $F(M)$ de telle sorte que
   a. pour $f \in \mathrm{Hom}(M, N)$, il existe un $F(f) \in \mathrm{Hom}(F(N), F(M))$,
   b. pour tout $f : M \to N$ et tout $g : N \to P$, on a $F(f) \circ F(g) = F(g \circ f)$ et
   c. on a $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$ pour tout objet M.

Définition 2.10.3 1. Soit F un morphisme covariant. Le foncteur F est dit **exact à gauche** si la chaine suivante

$$0 \to F(M') \to F(M) \to F(M'')$$

et exacte pour toute suite exacte $0 \to M' \to M \to M''$.

2. Soit F un foncteur covariant. Le foncteur F est dit **exact à droite** si la chaine

$$F(M') \to F(M) \to F(M'') \to 0$$

est exacte pour toute suite exacte $M' \to M \to M'' \to 0$.

3. Soit F un foncteur contravarianrt. Le foncteur F est dit **exact à gauche** si la chaine

$$0 \to F(M'') \to F(M) \to F(M')$$

est exacte pour tout suite exacte $M' \to M \to M'' \to 0$.

4. Soit F un foncteur contravariant. Le foncteur F est dit **exact à droite** si la chaine

$$F(M') \to F(M) \to F(M'') \to 0$$

est exacte pour toute suite exacte $0 \to M' \to M \to M''$.

Exemple Soit A un anneau et N un A-Modul.

1. Le foncteur $M \mapsto \mathrm{Hom}(N, M)$ est covariant exact à gauche. On note ce foncteur $\mathrm{Hom}(N, -)$

2. Le foncteur $M \mapsto \mathrm{Hom}(M, N)$ est contravariant exact à gauche. On note ce foncteur $\mathrm{Hom}(-, N)$

3. Le foncteur $M \mapsto M \otimes_A N$ est covariant exact à droite. On note ce foncteur $- \otimes_A N$

Définition 2.10.5 1. Une paire (F, G) de foncteur covariants est dite **paire de foncteurs adjoints** s'il existe des isomorphismes

$$\Psi_{M,N} : \mathrm{Hom}(M, G(N)) \simeq \mathrm{Hom}(F(M), N)$$

tels que pour tout morphismes $f : M \to M'$ et $g : N \to N'$, les diagrammes suivants sont commutatifs :

$$\begin{array}{ccc} \mathrm{Hom}(M', G(N)) & \xrightarrow{\bar{f}} & \mathrm{Hom}(M, G(N)) \\ {\scriptstyle \Psi_{M',N}}\downarrow & & \downarrow{\scriptstyle \Psi_{M,N}} \\ \mathrm{Hom}(F(M'), N) & \xrightarrow{\overline{F(f)}} & \mathrm{Hom}(F(M), N) \end{array} \qquad \begin{array}{ccc} \mathrm{Hom}(M, G(N)) & \xrightarrow{\overline{G(g)}} & \mathrm{Hom}(M, G(N')) \\ {\scriptstyle \Psi_{M,N}}\downarrow & & \downarrow{\scriptstyle \Psi_{M,N'}} \\ \mathrm{Hom}(F(M), N) & \xrightarrow{\bar{g}} & \mathrm{Hom}(F(M), N'). \end{array}$$

Le foncteur F s'appelle **adjoint à gauche** de G et le foncteur G s'appelle **adjoint à droite** de F.

2. De même, on peut définir des paires de foncteur adjoints contravariants. Funktoren.

Proposition 2.10.6 Les foncteurs $(- \otimes_A N, \mathrm{Hom}(N, -))$ forment une paire de foncteurs adjoints.

Preuve. Soit $F(M) = M \otimes_A M$ et $G(P) = \mathrm{Hom}(N, P)$. Nous montrons tout d'abord l'isomorphisme $\mathrm{Hom}(F(M), P) \simeq \mathrm{Hom}(M, G(P))$ c'est-à-dire qu'il existe un isomorphisme

$$\Phi_{M,P} : \mathrm{Hom}(M \otimes_A N, P) \simeq \mathrm{Hom}(M, \mathrm{Hom}(N, P)).$$

Soit $\varphi : M \otimes_A N \to P$. Alors on a une application bilinéaire $\varphi' : M \times N \to P$ définie par $\varphi'(m, n) = \varphi(m \otimes n)$. Nous définissons $\Phi_{M,P}(\varphi) : M \to \mathrm{Hom}(N, P)$ comme suit : $\Phi_{M,P}(\varphi)(m) : N \to P$ est l'application $\Phi_{M,P}(\varphi)(m)(n) = \varphi'(m, n) = \varphi(m \otimes n)$. On vérifie (exercice) que les applications $\Phi_{M,P}(\varphi)(m)$, $\Phi_{M,P}(\varphi)$ et $\Phi_{M,N}$ sont linéaires (l'application $(\varphi, m, n) \mapsto \varphi'(m, n) = \varphi(m \otimes n)$ est trilinéaire).

Soit $\psi : M \to \mathrm{Hom}(N, P)$. L'application $M \times N \to P$, $(m, n) \mapsto \psi(m)(n)$ est bilinéaire. Il existe donc une unique application linéaire $\Psi_{M,P}(\psi) : M \otimes_A N \to P$ telle que $\Psi_{M,P}(\psi)(m \otimes n) = \psi(m)(n)$.

Nous montrons que $\Psi_{M,P}$ et $\Phi_{M,P}$ sont inverses l'une de l'autre. On a $\Phi_{M,P}(\Psi_{M,P}(\psi))(m)(n) = \Psi_{M,P}(\psi)(m \otimes n) = \psi(m)(n)$. Par ailleurs, on a $\Psi_{M,P}(\Phi_{M,P}(\varphi))(m \otimes n) = \Phi_{M,P}(\varphi)(m)(n) = \varphi(m \otimes n)$.

Nous vérifions maintenant que les diagrammes de la définition ci-dessous sont commutatifs. Soit $f : M \to M'$, on a $(\Psi_{M',P} \circ \bar{f})(\psi)(m \otimes n) = \psi(f(m))(n)$. On a aussi $(\overline{F(f)} \circ \Psi_{M,P})(\psi)(m \otimes n) = \psi(f(m))(n)$. De manière analogue, on montre que le second diagramme est également commutatif. ∎

Lemme 2.10.7 Soit A un anneau.

1. Une chaine de morphismes $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ est une suite est exacte si et seulement si pour tout A-module N, la chaine suivante est une suite exacte : $0 \to \mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M) \xrightarrow{\bar{v}} \mathrm{Hom}(N, M'')$.

2. Une chaine de morphismes $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ est une suite exacte si et seulement si pour tout Amodule N, la chaine suivante est une suite exacte : $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$.

Preuve. Nous savons déjà que si $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ (resp. $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$) est une suite exacte, alors $0 \to \mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M) \xrightarrow{\bar{v}} \mathrm{Hom}(N, M'')$ (bzw. $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$) est aussi une suite exacte pour tout N.

1. Soit $N = A$. Alors on a $\mathrm{Hom}(N, M) = \mathrm{Hom}(A, M) \simeq M$ avec $f \mapsto f(1)$ et $m \mapsto (a \mapsto am)$. Modulo ces isomorphismes, l'application $\mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M)$ est exactement l'application $u : M' \to M$. Ce résultat en découle.

2. Soit $N = M''/\mathrm{Im}v$ et $\pi \in \mathrm{Hom}(M'', N)$ la projection canonique. L'application $\bar{v}(\pi) : M \to N = M''/\mathrm{Im}v$ est donnée par $\bar{v}(\pi)(m) = \pi(v(m)) = 0$, car $\mathrm{Im}v = \mathrm{Ker}\pi$. On a donc $\bar{v}(\pi) = 0$ et comme $\bar{v}$ est injective, on a $\pi = 0$. En particulier, on a $M''/\mathrm{Im}v = 0$ et $\mathrm{Im}v = M''$. L'application v est surjective.

Soient $N = M''$ et $\mathrm{Id}_{M''} \in \mathrm{Hom}(M'', N)$. On a $v \circ u = \mathrm{Id}_{M''} \circ v \circ u = \bar{v} \circ \bar{u}(\mathrm{Id}_{M''}) = 0$. On en déduit $\mathrm{Im}u \subset \mathrm{Ker}v$.

Soit $N = M/\mathrm{Im}u$ et $\pi \in \mathrm{Hom}(M, N)$ la projection canonique. On a $\bar{u}(\pi)(m') = \pi \circ u(m') = \pi(u(m')) = 0$, car $\mathrm{Im}u = \mathrm{Ker}\pi$. On a donc $\bar{u}(\pi) = 0$ et $\pi \in \mathrm{Ker}\bar{u} = \mathrm{Im}\bar{v}$. On a donc un $f \in \mathrm{Hom}(M'', N)$ tel que $\pi = \bar{v}(f) = f \circ v$. Soit maintenant $m \in \mathrm{Ker}v$. On a $\pi(m) = f \circ v(m) = 0$ et donc $m \in \mathrm{Im}u$. ∎

Proposition 2.10.8 Soit (F, G) une paire de foncteurs adjoints covariants (resp. contravariants). Alors on a l'équivalence

$$F \text{ est exact à droite } \Leftrightarrow G \text{ est exact à gauche.}$$

Preuve. ($\Rightarrow$) Soit $0 \to N' \to N \to N''$ une suite exacte et soit M un module. Alors on a une suite exacte $0 \to \mathrm{Hom}(F(M), N') \to \mathrm{Hom}(F(M), N) \to \mathrm{Hom}(F(M), N'')$. On en déduit la suite exacte $0 \to \mathrm{Hom}(M, G(N')) \to \mathrm{Hom}(M, G(N)) \to \mathrm{Hom}(M, G(N'))$. Ceci étant vrai pour tout M, le lemme précédent nous dit que la suite $0 \to G(N') \to G(N) \to G(N'')$ est exacte et G est exact à gauche.

($\Rightarrow$) Soit $M' \to M \to M'' \to 0$ une suite exacte et N un module. Alors on a une suite exacte $0 \to \mathrm{Hom}(M'', G(N)) \to \mathrm{Hom}(M, G(N)) \to \mathrm{Hom}(M', G(N))$. On en déduit la suite exacte $0 \to \mathrm{Hom}(F(M''), N) \to \mathrm{Hom}(F(M), N) \to \mathrm{Hom}(F(M'), N)$. Ceci étant vrai pour tout N, le lemme précédent nous dit que la suite $F(M') \to F(M) \to F(M'') \to 0$ est exacte et F est exact à droite.

La preuve pour des foncteurs contravariants est semblable. ∎

Corollaire Le foncteur $- \otimes_A N$ est exact à droite.

Preuve. C'est un adjoint à gauche du foncteur $\mathrm{Hom}(N, -)$ qui est exact à gauche. ∎

Définition 2.10.10 Un foncteur est appelé **exact** s'il est exact à gauche et à droite.

Définition 2.10.11 Un A-module M est dit **plat** si le foncteur $- \otimes_A M$ est exact.

Proposition 2.10.12 Soit N un A-module. Les assertions suivantes sont équivalentes :

1. N est plat ;
2. pour tout suite exacte $0 \to M' \to M \to M'' \to 0$ la suite $0 \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0$ exacte.
3. Si $f : M' \to M$ est injective, alors $f \otimes \mathrm{Id}_N : M' \otimes_A N \to M \otimes_A N$ est injective.

Preuve. (1. $\Leftrightarrow$ 2.) C'est la définition de la platitude.

(2. $\Leftrightarrow$ 3.) C'est le fait que le produit tensoriel est exact à droite. ∎

2.11. Restriction et extension des scalaires

Remarque Soit $f : A \to B$ un morphisme d'anneaux et N un B-module.

1. Alors B est un A-module pour la multiplication scalaire $a \cdot b = f(a)b$.

2. Plus généralement, N est un A-module pour la multiplication scalaire $a \cdot n = f(a)n$.

Définition 2.11.2 Soit $f : A \to B$ un morphisme d'anneaux et N un B-module. La structure de A-module définie sur N par $a \cdot n = f(a)n$ s'appelle **structure de A-module obtenue par restriction des scalaires**.

Exemple 2.11.3 Un $\mathbb{C}$-espace vectoriel est aussi un $\mathbb{R}$-espace vectoriel par restriction des scalaires.

Proposition 2.11.4 Soit $f : A \to B$ un morphisme d'anneaux et N un B-module. Si N est de type fini comme B-module et si B est de type fini comme A-module, alors N est de type fini comme A-module.

Preuve. Soit $n_1, \cdots, n_k$ une famille génératrice de N comme B-module et soit $b_1, \cdots, b_r$ une famille génératrice de B comme A-module. Soit $n \in N$. Alors il existe des scalaires $\lambda_1, \cdots, \lambda_k \in B$ tels que $n = \sum_i \lambda_i n_i$. Pour tout $i \in [1, k]$, il existe des scalaires $(a_{i,j})_{j\in[1,r]}$ tels que $\lambda_i = \sum_j a_{i,j} b_j$. On a alors

$$n = \sum_{i=1}^{k} \sum_{j=1}^{r} a_{i,j} b_j n_i$$

et la famille $(b_j n_i)_{i\in[1,k],j\in[1,r]}$ est une famille génératrice de N comme A-module. ∎

Remarque Lorsque $A = K$, $B = L$ et $N = M$ sont des corps avec $K \subset L \subset M$ des extensions finies, on restrouve le théorème de la base télescopique (voir le cours de théorie de Galois).

Lemme 2.11.6 Soit $f : A \to B$ un morphisme d'anneaux et soit M un A-module. Alors $B \otimes_A M$ est un B-module pour la multiplication scalaire $b(b' \otimes m) = bb' \otimes m$.

Preuve. Exercice. ∎

Définition 2.11.7 Soit $f : A \to B$ un morphisme d'anneaux et soit M un A-module. La structure de B-module définie sur $B \otimes_A M$ par $b \cdot (b' \otimes m) = bb' \otimes m$ s'appelle **structure de B-module obtenue par extension des scalaires**.

Exemple 2.11.8 Soit l'espace vectoriel $\mathbb{R}^n$. Alors $\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C}$ est isomorphe à l'espace vectoriel $\mathbb{C}^n$. C'est l'opération usuelle de complexification souvent utilisé pour les endomorphismes des espaces vectoriels réels.

Proposition 2.11.9 Soit $f : A \to B$ un morpihsme d'anneaux et soit M un A-module de type fini. Alors $B \otimes_A M$ est un B-module de type fini.

Preuve. Soit $m_1, \cdots, m_n$ une famille génératrice de M comme A-module. Soit $b \otimes m \in B \otimes_A M$. Il existe alors des éléments $a_1, \cdots, a_n \in A$ tels que $m = \sum_i a_i m_i$. On a donc $\sum_i f(a_i)b(1 \otimes m_i) = \sum_i b \otimes a_i m_i = b \otimes m$ et la famille $(1 \otimes m_i)_{i \in [1,n]}$ est génératrice de $B \otimes_A M$ comme B-module. ∎

2.12. Algèbres

Définition 2.12.1 Soit A un anneau.

1. **Une A-algèbre** B est un anneau B muni d'un morphisme d'anneaux $f : A \to B$.

2. Soient $f : A \to B$ et $g : A \to C$ deux A-algèbres. **Un morphisme de A-algèbres** de B vers C est un morphisme d'anneaux $\varphi : B \to C$ tel que φ est A-linéaire.

Remarque Une A-algèbre B est un A-module pour la multiplication scalaire $a \cdot b = f(a)b$. De plus on a les règles de calcul usuelles suivantes :

1. $a(b + b') = ab + ab'$
2. $(a + a')b = ab + a'b$
3. $(aa')b = a(a'b)$
4. $a(bb') = (ab)b' = b(ab')$
5. $a1 = a$ et $1b = b$.

Lemme 2.12.3 Soient $f : A \to B$ et $g : A \to C$ deux A-algèbres.

1. Alors $B \otimes_A C$ est une A-algèbre pour la multiplication $(b \otimes c)(b' \otimes c') = bb' \otimes cc'$ et l'application $A \to B \otimes_A C$, $a \mapsto f(a) \otimes g(a)$.

2. Les applications $B \to B \otimes_A C$, $b \mapsto b \otimes 1$ et $C \to B \otimes_A C$, $c \mapsto 1 \otimes c$ sont des morphismes d'anneaux.

Preuve. 1. L'application $B \times C \times B \times C \to B \otimes_A C$ définie par $(b, c, b', c') \mapsto bb' \otimes cc'$ est 4-linéaire. Il existe donc une application linéaire $B \otimes_A C \otimes_A B \otimes_A C \to B \otimes C$ définie par $b \otimes c \otimes b' \otimes c' \mapsto bb' \otimes cc'$. On en déduit que l'application $B \otimes_A C \times B \otimes_A C \to B \otimes_A C$ définie par $(b \otimes c, b' \otimes c') \mapsto bb' \otimes cc'$ est bilinéaire. On vérifie qu'elle est associative et que l'on a $(b \otimes c)(1 \otimes 1) = (1 \otimes 1)(b \otimes c) = b \otimes c$, et donc $B \otimes_A C$ est un anneau. L'application $A \to B \otimes_A C$ définie par $a \mapsto f(a) \otimes g(a)$ est un morphisme d'anneau et donc $B \otimes_A C$ est une A-algèbre.

2. Exercice. ∎

Remarque Le morphisme d'anneaux $B \to B \otimes_A C$, $b \mapsto b \otimes 1$ n'est pas toujours un morphisme de A-algèbres.

Par exemple, soient $A = B = C = \mathsf{k}$, avec k un corps. Soient $f = g = \mathrm{Id}_{\mathsf{k}}$. L'application $\varphi : B \to B \otimes_A C$ est donnée par $x \mapsto x \otimes 1 = x(1 \otimes 1)$. L'application $f \otimes g : A \to B \otimes_A C$ est donnée par $(f \otimes g)(x) = x \otimes x = x(1 \otimes x) = x^2(1 \otimes 1)$. On a donc $\varphi(f(x)y) = \varphi(xy) = xy(1 \otimes 1)$ et $(f \otimes g)(x) \cdot \varphi(y) = (x \otimes x)(y \otimes 1) = xy \otimes x = x^2y(1 \otimes 1) \neq xy(1 \otimes 1) = \varphi(f(x)y)$.

Exemple Soit B un anneau et $A = \mathbb{Z}$. Alors l'application $f : A \to B$ définie par

$$f(n) = nb = \underbrace{1 + \cdots + 1}_{n-\text{fois}}$$

est un morphisme d'anneaux et tout anneau est donc aussi une $\mathbb{Z}$-algèbre.

Définition 2.12.6 Soit A un anneau.

1. Un morpihsme d'anneaux $f : A \to B$ est dit **fini** si B est un A-module de type fini. On dit alors que B est une **algèbre finie sur** A.

2. Un morphisme d'anneaux $f : A \to B$ est dit **de type fini** s'il existe des éléments $x_1, \cdots, x_r \in B$ tels que tout élément de B peut s'exprimer comme polynôme à coefficients dans $f(A)$ en les $x_1, \cdots, x_r$. On dit alors que B est une **algèbre de type fini ou finiment engendrée sur** A.

3. L'anneau A est dit **finiment engendré**, si A est une $\mathbb{Z}$-algèbre de type fini.

Remarque Une A-algèbre B est de type fini si et seulement s'il existe un morphisme d'nnaeaux surjectif $A[T_1, \cdots, T_r] \to B$.

3. Localisation

Dans ce chapitre, on généralise la construction du corps des fractions.

3.1. Anneaux

Définition 3.1.1 Soit A un anneau. Un sous-ensemble $S \subset A$ est dit **multiplicatif** si $1 \in S$ et si on a : $(x, y \in S \Rightarrow xy \in S)$.

Exemple 1. Soit A un anneau, allors $S = A$ est multiplicatif.

2. Soit A un anneau, alors $S = A^\times$ est multiplicatif.

3. Soit A un anneau, alors $S = A \setminus \{\text{Nullteiler}\}$ est multiplicatif.

4. Soit A un anneau et $\mathfrak{p}$ un idéal premier, alors $S = A \setminus \mathfrak{p}$ est multiplicatif.

5. Soit A un anneau, alors $S = \{f^n \mid n \geq 0\}$ est multiplicatif.

6. Soit A un anneau et $\mathfrak{a}$ un idéal, alors $S = 1 + \mathfrak{a} = \{1 + x \in A \mid x \in \mathfrak{a}\}$ est multiplicatif.

6. Soit A un anneau intègre, alors $S = A \setminus \{0\}$ est multiplicatif.

Définition 3.1.3 Soit A un anneau et $S \subset A$ un sous-ensemble multiplicatif. On définit une relation d'équivalence $\equiv$ sur le produit $A \times S$ par

$$(a, s) \equiv (a', s') \Leftrightarrow \exists t \in S,\ t(as' - a's) = 0.$$

Lemme 3.1.4 La relation $\equiv$ est une relation d'équivalence.

Preuve. Exercice. ∎

Définition 3.1.5 On écrit a/s ou encore $\frac{a}{s}$ pour la classe d'équivalence de (a, s) pour la relation $\equiv$. On note $S^{-1}A$ l'ensemble des classes d'équivalence.

Exemple Soit $A = \mathbb{Z}$ et $S = \mathbb{Z} \setminus \{0\}$. Alors $S^{-1}A = \mathbb{Q}$.

Proposition 3.1.7 Soit A un anneau et $S \subset A$ un sous-ensemble multiplicatif.

1. Alors $S^{-1}A$ est muni d'une structure d'anneau pour les opérations suivantes avec $0 = 0/1$ et $1 = 1/1$:

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \text{ et } \frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}.$$

2. On a $s/1 \in (S^{-1}A)^\times$.

3. L'application $\lambda : A \to S^{-1}A$, $a \mapsto a/1$ est un morphisme d'anneaux.

Preuve. 1. On vérifie (exercice) que les opérations sont bien définies et on vérifie (calcul d'école) qu'elles définissent une structure d'anneaux.

2. On a $(s/1)(1/s) = 1/1$.

3. On a $\lambda(1) = 1/1$, $\lambda(a+b) = (a+b)/1 = a/1 + b/1 = \lambda(a) + \lambda(b)$ et $\lambda(ab) = ab/1 = (a/1)(b/1)$. ∎

Remarque Le morphisme $A \to S^{-1}A$ n'est pas nécessairement injectif. Par exemple, si $0 \in S$, on a $0(a \cdot 1 - s \cdot 0) = 0$ et donc $a/s \equiv 0/1$. On a donc

$$\frac{a}{s} = \frac{0}{1} \text{ pour tout } \frac{a}{s} \in S^{-1}A \text{ et donc } S^{-1}A = 0.$$

L'application $\lambda : A \to S^{-1}A$ est l'application nulle.

L'anneau $S^{-1}A$ peut également être défini via une propriété universelle.

Proposition 3.1.9 Soit $f : A \to B$ un morphisme d'anneaux tel que $f(s) \in B^\times$ pour tout $s \in S$. Alors il existe un unique morphisme d'anneaux $g : S^{-1}A \to B$ tel que $f = g \circ \lambda$.

Preuve. On définit $g : S^{-1}A \to B$ par $g(a/s) = f(a)f(s)^{-1}$. On vérifie que cette définition ne dépend pas du choix du représentant. Soit donc $a'/s' \in S^{-1}A$ tel que $a'/s' = a/s$. Il existe alors un $t \in S$ tel que $t(as' - a's) = 0$. On en déduit $f(t)(f(a)f(s') - f(a')f(s)) = 0$. Comme $f(t)$ est inversible, on a $f(a)f(s') - f(a')f(s) = 0$ et donc $f(a)f(s)^{-1} = f(a')f(s')^{-1}$. L'application g est bien définie et on vérifie (exercice) que c'est un morphisme d'anneaux.

Montron que $f = g \circ \lambda$. Soit $a/s \in S^{-1}A$. On a $g(\lambda(a)) = g(a/1) = f(a)f(1)^{-1} = f(a)$.

Montrons maintenant l'unicité de g. Soit $h : S^{-1}A \to B$ un autre morphisme d'anneaux tel que $f = h \circ \lambda$. On a $h(a/s) = h(a/1)h(1/s) = h(a/1)h((s/1)^{-1}) = h(a/1)h(s/1)^{-1}$. On a donc $h(a/s) = h(\lambda(a))h(\lambda(s))^{-1} = f(a)f(s)^{-1} = g(a/s)$. ∎

Lemme 3.1.10 Soit $S \subset A$ un sous-ensemble multiplcatif.

1. Pour $s \in S$, on a $\lambda(s) \in S^{-1}A^{\times}$.

2. Soit $a \in A$. On a ($\lambda(a) = 0 \Leftrightarrow$ il existe $s \in S$ tel que $sa = 0$).

3. Tout élément de $S^{-1}A$ est de la forme $\lambda(a)\lambda(s)^{-1}$, où $a \in A$ et $s \in S$.

Preuve. 1. On a $\lambda(s) = s/1 \in S^{-1}A^{\times}$.

2. On a $\lambda(a) = 0 \Leftrightarrow a/1 = 0 \Leftrightarrow$ (il existe $s \in S$ tel que $sa = s(a-0) = 0$).

3. On a $a/s = \lambda(a)\lambda(s)^{-1}$. ∎

Ces propriétés caractérisent le morphisme $\lambda : A \to S^{-1}A$.

Proposition 3.1.11 Soit $f : A \to B$ un morphisme d'anneaux tel que

1. pour $s \in S$, on a $f(s) \in B^{\times}$;
2. pour $a \in A$, on a ($\lambda(a) = 0 \Rightarrow$ il existe $s \in S$ tel que $sa = 0$) ;
3. tout élément de B est de la forme $f(a)f(s)^{-1}$, avec $a \in A$ et $s \in S$.

Alors il exise un isomorphisme $g : S^{-1}A \to B$ tel que $f = g \circ \lambda$.

Preuve. On pose $g(a/s) = f(a)f(s)^{-1}$. Par la Proposition 3.1.9 ceci est bien défini, c'est un morphisme d'anneaux et on a $f = g \circ \lambda$. Montrons que g est un isomorphisme.

Soit $a/s \in \mathrm{Ker}g$. On a $g(a/s) = f(a)f(s)^{-1} = 0$ et comme $f(s)$ est inversible, on a $f(a) = 0$. On a donc un élément $t \in S$ tel que $ta = 0$ et donc $t(a \cdot 1 - s \cdot 0) = 0$. On en déduit $a/s = 0$ et g est injective.

Soit $b \in B$. Il existe $a \in A$ et $s \in S$ tels que $b = f(a)f(s)^{-1}$. On a donc $b = g(a/1)g(s/1)^{-1} = g(a/1)g(1/s) = g(a/s)$ et g est surjective. ∎

Exemple 1. On a : $S^{-1}A = 0 \Leftrightarrow 0 \in S \Leftrightarrow S$ contient des éléments nilpotents.

2. Soit A un anneau intègre et soit $S = A \setminus \{0\}$. Alors $S^{-1}A = \mathrm{Frac}(A)$ est le corps des fractions de A.

3. Soit $S = A \setminus \mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier, alors on note $S^{-1}A = A_{\mathfrak{p}}$.

4. Soit $A = \mathbb{Z}$ et $\mathfrak{p} = (p)$, avec p un nombre premier. Alors on a

$$A_{\mathfrak{p}} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ avec } \mathrm{pgcd}(b, p) = 1 \right\}.$$

5. Soit $f \in A$ et $S = \{f^n \mid n \geq 0\}$. On note $S^{-1}A = A[f^{-1}]$.

6. Soit $A = \mathbb{Z}$ et $f = p$, avec p un nombre premier. Alors on a

$$A[p^{-1}] = \left\{ \frac{a}{p^n} \in \mathbb{Q} \mid a \in \mathbb{Z},\ n \geq 0 \right\}.$$

3.2. Modules

Définition 3.2.1 Soit A un anneau, soit $S \subset A$ un sous-ensemble multiplicatif et M un A-module. On définit la relation d'équivalence $\equiv$ sur $M \times S$ par

$$(m, s) \equiv (m', s') \Leftrightarrow \exists t \in S,\ t(s'm - sm') = 0.$$

Lemme 3.2.2 La relation $\equiv$ est une relation d'équivalence.

Preuve. Exercice. ∎

Définition 3.2.3 On écrit m/s ou encore $\frac{m}{s}$ pour la classe d'équivalence de (m, s) pour la relation $\equiv$. On note $S^{-1}M$ l'ensemble des classes d'équivalence.

Lemme 3.2.4 L'ensemble $S^{-1}M$ est un $S^{-1}A$-module pour l'addition et la multiplication scalaire définies par

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \text{ et } \frac{a}{s}\frac{m}{t} = \frac{am}{st}.$$

En particulier $S^{-1}M$ est un A-module pour la multiplication scalaire $a\dfrac{m}{s} = \dfrac{am}{s}$.

Preuve. Exercice. ∎

Exemple 1. Si $S = A \setminus \mathfrak{p}$ avec $\mathfrak{p}$ un idéal premier, on note $S^{-1}M = M_{\mathfrak{p}}$.

2. Si $S = \{f^n \mid n \geq 0\}$, avec $f \in A$, on note $S^{-1}M = M_f$.

Remarque On a ($m/s = 0 \Leftrightarrow$ il existe un $t \in S$ tel que $tm = 0$).

Lemme 3.2.7 La correspondance $M \mapsto S^{-1}M$ est un foncteur : pour tout morphisme de A-modules $f : M \to N$, il existe un morphisme de $S^{-1}A$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ défini par

$$S^{-1}f\left(\frac{m}{s}\right) = \frac{f(m)}{s}.$$

Preuve. On vérifie que c'est bien défini. Soit $m'/s' = m/s$. Il existe un $t \in S$ tel que $t(ms' - m's) = 0$. On a donc $0 = f(t(s'm - sm')) = t(s'f(m) - sf(m'))$ et donc

$$\frac{f(m)}{s} = \frac{f(m')}{s'}.$$

On vérifie (exercice) que f est un morphisme de modules. ∎

Définition 3.2.8 Le foncteur $M \mapsto S^{-1}M$ s'appelle **foncteur de localisation**.

Proposition 3.2.9 Le foncteur de localisation est exact.

Preuve. Soit $M' \xrightarrow{u} M \xrightarrow{v} M''$ une suite exacte. Alors il existe une chaine $S^{-1}M' \xrightarrow{S^{-1}u} S^{-1}M \xrightarrow{S^{-1}v} S^{-1}M''$, où $S^{-1}u(m'/s) = u(m)/s$ et $v(m/s) = v(m)/s$ pour $m' \in M'$, $m \in M$ et $s \in S$. On en déduit $S^{-1}v(S^{-1}u(m'/s)) = S^{-1}v(u(m')/s) = v(u(m'))/s = 0/s = 0$ et donc $\mathrm{Im}S^{-1}u \subset \mathrm{Ker}S^{-1}v$.

Soit $m/s \in \mathrm{Ker}S^{-1}v$. On a $v(m)/s = 0$ et donc il existe un $t \in S$ tel que $tv(m) = 0$. On a donc $v(tm) = 0$ et $tm \in \mathrm{Ker}v = \mathrm{Im}u$. Soit donc $m' \in M'$ tel que $u(m') = tm$. On a $u(m'/ts) = u(m')/ts = tm/ts = m/s$ et donc $m/s \in \mathrm{Im}u$. ∎

Corollaire Soit $N \subset M$ un sous-module. Alors $S^{-1}N \to S^{-1}M$ est injective et on peut voir $S^{-1}N$ comme un sous-module de $S^{-1}M$:

$$S^{-1}N = \left\{ \frac{n}{s} \mid n \in N \text{ et } s \in S \right\} \subset S^{-1}M = \left\{ \frac{m}{s} \mid m \in M \text{ et } s \in S \right\}.$$

Corollaire Soient $N, P \subset M$ des sous-modules. Alors on a

1. $S^{-1}(N + P) = S^{-1}N + S^{-1}P$;

2. $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$;

3. $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ comme $S^{-1}A$-modules.

Preuve. 1. Exercice.

2. Si $x \in S^{-1}N \cap S^{-1}P$, alors on a $x = /s = p/s'$, où $n \in N$, $p \in P$ et $s, s' \in S$. On en déduit qu'il existe $t \in S$ tel que $t(s'n - sp) = 0$. On a donc $N \ni ts'n = tsp \in P$ et $ts'x = tsx \in N \cap P$ puis $x = tsx/ts \in S^{-1}(N \cap P)$. L'inclusion inverse est claire.

3. La suite $0 \to N \to M \to M/N \to 0$ est exacte et donc la suite $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$ est exacte. Le résultat en découle. ∎

Proposition 3.2.12 On a un isomorphisme $S^{-1}M \simeq M \otimes_A S^{-1}A$ de $S^{-1}A$-modules. Les isomorphismes sont donnés par $m/s \mapsto m \otimes 1/s$ et $m \otimes a/s \mapsto am/s$.

Preuve. L'application $M \times S^{-1}A \to S^{-1}M$ définie par $(m, a/s) \mapsto am/s$ est A-bilinéaire. L'application $M \otimes_A S^{-1}A \to S^{-1}M$, $m \otimes a/s \mapsto am/s$ est donc bien définie. On vérifie qu'elle est $S^{-1}A$-linéaire.

L'application $m/s \mapsto m \otimes 1/s$ est bien définie : si $m'/s' = m/s$, il existe $t \in S$ mit $t(s'm - sm') = 0$. On a alors $m' \otimes 1/s' = m' \otimes ts/s'ts = tsm' \otimes 1/s'ts = tsm \otimes 1/s'ts = m \otimes ts/s'ts = m \otimes 1/s$. Cette application est $S^{-1}A$-linéaire (exercice).

Ces applications sont inverses l'une de l'autre : on a $m/s \mapsto m \otimes 1/s \mapsto m/s$ et $m \otimes a/s \mapsto am/s \mapsto am \otimes 1/s = m \otimes a/s$. ∎

Corollaire Le A-module $S^{-1}A$ est plat.

Preuve. Soit $M' \to M \to M''$ une suite exacte. Alors $S^{-1}M' \to S^{-1}M \to S^{-1}M''$ est exacte et donc $M' \otimes_A S^{-1}A \to M \otimes_A S^{-1}A \to M'' \otimes_A S^{-1}A$ est exacte. ∎

Proposition 3.2.14 Soient M et N deux A-modules. Alors il existe un unique isomorphisme de $S^{-1}A$-modules $f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ tel que $f((m/s) \otimes (n/s')) = (m \otimes n)/ss'$.

Preuve. On a $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} S^{-1}N = M \otimes_A N \otimes_A S^{-1}A = S^{-1}(M \otimes_A N)$ (voir aussi le Lemme 3.3.7). L'inverse de f est donné par $(m \otimes n)/s \mapsto m/s \otimes n = m \otimes n/s$. ∎

Corollaire Pour un idéal premier $\mathfrak{p}$, on a un isomorphsme de $A_\mathfrak{p}$-modules :

$$M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \simeq (M \otimes_A N)_\mathfrak{p}.$$

3.3. Propriétés locales

Définition 3.3.1 Une propriété P d'un anneau A (resp. d'un module M) est dite **locale** si on a

P est vraie pour A (resp. M) $\Leftrightarrow$ P est vraie pour $A_\mathfrak{p}$ (resp. $M_\mathfrak{p}$) pour tout idéal premier $\mathfrak{p} \subset A$.

Proposition 3.3.2 Soit A un anneau et M un A-module. Les propriétés suivantes sont équivalentes :

1. $M = 0$;
2. $M_\mathfrak{p} = 0$ pour tout idéal premier $\mathfrak{p} \subset A$;
3. $M_\mathfrak{m} = 0$ pour tout idéal maximal $\mathfrak{m} \subset A$.

En particulier, la propriété (M est le module nul) est locale.

Preuve. Les implications $(1 \Rightarrow 2)$ et $(2 \Rightarrow 3)$ sont claires.

$(3 \Rightarrow 1)$ Supposons $M \neq 0$. Soit $m \in M$ tel que $m \neq 0$. Soit alors $\mathfrak{a} = \mathrm{Ann}(m) = \{a \in A \mid am = 0\}$. On a $1m = m \neq 0$ et donc $\mathfrak{a} \subsetneq A$. Soit $\mathfrak{m}$ un idéal maximal tel que $\mathfrak{a} \subset \mathfrak{m}$. On a $m/1 \in M_\mathfrak{m} = 0$. Il existe donc $s \in A \setminus \mathfrak{m}$ tel que $sm = 0$ et donc $s \in \mathrm{Ann}(m) = \mathfrak{a} \subset \mathfrak{m}$, une contradiction. ∎

Corollaire Soit A un anneau et soit $f : M \to N$ un morphisme de A-modules. Les assertions suivantes sont équivalentes :

1. f est injective (resp. surjective) ;
2. $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ est injective (resp. surjective) pour tout idéal premier $\mathfrak{p} \subset A$;
3. $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ est injective (resp. surjective) pour tout idéal maximal $\mathfrak{m} \subset A$.

En particulier les propriétés (f est injective), (f est surjective) et (f est bijective) sont locales.

Preuve. L'application f est injective (resp. surjective) lorsque $\mathrm{Ker}f = 0$ (resp. $\mathrm{Coker}f = 0$). Mais la suite

$$0 \to \mathrm{Ker}f \to M \xrightarrow{f_\mathfrak{p}} N \to \mathrm{Coker}f \to 0$$

est exacte et la localisation est exacte donc la suite

$$0 \to (\mathrm{Ker}f)_\mathfrak{p} \to M_\mathfrak{p} \xrightarrow{f_\mathfrak{p}} N_\mathfrak{p} \to (\mathrm{Coker}f)_\mathfrak{p} \to 0$$

est aussi exacte pour tout idéal premier $\mathfrak{p} \subset A$. On a donc $\mathrm{Ker}(f_\mathfrak{p}) = (\mathrm{Ker}f)_\mathfrak{p}$ et $\mathrm{Coker}(f_\mathfrak{p}) = (\mathrm{Coker}f)_\mathfrak{p}$. On déduit de la proposition précédente que les assertions $(\mathrm{Ker}f = 0)$, $(\mathrm{Ker}f_\mathfrak{p} = 0$ pour tout idéal premier $\mathfrak{p})$ et $(\mathrm{Ker}f_\mathfrak{m} = 0$ pour tout idéal maximal $\mathfrak{m})$ sont équivalentes. Les assertions pour l'injectivité et la surjectivité en découlent. ∎

Corollaire Soit $n \in \mathbb{N}$ un entier et soit $(x_1, \cdots, x_n)$ une famille génératrice de A^n. Alors $(x_1, \cdots, x_n)$ est une base *i.e.* l'application $f : A^n \to A^n$ définie par $f(a_1, \cdots, a_n) = a_1x_1 + \cdots + a_nx_n$ est un isomorphisme.

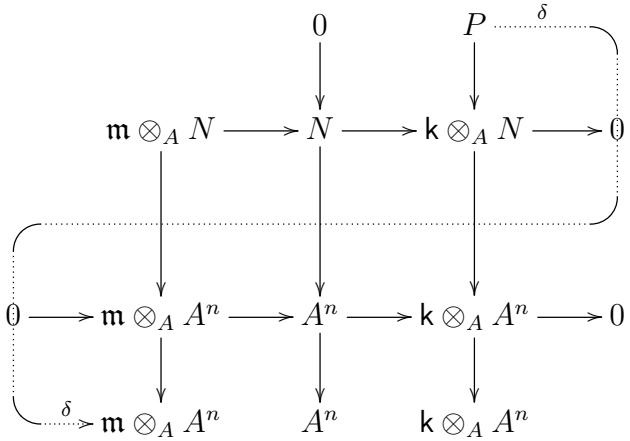
Preuve. L'application ci-dessus est surjective. Soit $N = \mathrm{Ker}f$. Nous avons une suite exacte $0 \to N \to A^n \xrightarrow{f} A^n \to 0$ et montrons $N = 0$.

Il suffit de montrer que $N_\mathfrak{m} = 0$ pour tout idéal maximal $\mathfrak{m}$. En remplaçant A par $A_\mathfrak{m}$ et N par $N_\mathfrak{m}$, on peut supposer que A est un anneau local d'idéal maximal $\mathfrak{m}$. Le quotient $\mathsf{k} = A/\mathfrak{m}$ est un corps.

Lemme 3.3.5 La suite $0 \to \mathsf{k} \otimes_A N \to \mathsf{k} \otimes_A A^n \to \mathsf{k} \otimes_A A^n \to 0$ est exacte.

Preuve. On a une suite exacte $\mathfrak{m} \otimes_A N \to A \otimes_A N \to \mathsf{k} \otimes_A N \to 0$. Comme A est plat comme A-module, on a une suite exacte $0 \to \mathfrak{m} \otimes_A A^n \to A \otimes_A A^n \to \mathsf{k} \otimes_A A^n \to 0$.

On obtient un diagramme commutatif à lignes exactes :



Le conoyau de l'application $N \to A^n$ (resp. $\mathsf{k} \otimes_A N \to \mathsf{k} \otimes_A A^n$) est A^n (resp. $\mathsf{k} \otimes_A A^n$) et l'application vers ce conoyau est f (resp. $\mathrm{Id}_\mathsf{k} \otimes f$). Le noyau de l'application $N \to A^n$

est 0 (cette application est injective). Soit P le noyau de l'application $\mathsf{k}\otimes_A N \to \mathsf{k}\otimes_A A^n$. Par le lemme du serpent, la suite $0 \to P \to \mathfrak{m} \otimes_A A^n \to A^n \to \mathsf{k} \otimes_a A^n$ est exacte. Mais l'application $\mathfrak{m}\otimes_A A^n \to A^n$ est injective (car A^n est plat). On en déduit $P = 0$.∎

Par ailleurs, on a $\mathsf{k} \otimes_A A^n = (\mathsf{k} \otimes_A A)^n = \mathsf{k}^n$ et donc la dernière application de la suite exacte du lemme précédent est un isomorphisme de k-espaces vectoriels. On a donc $0 = \mathsf{k} \otimes_A N = A/\mathfrak{m} \otimes_A N = N/\mathfrak{m}N$.

Le sous-module N est de type fini (cf. Exercice 2 feuille 3) et par Nakayama on a $N = 0$. ∎

Proposition 3.3.6 soit A un anneau et M un A-module. Les assertions suivantes sont équivalentes :

1. M est un A-module plat ;
2. $M_\mathfrak{p}$ est un $A_\mathfrak{p}$-module plat pour tout idéal premier $\mathfrak{p} \subset A$;
3. M est un $A_\mathfrak{m}$-module plat pour tout idéal maximal $\mathfrak{m} \subset A$.

En particulier la propriété (M est plat) est locale.

Preuve. ($1 \Rightarrow 2$) Nous començons par un lemme.

Lemme 3.3.7 Soit $f : A \to B$ un morphisme d'anneaux et M un A-module.

1. Soit N un B-module. Alors on a un isomorphisme de B-modules $N \otimes_B (B \otimes_A M) \simeq N \otimes_A M$.

2. Si M est un A-module plat, alors $B \otimes_A M$ est un B-module plat.

Preuve. 1. La structure de A-module de N est donnée par $a \cdot n = f(a)n$. Le structure de B-module de $N \otimes_B M$ est donnée par $b \cdot (n \otimes m) = bn \otimes m$.

Soit $\varphi : N \times B \times M \to N \otimes_A M$ l'application définie par $\varphi(n, b, m) = bn \otimes m$. Elle est A-bilinéaire en les deux dernières variables et se factorise donc en une application $N \times (B \otimes_A M)$ défnie par $(n, b \otimes m) \mapsto bn \otimes m$. Cette application est B-bilinéaire. Il existe donc une application B-linéaire $\bar\varphi : N \otimes_B (B \otimes_A M) \to N \otimes_A M$, $n \otimes (b \otimes m) \mapsto bn \otimes m$. De la même manière, il existe une appllication A-bilinéaire $\psi : N \times M \to N \otimes_B (B \otimes_A M)$ définie par $\psi(n, m) = n \otimes (1 \otimes m)$. On en déduit une application A-linéaire $\bar\psi : N \otimes_A M \to N \otimes_B (B \otimes_A M)$, $n \otimes m \mapsto n \otimes (1 \otimes m)$. Cette application est aussi B-linéaire. En effet, on a $\bar\psi(b \cdot (n \otimes m)) = \bar\psi(bn \otimes m) = bn \otimes (1 \otimes m) = b\bar\psi(n \otimes m)$.

Nous montrons que $\bar\varphi$ et $\bar\psi$ sont inverses l'une de l'autre. On a $\bar\varphi(\bar\psi(n \otimes m)) = \bar\varphi(n \otimes (1 \otimes m)) = n \otimes m$ et $\bar\psi(\bar\varphi(n \otimes (b \otimes m))) = \bar\psi(bn \otimes m) = bn \otimes (1 \otimes m) = n \otimes (b \cdot (1 \otimes m)) = n \otimes (b \otimes m)$.

2. Soit $N' \to N \to N''$ une suite exacte de B-modules. Alors la suite $N' \otimes_B (A \otimes_A M) \to N \otimes_B (A \otimes_A M) \to N'' \otimes_B (A \otimes_A M)$ est exactement la suite $N' \otimes_A M \to N \otimes_A M \to N'' \otimes_A M$. Comme M est plat, cette dernière est exacte. ∎

On a $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}} \otimes_A M$. Par le lemme précédent, on a que $M_{\mathfrak{p}}$ est plat car M est plat.

L'implication $(2 \Rightarrow 3)$ est claire.

$(3 \Rightarrow 1)$ Comme le produit tensoriel est exact à droite, il suffit de montrer que pour une suite exacte $0 \to N' \xrightarrow{f} N$, la suite $0 \to M \otimes_A N' \xrightarrow{\mathrm{Id}_M \otimes f} M \otimes_A N$ est encore exacte. Pour tout idéal maximal $\mathfrak{m} \subset A$, les suites suivantes sont exactes (la première parceque la localisation est exacte et la suivante parceque $M_{\mathfrak{m}}$ est plat) :

$$0 \to N'_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \text{ et } 0 \to M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N'_{\mathfrak{m}} \xrightarrow{\mathrm{Id}_{M_{\mathfrak{m}}} \otimes f_{\mathfrak{m}}} M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}}.$$

On vérifie cependant aisément que l'on a $(\mathrm{Id}_M \otimes f)_{\mathfrak{m}} = \mathrm{Id}_{M_{\mathfrak{m}}} \otimes f_{\mathfrak{m}}$. On en déduit que $(\mathrm{Id}_M \otimes f)_{\mathfrak{m}}$ est injective pour tout idéal maximal $\mathfrak{m} \subset A$. Par conséquent $\mathrm{Id}_M \otimes f$ est injective. ∎

3.4. Idéaux et localisation

Proposition 3.4.1 Soit A un anneau et soit $S \subset A$ un sous-ensemble multiplicatif.

1. Soit $\mathfrak{a}$ un idéal de A. Alors on a $(\lambda(\mathfrak{a})) = S^{-1}\mathfrak{a}$.

2. Soit $\mathfrak{b}$ un idéal de $S^{-1}A$. Alors $\mathfrak{b}$ est de la forme $S^{-1}\mathfrak{a}$ pour un idéal $\mathfrak{a}$ de A. Plus précisément, on a $\mathfrak{b} = S^{-1}(\lambda^{-1}(\mathfrak{b}))$.

3. Soit $\mathfrak{a}$ un idéal de A. On a $\lambda^{-1}(S^{-1}\mathfrak{a}) = \lambda^{-1}((\lambda(\mathfrak{a}))) = \cup_{s \in S}(\mathfrak{a} : s)$.

4. Un idéal $\mathfrak{a}$ de A est de la forme $\lambda^{-1}(\mathfrak{b})$ pour un idéal $\mathfrak{b} \subset S^{-1}A$, si et seulement si aucun élément de S n'est envoyé sur un diviseur de zéro dans $A/\mathfrak{a}$. Dans ce cas, on a $\mathfrak{a} = \lambda^{-1}(S^{-1}(\mathfrak{a}))$.

5. On a des bijections réciproques $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ et $\mathfrak{q} \mapsto \lambda^{-1}(\mathfrak{q})$ entre les ensembles

$$\{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ idéal premier tel que } \mathfrak{p} \cap S = \emptyset\} \leftrightarrow \{\mathfrak{q} \subset S^{-1}A \mid \mathfrak{q} \text{ idéal premier }\}.$$

6. Soient $\mathfrak{a}$ et $\mathfrak{a}'$ des idéaux de A. On a

   a. $S^{-1}(\mathfrak{a} + \mathfrak{a}') = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{a}'$
   b. $S^{-1}(\mathfrak{a}\mathfrak{a}') = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{a}')$
   c. $S^{-1}(\mathfrak{a} \cap \mathfrak{a}') = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{a}'$
   d. $\sqrt{S^{-1}\mathfrak{a}} = S^{-1}\sqrt{\mathfrak{a}}$.

Preuve. 1. On a $\lambda(\mathfrak{a}) \subset S^{-1}\mathfrak{a}$ et donc $(\lambda(\mathfrak{a})) \subset S^{-1}\mathfrak{a}$. Soit $a/s \in S^{-1}\mathfrak{a}$ tel que $a \in \mathfrak{a}$ et $s \in S$. On a alors $a/s = 1/s \cdot a/1 = 1/s \cdot \lambda(a) \in (\lambda(\mathfrak{a}))$.

2. On a $S^{-1}(\lambda^{-1}(\mathfrak{b})) = ((\lambda(\lambda^{-1}(\mathfrak{b})))) = ((\mathfrak{b})) = \mathfrak{b}$.

3. Soit $a \in \lambda^{-1}(S^{-1}(\mathfrak{a}))$. On a $\lambda(a) = a'/s$, où $a' \in \mathfrak{a}$ et $s \in S$. On en déduit qu'il existe $t \in S$ tel que $t(as - a') = 0$ et donc $tsa = ta' \in \mathfrak{a}$. On a donc $a \in (\mathfrak{a} : ts)$. Réciproquement, soit $a \in (\mathfrak{a} : s)$, on a $sa = a' \in \mathfrak{a}$. On en déduit $\lambda(a) = a/1 = sa/s = a'/s \in S^{-1}\mathfrak{a}$.

4. Soit $\mathfrak{a}$ de la forme $\mathfrak{a} = \lambda^{-1}(\mathfrak{b})$. On a alors $S^{-1}(\mathfrak{a}) = \mathfrak{b}$. Soit $s \in S$ et $\bar{s}$ la classe de s dans $A/\mathfrak{a}$. Si $\bar{s}$ est diviseur de zéro, il existe $a \in A$ tel que $\bar{a} \neq 0$ et $\bar{a}\bar{s} = 0$. On a donc $sa \in \mathfrak{a}$ et $a \in (\mathfrak{a} : s)$. Par 3., on a $a \in \lambda^{-1}(S^{-1}(\mathfrak{a})) = \lambda^{-1}(\mathfrak{b}) = \mathfrak{a}$ *i.e.* $\bar{a} = 0$ une contradiction.

Réciproquement, si aucun élément de S n'est envoyé sur un diviseur de zéro dans $A/\mathfrak{a}$, nous montrons que $\mathfrak{a} = \lambda^{-1}(S^{-1}(\mathfrak{a}))$. On a toujours $\mathfrak{a} \subset \lambda^{-1}(S^{-1}(\mathfrak{a}))$. Soit donc $a \in \lambda^{-1}(S^{-1}(\mathfrak{a}))$. Par 3., il existe un $s \in S$ tel que $sa \in \mathfrak{a}$. On a donc $\bar{s}\bar{a} = 0$ dans $A/\mathfrak{a}$. Comme $\bar{s}$ n'est pas diviseur de zéro, on a $\bar{a} = 0$ et $a \in \mathfrak{a}$.

5. Soit $\mathfrak{p}$ un idéal premier tel que $\mathfrak{p} \cap S = \emptyset$. Nous montrons que $S^{-1}\mathfrak{p}$ est un idéal premier. Notons que $S \cap \mathfrak{p} = \emptyset$ impose que $S^{-1}\mathfrak{p} \subsetneq S^{-1}A$. Soient a/s et a'/s' dans $S^{-1}A$ tels que $(a/s)(a'/s') \in S^{-1}\mathfrak{p}$. On a alors un $b \in \mathfrak{p}$ et un $t \in S$ tels que $aa'/ss' = b/t$. Il existe donc $t' \in S$ tel que $t'(aa't - bss') = 0$. On en déduit $tt'aa' = t'bss' \in \mathfrak{p}$. Comme $t, t' \in S$, on a $t, t' \notin \mathfrak{p}$. On a donc $a \in \mathfrak{p}$ ou $a' \in \mathfrak{p}$ et donc $a/s \in S^{-1}\mathfrak{p}$ ou $a'/s' \in S^{-1}\mathfrak{p}$.

Pour $\mathfrak{p}$ idéal premier tel que $\mathfrak{p} \cap S = \emptyset$, on a $0 \neq \bar{s} \in A/\mathfrak{p}$ et comme $A/\mathfrak{p}$ est intègre, on a que $\bar{s}$ n'est pas diviseur de zéro. On a donc $\mathfrak{p} = \lambda^{-1}(S^{-1}(\mathfrak{p}))$.

Réciproquement, par 2., on a $S^{-1}(\lambda^{-1}(\mathfrak{q})) = \mathfrak{q}$.

6. Exercice. ∎

Proposition 3.4.2 On a $\mathfrak{n}(S^{-1}A) = S^{-1}\mathfrak{n}(A)$.

Preuve. Soit $a \in \mathfrak{n}(A)$ tel que $a^n = 0$. On a $(a/s)^n = a^n/s^n = 0$ et $a/s \in \mathfrak{n}(S^{-1}A)$ pour tout $s \in S$. Réciproquement, soit $a/s \in \mathfrak{n}(S^{-1}A)$. On a $a^n/s^n = (a/s)^n = 0$. Il existe donc $t \in S$ tel que $ta^n = 0$ et donc $(ta)^n = 0$. On a donc $a/s = ta/ts \in S^{-1}\mathfrak{n}(A)$. ∎

Proposition 3.4.3 Soit $\mathfrak{p}$ un idéal premier. Il existe une bijection $\mathfrak{q} \mapsto \mathfrak{q}_\mathfrak{p}$ et $\mathfrak{r} \mapsto \lambda^{-1}(\mathfrak{r})$ entre les ensembles suivants :

$$\{\mathfrak{q} \subset A \mid \mathfrak{q} \subset \mathfrak{p} \text{ idéal premier } \} \longleftrightarrow \{\mathfrak{r} \subset A_\mathfrak{p} \mid \mathfrak{r} \text{ idéal premier } \}.$$

Preuve. Soit $S = A \setminus \mathfrak{p}$. On a $\mathfrak{q} \cap S = \emptyset \Leftrightarrow \mathfrak{q} \subset \mathfrak{p}$. L'assertion résulte de la Proposition 3.4.1.5. ∎

Proposition 3.4.4 Soit M un A-module de type fini. Alors on a $S^{-1}\mathrm{Ann}(M) = \mathrm{Ann}(S^{-1}M)$.

Preuve. Soit $a \in \mathrm{Ann}(M)$, soit $s \in S$ et soit $m/t \in S^{-1}M$, avec $m \in M$ et $t \in S$. On a $am = 0$. On en déduit $a/s \cdot m/t = am/st = 0$ et $a/s \in \mathrm{Ann}(S^{-1}M)$.

Réciproquement, soit $a/s \in \mathrm{Ann}(S^{-1}M)$ et soient $m_1, \cdots, m_n$ des générateurs de M. Pour tout $i \in [1, n]$, on a $am_i/s = a/s \cdot m_i/1 = 0$. Il existe donc $t_i \in S$ tel que $tam_i = 0$. On a donc $t_1 \cdots t_n am_i = 0$ pour tout $i \in [1, n]$ et donc $t_1 \cdots t_n a \in \mathrm{Ann}(M)$. On en déduit $a/s = t_1 \cdots t_n a/t_1 \cdots t_n s \in S^{-1}\mathrm{Ann}(M)$. ∎

Exemple Soit $A = \mathbb{Z}$ et $M = \mathbb{Q}/\mathbb{Z}$. Commençons par montrer que $\mathrm{Ann}(M) = 0$. En effet, soit $a \in \mathrm{Ann}(M)$. Alors $am = 0$ pour tout $m \in M$. En particulier, $a[1/p] = 0$ pour tout nombre premier p donc $[a/p] = 0$ ou encore $a/p \in \mathbb{Z}$ ce qui signifie que p divise a pour tout nombre premier p. L'entier a est donc divisible par tous les nombres premiers et ainsi $a = 0$. On en déduit

$$S^{-1}\mathrm{Ann}(M) = S^{-1}0 = 0.$$

Soit $S = \mathbb{Z} \setminus \{0\}$. Montrons maintenant que $S^{-1}M = 0$. En effet, un élément de ce module est de la forme $\frac{[a/b]}{s}$ avec $a \in \mathbb{Z}$ et $b, s \in \mathbb{Z} \setminus \{0\}$. On a alors

$$\frac{[a/b]}{s} = \frac{b[a/b]}{bs} = \frac{[ab/b]}{bs} = \frac{[a/1]}{bs} = \frac{0}{bs} = 0.$$

Mais alors $\mathrm{Ann}(S^{-1}M) = \mathrm{Ann}(0) = \{x \in S^{-1}A \mid xy = 0 \text{ pour tout } y \in S^{-1}M\} = S^{-1}A = \mathbb{Q}$ donc

$$\mathrm{Ann}(S^{-1}M) = \mathbb{Q}.$$

En particulier on a pas $S^{-1}\mathrm{Ann}(M) = \mathrm{Ann}(S^{-1}M)$ et ceci prouve que $\mathbb{Q}/\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module de type fini.

Corollaire soient $N, P \subset M$ des sous-modules avec P de type fini. Alors on a $S^{-1}(N : P) = (S^{-1}N, S^{-1}P)$.

Preuve. On a un morphisme $P \to P + N/N$ défini par $p \mapsto [p]$. Ce morphisme est surjectif : en effet, on a $[p + n] = [p]$. On a donc que $P + N/N$ est de type fini. Nous montrons $(N : P) = \mathrm{Ann}(P + N/N)$. Soit $a \in (N : P)$. Alors on a $a(P + N) = aP + N \subset N$ et donc $a(P + N/N) = 0$ et $a \in \mathrm{Ann}(P + N/N)$. Réciproquement, soit $a \in \mathrm{Ann}(P + N/N)$. Alors on a $a(P + N) \subset N$ et donc $aP \subset N$ et $a \in (N : P)$. On en déduit

$$\begin{aligned} S^{-1}(N : P) &= S^{-1}\mathrm{Ann}(P + N/N) = \mathrm{Ann}(S^{-1}(P + N/N)) \\ &= \mathrm{Ann}(S^{-1}P + S^{-1}N/S^{-1}N) = (S^{-1}N : S^{-1}P). \end{aligned}$$

Proposition 3.4.7 Soit $f : A \to B$ un morphisme d'anneaux et soit $\mathfrak{p} \subset A$ un idéal premier. On a une équivalence :

(il existe un idéal premier $\mathfrak{q} \subset B$ tel que $f^{-1}(\mathfrak{q}) = \mathfrak{p}$) $\Leftrightarrow$ ($\mathfrak{p} = f^{-1}((f(\mathfrak{p}))))$.

Preuve. Soit $\mathfrak{q} \subset B$ premier tel que $\mathfrak{p} = f^{-1}(\mathfrak{q})$. On a $f(\mathfrak{p}) \subset \mathfrak{q}$ et $f^{-1}(f(\mathfrak{p})) \subset f^{-1}(\mathfrak{q}) = \mathfrak{p}$. On en déduit $\mathfrak{p} = f^{-1}((f(\mathfrak{p})))$.

Réciproquement, soit $\mathfrak{p}$ premier tel que $\mathfrak{p} = f^{-1}((f(\mathfrak{p})))$. On pose $S = f(A \setminus \mathfrak{p}) \subset B$. C'est un ensemble multiplicatif. En effet, $1 = f(1) \in f(A \setminus \mathfrak{p}) = S$ et pour $x, x' \in S$ il existe $a, a' \in A \setminus \mathfrak{p}$ tels que $f(a) = x$ et $f(a') = x'$. On a alors $aa' \in A \setminus \mathfrak{p}$ donc $xx' = f(a)f(a') = f(aa') \in S$.

On a $(f(\mathfrak{p})) \cap S = \emptyset$. En effet, si $x \in (f(\mathfrak{p})) \cap S$, il existe $a \in A \setminus \mathfrak{p}$ tel que $f(a) = x$ donc $a \in f^{-1}((f(\mathfrak{p}))) = \mathfrak{p}$, une contradiction. On en déduit que $S^{-1}(f(\mathfrak{p}))$ est un idéal distinct de $S^{-1}B$. En effet, si on avait $S^{-1}(f(\mathfrak{p})) = B$ alors on aurait $1 \in S^{-1}(f(\mathfrak{p}))$ et donc il existe $s \in S$ tel que $s = s \cdot 1 \in (f(\mathfrak{p}))$, une contradiction.

Soit maintenant $\mathfrak{m}$ un idéal maximal de $S^{-1}B$ tel que $(f(\mathfrak{p})) \subset \mathfrak{m}$ et soit $\lambda : B \to S^{-1}B$. On pose $\mathfrak{q} = \lambda^{-1}(\mathfrak{m})$, c'est un idéal premier de B.

Nous montrons que $f^{-1}(\mathfrak{q}) = \mathfrak{p}$. Soit $a \in \mathfrak{p}$, on a $\lambda(f(a)) \in \lambda(f(\mathfrak{p})) \subset S^{-1}(f(\mathfrak{p})) \subset \mathfrak{m}$ et donc $f(a) \in \mathfrak{q}$. Réciproquement, soit $a \in f^{-1}(\mathfrak{q})$. Si $a \notin \mathfrak{p}$, on a $f(a) \in S$. Mais on a $f(a) \in \mathfrak{q}$ donc $S \cap \mathfrak{q} \neq \emptyset$. On en déduit $\lambda\mathfrak{q} = S^{-1}\mathfrak{q} = S^{-1}B$, une contradiction. ∎

4. Éléments entiers

4.1. Éléments entiers

Définition 4.1.1 Soit B un anneau et A un sous-anneau de B. Un élément $x \in B$ est dit **entier sur** A s'il existe un polynôme $P \in A[X]$ de coefficient dominant 1 tel que $P(x) = 0$ ou encore s'il existe des éléments $a_i \in A$ pour $i \in [1, n]$ tels que

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

Remarque Les éléments de A sont entiers sur A.

Exemple Soit $A = \mathbb{Z}$ et $B = \mathbb{Q}$. Un élément $x \in \mathbb{Q}$ est entier si et seulement si $x \in \mathbb{Z}$ (exercice).

Proposition 4.1.4 Soit $A \subset B$ un sous-anneau et soit $x \in B$. On a équivalence entre :

1. x est entier sur A ;
2. $A[x]$ est un A-module de type fini ;
3. $A[x] \subset C$ avec C un sous-anneau de B qui est de type fini comme A-module ;
4. il existe un $A[x]$-module fidèle M, qui est de type fini comme A-module.

Preuve. (1. $\Rightarrow$ 2.) On a $x^{n+r} = -(a_1 x^{n+r-1} + \cdots + a_n x^r)$ pour tout $r \geq 0$. On a donc que $A[x]$ est engendré par la famille finie $(1, \cdots, x^{n-1})$.

(2. $\Rightarrow$ 3.) Il suffit de prendre $C = A[x]$.

(3. $\Rightarrow$ 4.) On pose $M = C$. Soit $P \in A[x]$ tel que $P \in \mathrm{Ann}(M)$ *i.e* $P \cdot M = 0$. Comme $1 \in C = M$, on a $P = P \cdot 1 = 0$ donc $\mathrm{Ann}(M) = 0$ et M est fidèle.

(4. $\Rightarrow$ 1.) Soit M un $A[x]$-module fidèle tel que M est de type fini comme A-module. Soit $f : M \to M$ l'application A-linéaire définie par $f(m) = xm$. Soit $\mathfrak{a} = A$. Par la Proposition 2.7.1, il existe des éléments $a_1, \cdots, a_n \in \mathfrak{a} = A$ tels que $f^n + a_1 f^{n-1} + \cdots + a_n \mathrm{Id}_M = 0$. Pour tout $m \in M$, on a alors $(x^n + a_1 x^{n-1} + \cdots + a_n)m = 0$. Comme M est fidèle, on en déduit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. ∎

Corollaire Soient $x_1, \cdots, x_n$ des éléments entiers sur A. Alors $A[x_1, \cdots, x_n]$ est un A-module de type fini.

Preuve. Par la proposition précédente, on a que $A[x_1]$ est un A-module de type fini. Par récurrence, on obtient que $A[x_1, \cdots, x_{n-1}]$ est de type fini sur A. Mais x_n est entier sur A donc aussi sur $A[x_1, \cdots, x_{n-1}]$. Le A-module $A[x_1, \cdots, x_n]$ est donc de type fini sur $A[x_1, \cdots, x_{n-1}]$ et $A[x_1, \cdots, x_{n-1}]$ est de type fini sur A. Par la Proposition 2.11.4, on en déduit le résultat. ∎

Corollaire Soit $A \subset B$ un sous-anneau. L'ensemble des éléments de B entiers sur A forme un sous-anneau de B contenant A.

Preuve. On sait déjà que les éléments de A sont entiers sur A. Soient $x, y \in B$ entiers sur A. Alors $C = A[x, y]$ est un A-module de type fini contenant $A[x+y]$ et $A[xy]$. De la Proposition précédente (cas 3.) on en déduit que $x + y$ et xy sont entiers sur A. ∎

Définition 4.1.7 Soit $A \subset B$ un sous-anneau.

1. Le sous-anneau de B formé des éléments entiers sur A s'appelle **la fermeture ou cloture intégrale de A dans B**. On la note $\overline{A}^B$.

2. Si A est égale à sa cloture intégrale dans B (*i.e.* $A = \overline{A}^B$), on dit que A **est intégralement clos dans B**.

3. Lorsque B est la cloture intégrale de A dans B (*i.e* $B = \overline{A}^B$) ou encore si tous les éléments de B sont entiers sur A, on dit que B est **entier sur A**.

Définition 4.1.8 Soit $f : A \to B$ un morphisme d'anneaux (c'est-à-dire que B est une A-algèbre). La A-algèbre B est dite **entière** lorsque B est entier sur $f(A)$.

Lemme 4.1.9 Soit $f : A \to B$ une A-algèbre. On a équivalence entre

1. B est un A-module de type fini ;
2. B est une A-algèbre finiment engendrée sur A et entière sur A.

Preuve. ($\Rightarrow$) Découle de ce qui précède.

($\Leftarrow$) Soit $(x_1, \cdots, x_n)$ une famille génératrice de B comme A-algèbre. On a alors $f(A)[x_1, \cdots, x_n] = B$. Comme B est entier sur A, les éléments x_i sont aussi entiers et le module B est aussi de type fini. ∎

Proposition 4.1.10 Soient $A \subset B \subset C$ des sous-anneaux. Si B est entier sur A et si C est entier sur B, alors C est entier sur A.

Preuve. Soit $x \in C$. Il existe des éléments $b_1, \cdots, b_n \in B$ tels que $x^n + b_1 x^{n-1} + \cdots + b_n = 0$. Soit $B' = A[b_1, \cdots, b_n]$. Comme tous les b_i sont entiers sur A, le A-module B' est de type fini. Comme x est entier sur B', le B'-module $B'[x]$ est de type fini. On en déduit que $B'[x]$ est de type fini comme A-module. Comme $A[x]$ est contenu dans cet anneau, on a bien que x est entier sur A par la Proposition 4.1.4.3. ∎

Corollaire 4.1.11 Soit $A \subset B$ un sous-anneau et soit C la cloture intégrale de A dans B. ALors C est intégralement clos dans B.

Preuve. Soit $\overline{C}^B$ la cloture intégrale de C dans B. Alors $\overline{C}^B$ est entier sur A donc $\overline{C}^B \subset C$. Comme on a toujours $C \subset \overline{C}^B$ on a le résultat. ∎

Proposition 4.1.12 Soient $A \subset B$ tels que B est entier sur A.

1. Soit $\mathfrak{b} \subset B$ un idéal et $\mathfrak{a} = A \cap \mathfrak{b}$. Alors $B/\mathfrak{b}$ est entier sur $A/\mathfrak{a}$.

2. Soit $S \subset A$ une partie multiplicative. Alors $S^{-1}B$ est entier sur $S^{-1}A$.

Preuve. 1. Soit $x \in B$. Alors il existe $a_1, \cdots, a_n \in A$ tels que $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. On en déduit $[x]^n + [a_1][x]^{n-1} + \cdots + [a_n] = 0$.

2. Soit $x/s \in S^{-1}B$ avec $x \in B$ et $s \in S$. Il existe $a_1, \cdots, a_n \in A$ tels que $x^n + a_1 x^{n-1} + \cdots + x_n = 0$. On en déduit $(x/s)^n + (a_1/s)(x/s)^{n-1} + \cdots + (a_n/s^n) = 0$. ∎

4.2. Théorème "Going-up"

Proposition 4.2.1 Soit $A \subset B$ avec B intègre et entier sur A. On a l'équivalence

$$A \text{ est un corps} \Leftrightarrow B \text{ est un corps.}$$

Preuve. ($\Rightarrow$) Soit $b \in B$ tel que $b \neq 0$. Il existe $a_1, \cdots, a_n \in A$ tels que $b^n + a_1 b^{n-1} + \cdots + a_n = 0$. Soit n pour qu'il existe une telle relation. Si $a_n = 0$, alors $b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = 0$ donc $b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1} = 0$ ce qui contredit la minimalité de n. On a donc $a_n \neq 0$ et il existe $a_n^{-1} \in A$. On a alors $-b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1})a_n^{-1} = 1$ donc b est inversible.

($\Leftarrow$) Soit $a \in A$ tel que $a \neq 0$. Comme B est un corps, il existe $a^{-1} \in B$. Montrons que $a^{-1} \in A$. Comme B est entier, il existe $a_1, \cdots, a_n \in A$ tels que $a^{-n} + a_1 a^{-n+1} + \cdots + a_n = 0$. En multipliant par a^{n-1} on obtient $a^{-1} + a_1 + \cdots + a_n a^{n-1}$ et donc $a^{-1} = -(a_1 + \cdots + a_n a^{n-1}) \in A$. ∎

Corollaire Soient $A \subset B$ des anneaux avec B entier sur A. Soit $\mathfrak{q}$ un idéal premier de B et soit $\mathfrak{p} = A \cap \mathfrak{q}$. On a alors

$$\mathfrak{q} \text{ maximal} \Leftrightarrow \mathfrak{p} \text{ maximal.}$$

Preuve. L'anneau $B/\mathfrak{q}$ est entier sur $A/\mathfrak{p}$ et est intègre. L'assertion découle directement de la proposition. ∎

Corollaire Soient $A \subset B$ des anneaux avec B entier sur A. Soient $\mathfrak{q}$ et $\mathfrak{q}'$ des idéaux premiers tels que $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Si $\mathfrak{q} \subset \mathfrak{q}'$, alors $\mathfrak{q} = \mathfrak{q}'$.

Preuve. Soit $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. L'anneau $B_\mathfrak{p}$ est entier sur $A_\mathfrak{p}$. Soit $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$ l'idéal de $A_\mathfrak{p}$ engendré par $\mathfrak{p}$. Alors $\mathfrak{m}$ est l'unique idéal maximal de $A_\mathfrak{p}$. Soient $\mathfrak{n}$ et $\mathfrak{n}'$ les idéaux de $B_\mathfrak{p}$ engendrés par $\mathfrak{q}$ et $\mathfrak{q}'$. On vérifie (exercice) que $\mathfrak{n} \subset \mathfrak{n}'$ et $\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{m} = \mathfrak{n}' \cap A_\mathfrak{p}$. Comme $\mathfrak{m}$ est maximal, les idéaux $\mathfrak{n}$ et $\mathfrak{n}'$ sont maximaux. On a donc $\mathfrak{n} = \mathfrak{n}'$. On utilise maintenant la bijection entre idéaux premiers de B ne rencontrant pas $S = A \setminus \mathfrak{p}$ et les idéaux premiers de $S^{-1}B = B_\mathfrak{p}$. Comme $A \cap \mathfrak{q} = \mathfrak{p} = A \cap \mathfrak{q}'$, on a $\mathfrak{q} \cap S = \emptyset = \mathfrak{q}' \cap S$ d'où il découle que $\mathfrak{q} = \mathfrak{q}'$. ∎

Théorème 4.2.4 Soient $A \subset B$ des anneaux avec B enter sur A. Soit $\mathfrak{p}$ un idéal premier de A. Alors il existe un idéal premier $\mathfrak{q}$ de B tel que $\mathfrak{q} = A \cap \mathfrak{q}$. □

Preuve. On a un diagramme commutatif

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle \lambda_A}\downarrow & & \downarrow{\scriptstyle \lambda_B} \\ A_\mathfrak{p} & \longrightarrow & B_\mathfrak{p}. \end{array}$$

Soit $\mathfrak{n}$ maximal dans $B_\mathfrak{p}$. Alors $\mathfrak{m} = \mathfrak{n} \cap A_\mathfrak{p}$ est maximal dans $A_\mathfrak{p}$. Cet anneau est local d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$, on a donc $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$. Soit $\mathfrak{q} = \lambda_B^{-1}(\mathfrak{n})$. C'est un idéal premier de B et on a $\mathfrak{q} \cap A = \lambda_A^{-1}(\mathfrak{m}) = \lambda^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$. ∎

Remarque Soit $\mathrm{Spec}(A) = \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ idéal premier }\}$. Pour un morphisme d'anneau $f : A \to B$ on a une application $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ définie par $\mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$. La proposition précédente nous dit que si B est entier sur A, cette application est surjective.

Théorème 4.2.6 (Going-up Theorem) Soient $A \subset B$ des anneaux avec B entier sur A. Soit $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ une suite d'idéaux premiers de A et soit $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ avec $m < n$ une suite d'idéaux premiers de B telle que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ pour tout $i \in [1, m]$.

Alors on peut compléter la suite $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ en une suite d'idéaux premiers $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ tels que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ pour tout $i \in [1, n]$. □

Preuve. Par récurrence, il suffit de montrer l'énoncé pour $m = 1$ et $n = 2$. On a un diagramme commutatif

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_B} \\ A/\mathfrak{p}_1 & \longrightarrow & B/\mathfrak{q}_1, \end{array}$$

où π_A et π_B sont les projections canoniques. Soit $\mathfrak{p} = \pi_A(\mathfrak{p}_2)$. Comme $\mathfrak{p}_1 \subset \mathfrak{p}_2$, l'idéal $\mathfrak{p}$ est premier dans $A/\mathfrak{p}_1$. L'anneau $B/\mathfrak{q}_1$ est entier sur $A/\mathfrak{p}_1$ donc il existe, par le théorème précédent, un idéal premier $\mathfrak{q} \subset B/\mathfrak{q}_1$ tel que $\mathfrak{q} \cap (A/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$. Soit $\mathfrak{q}_2 = \pi_B^{-1}(\mathfrak{q})$. Alors on a $\mathfrak{q}_2$ premier et $\mathfrak{q}_2 \cap A = \pi_A^{-1}(\mathfrak{q} \cap (A/\mathfrak{p}_1) = \pi_A^{-1}(\mathfrak{p}) = \mathfrak{p}_2$. ∎

Deuxième partie .

Application à la géométrie

5. Ensembles algébriques

Soit k un corps.

5.1. Premières définitions

Définition 5.1.1 Soit $n \in \mathbb{N}$.

1. L'ensemble k^n des n-uplets $x = (x_1, \ldots, x_n) \in \mathsf{k}^n$ est appelé **espace affine de dimension n sur k**. On le note aussi $\mathbb{A}_n(\mathsf{k})$.

2. Pour $x = (x_1, \ldots, x_n) \in \mathbb{A}_n(\mathsf{k})$ et pour un polynôme $P \in \mathsf{k}[X_1, \ldots, X_n]$, on utilisera la notation $P(x) := P(x_1, \ldots, x_n)$.

3. Soit $S \subset \mathsf{k}[X_1, \ldots, X_n]$ un sous-ensemble. On pose

$$V(S) = \{x \in \mathbb{A}_n(\mathsf{k}) \mid P(x) = 0 \text{ pour tout } P \in S\}.$$

L'ensemble $V(S)$ s'appelle **l'ensemble algébrique associé à S**.

4. Pour un ensemble fini $S = \{P_1, \ldots, P_r\}$, on utilisera la notation $V(S) = V(P_1, \ldots, P_r)$.

Exemple 1. L'ensemble vide $\emptyset$ est un ensemble algébrique. En effet, on a $V(1) = \emptyset$.

2. L'espace affine tout entier $\mathbb{A}_n(\mathsf{k})$ est un ensemble algébrique $V(0) = \mathbb{A}_n(\mathsf{k})$.

3. Pour $n = 1$ et $S \neq \{0\}$, l'ensemble $V(S)$ est fini.

Lemme 5.1.3 Soit $n = 1$. Les ensembles algébriques de $\mathbb{A}_1(\mathsf{k})$ sont $\emptyset$, $\mathbb{A}_1(\mathsf{k})$ et tous les ensembles finis de $\mathbb{A}_1(\mathsf{k})$.

Preuve. Exercice. ∎

Exemple 1. Pour $n = 2$, les ensembles algébriques de $\mathbb{A}_2(\mathsf{k})$ sont de la forme suivante : $\emptyset$, $\mathbb{A}_2(\mathsf{k})$, tous les sous-ensembles finis de $\mathbb{A}_2(\mathsf{k})$ et enfin les "courbes planes". Par exemple, on a les ensembles algébriques suivants

$$V(X, Y) = \{(0, 0)\},\ V(X(X-1), Y) = \{(0, 0), (1, 0)\},\ V(X) = \text{ Droite},$$
$$V(X^2 + Y^2 - 1) = \text{ Cercle},\ V(Y^2 - X(X-1)(X+1) = \text{ Courbe elliptique}.$$

2. Un point $(a_1, \ldots, a_n) \in \mathbb{A}_n(\mathsf{k}) = \mathsf{k}^n$ est toujours un ensemble algébrique. En effet, on a l'égalité :

$$\{(a_1, \ldots, a_n)\} = V(X_1 - a_1, \ldots, X_n - a_n).$$

Lemme 5.1.5 Soient $S \subset S'$ deux sous-ensembles de $\mathsf{k}[X_1, \ldots, X_n]$. Alors on a $V(S') \subset V(S)$.

Preuve. Exercice. ∎

Lemme 5.1.6 Soit $S \subset \mathsf{k}[X_1, \ldots, X_n]$. Notons $\langle S \rangle$ l'idéal engendré par S. On a $V(S) = V(\langle S \rangle)$.

Preuve. On a $S \subset \langle S \rangle$ et donc, d'après le Lemme 5.1.5, on obtient $V(\langle S \rangle) \subset V(S)$. Réciproquement, soit $x \in V(S)$ et $P \in \langle S \rangle$. Il existe des éléments $P_1, \ldots, P_r \in S$ et $Q_1, \ldots, Q_r \in \mathsf{k}[X_1, \ldots, X_r]$ tels que $P = P_1Q_1 + \ldots + P_rQ_r$. On en déduit

$$P(x) = P_1(x)Q_1(x) + \ldots + P_r(x)Q_r(x).$$

Comme $x \in V(S)$, on a $P_1(x) = \ldots = P_r(x) = 0$ et on en déduit $P(x) = 0$ *i.e* $x \in V(\langle S \rangle)$. ∎

Remarque Deux sous-ensembles de $\mathsf{k}[X_1, \ldots, X_n]$ peuvent définir les mêmes ensembles algébriques. Par exemple, on a

$$V(X) = V(X^2) = V(X^k)$$

pour tout $k \geq 1$.

5.2. Anneaux noethériens

Définition 5.2.1 Soit A un anneau et I un idéal.

1. L'idéal I est dit **finiment engendré**, s'il existe des éléments $a_1, \cdots, a_n \in A$ tels que $I = (a_1, \ldots, a_n)$.

2. Un anneau est dit **noethérien**, si tous ses idéaux sont finiment engendrés.

Exemple 1. Un anneau principal est noethérien.

2. En particulier, les anneaux $\mathbb{Z}$ et $\mathsf{k}[X]$ sont noethériens.

Proposition 5.2.3 Soit A un anneau commutatif. On a équivalence entre les propositions suivantes :

1. l'anneau est A noethérien ;
2. toute suite croissante d'idéaux $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ est stationnaire *i.e.* il exite un $N \in \mathbb{N}$ tel que $I_n = I_N$ pour tout $n \geq N$.
3. Toute famille non vide d'idéaux $(I_\lambda)_{\lambda \in \Lambda}$ a un élément maximal.

Preuve. (1. $\Rightarrow$ 2.) Soit $I = \bigcup_n I_n$. Alors I est un idéal. Comme A est noethérien, il existe des éléments $a_1, \ldots, a_k \in A$ tels que $I = (a_1, \ldots, a_k)$. Pour tout $i \in [1, k]$, il existe donc n_i tel que $a_i \in I_{n_i}$. Soit $N = \max_i\{n_i\}$, on a $a_i \in I_{n_i} \subset I_N$ pour tout i. On a donc $I = (a_1, \ldots, a_k) \subset I_N$ et $I = I_N$. On a donc $I_n \subset I = I_N$ pour tout n et $I_n = I_N$ pour tout $n \geq N$.

(2. $\Rightarrow$ 3.) Supposons que la famille $(I_\lambda)_{\lambda \in \Lambda}$ n'a pas d'élément maximal. On construit par récurrence une suite croissante non stationnaire d'idéaux. Soit $I_1 := I_{\lambda_1}$ un éléments de la famille. Coome il n'est pas maximal, il existe $\lambda_2 \in \Lambda$ tel que $I_1 \subsetneq I_2 := I_{\lambda_2}$. Si on a déjà construit $I_1 \subsetneq \ldots \subsetneq I_n$, comme I_n n'est pas maximal, il existe un $\lambda_{n+1} \in \Lambda$ tel que $I_n \subsetneq I_{n+1} := I_{\lambda_{n+1}}$.

(3. $\Rightarrow$ 1.) Soit I un idéal et $E = \{J \text{ finiment engendré avec } J \subset I\}$. Comme $(0) \subset E$, la famille E n'est pas vide et a donc un élément maximal J. Si $J \subsetneq I$, alors il existe un élément $a \in I$ tel que $a \notin J$. Alors l'idéal $J + (a)$ est de type fini et on a $J \subsetneq J + (a) \subset I$. Ceci contredit la maximalité de J, donc $J = I$ et I est finiment engendré. ∎

Exemple 3. L'anneau des polynômes $A = \mathsf{k}[X_1, \ldots, X_n, \ldots]$ avec un nombre infini d'indéterminées n'est pas noethérien. En effet, on a la suite croissante non stationnaire d'idéaux suivante : $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n) \subsetneq \ldots$

Théorème 5.2.5 Soit A un anneau noethérien. Alors $A[X]$ est aussi noethérien. □

Preuve. Soit I un idéal de $A[X]$ et soit

$$D = \{0\} \cup \{a \in A \mid \exists\ P \in I \text{ de coefficient dominant } a\}.$$

Montrons que D est un idéal de A. Soient $a, a' \in D$ avec $a + a' \neq 0$ et soit $b \in A$. Il existe des polynômes $P, Q \in I$ de coefficients dominants respectifs a et a'. Soit $k = \min(\deg P, \deg Q)$. Comme I est un idéal, on a $T = X^{\deg Q - k}P + X^{\deg P - k}Q \in I$ (on peut remarquer que $\deg(T) = \max(\deg(P), \deg(Q))$) et T a un coefficient égal à $a + a'$. On en déduit $a + a' \in D$. On a aussi $bP \in I$ qui a pour coefficient dominant ab, donc $ab \in D$ et D est un idéal.

Comme A est noethérien, l'idéal D est finiment engendré. Il existe donc des éléments $a_1, \ldots, a_r \in A$ tels que $D = (a_1, \ldots, a_r)$. Pour $i \in [1, r]$, soit $P_i \in I$ un polynôme dont le coefficient dominant est a_i et soit $d_i = \deg P_i$. Posons $d = \max(d_1, \ldots, d_r)$.

Pour $m \leq d$ nous définissons

$$D_m = \{0\} \cup \{a \in A \mid \exists\ P \in I \text{ avec } \deg(P) \leq m \text{ et de coefficient dominant } a\}.$$

Comme ci-dessus, on peut montrer que D_m est un idéal de A. Il est donc de type fini et on écrit $D_m = (b_{1,m}, \ldots, b_{r_m,m})$. Pour tout $m \leq d$ et tout $i \in [1, r_m]$, soit $Q_{i,m} \in I$ un polynôme tel que $\deg(Q_{i,m}) \leq m$ et de coefficient dominant $b_{i,m}$.

Nous montrons maintenant que I est engendré par les polynômes $P_1, \ldots, P_r$ et tous les polynômes $(Q_{i,m})_{m \leq d, i \in [1,r_m]}$. Soit I' l'idéal engendré par ces éléments. On a $I' \subset I$. Supposons que $I' \subsetneq I$ et soit $P \in I \setminus I'$ un Élément de degré minimal pour cette propriété.

Si on a $\deg P > d$, soit alors a son coefficient dominant. On a $a \in D$, donc on peut écrire $a = a_1 c_1 + \ldots + a_r c_r$ avec $c_1, \ldots, c_r \in A$. Le polynôme

$$T = X^{\deg P - d_1} c_1 P_1 + \ldots + X^{\deg P - d_r} c_r P_r$$

a donc a pour coefficient dominant. Si $T = P$, on a $P \in I'$ ce qui est absurde. Sinon, on a $P - T \in I \setminus I'$ avec $\deg(P - T) < \deg P$ ce qui cntredit la minimalité.

Si $\deg P = m \leq d$, soit toujours a son coefficient dominant. On a $a \in D_m$ et on peut écrire $a = b_{1,m} c_1 + \ldots + b_{r_m,m} c_{r_m}$ avec $c_1, \ldots, c_{r_m} \in A$ et le polynôme

$$T = X^{m - \deg Q_{1,m}} c_1 Q_{1,m} + \ldots X^{m - \deg Q_{r_m,m}} c_{r_m} Q_{r_m,m}$$

a pour coefficient dominant a. Si $T = P$, alors $P \in I'$ ce qui est absurde. Sinon, on a $P - T \in I \setminus I'$ avec $\deg(P - T) < \deg P$ ce qui contredit la minimalité. ∎

Corollaire Soit A un anneau noethérien. Alors $A[X_1, \ldots, X_n]$ est noethérien.

Corollaire L'aneau $\mathsf{k}[X_1, \ldots, X_n]$ est noethérien.

Corollaire Soit $V(S)$ un ensemble algébrique. Alors il existe des polynômes $P_1, \ldots, P_r \in \mathsf{k}[X_1, \ldots, X_r]$ tels ue

$$V(S) = V(P_1, \ldots, P_r).$$

Preuve. On a $V(S) = V(\langle S \rangle)$ et comme $\mathsf{k}[X_1, \ldots, X_n]$ est noethérien, l'idéal $\langle S \rangle$ est finiment engendré. Il existe donc $P_1, \ldots, P_r \in \mathsf{k}[X_1, \ldots, X_r]$ tels que $\langle S \rangle = (P_1, \ldots, P_r) = \langle \{P_1, \ldots, P_r\} \rangle$. On a donc $V(S) = V(P_1, \ldots, P_r)$. ∎

5.3. Premières propriétés

Lemme 5.3.1 Soit $(S_\lambda)_{\lambda \in \Lambda}$ une famille de sous-ensembles de $\mathsf{k}[X_1, \ldots, X_n]$ et soit $(I_\lambda)_{\lambda \in \Lambda}$ une famille d'idéaux de $\mathsf{k}[X_1, \ldots, X_n]$. Alors on a

$$\bigcap_{\lambda \in \Lambda} V(S_\lambda) = V\left(\bigcup_{\lambda \in \Lambda} S_\lambda \right) \text{ et } \bigcap_{\lambda \in \Lambda} V(I_\lambda) = V\left(\sum_{\lambda \in \Lambda} I_\lambda \right).$$

En particulier, une intersection quelconque d'ensembles algébriques est encore un ensemble algébrique.

Preuve. Exercice. ∎

Lemme 5.3.2 Soient I et J des idéaux de $\mathsf{k}[X_1, \ldots, X_n]$. On a alors

$$V(I \cap J) = V(I) \cup V(I) = V(IJ).$$

En particilier, une union de deux ensembles algébriques est encore un ensembles algébrique.

Preuve. On a $IJ \subset I \cap J \subset I, J$. On en déduit $V(IJ) \supset V(I \cap J) \supset V(I) \cup V(J)$. Il suffit donc de montrer l'inclusion $V(IJ) \subset V(I) \cup V(J)$.

Soit $x \in V(IJ)$ avec $x \notin V(I)$. Il existe alors $P \in I$ tel que $P(x) \neq 0$. Soit $Q \in J$, alors $PQ \in IJ$, donc $P(x)Q(x) = (PQ)(x) = 0$ (car $x \in V(IJ)$). Comme $P(x) \neq 0$, on en déduit $Q(x) = 0$ pour tout $Q \in J$ et donc $x \in V(J)$. ∎

Corollaire Soient $I_1, \ldots, I_r$ des idéaux de $\mathsf{k}[X_1, \ldots, X_n]$. Alors on a

$$V(I_1) \cup \ldots \cup V(I_r) = V(I_1 \cdots I_r) = V(I_1 \cap \cdots \cap I_r).$$

En particulier, une union finie d'ensembles algébriques est encore un ensemble algébrique.

Preuve. Par récurrence grâce au lemme précédent. ∎

Corollaire Tout sous-ensemble fini de $\mathbb{A}_n(\mathsf{k})$ est un ensemble algébrique.

Preuve. On a vu que tout point est un ensemble algébrique (Exemple 5.1.4.(2)). On conclue par le corollaire précédent. ∎

Définition 5.3.5 Soit $P \in \mathsf{k}[X_1, \ldots, X_n]$ tel que $P \neq 0$. L'ensemble algébrique $V(P)$ est appelé **hypersurface de $\mathbb{A}_n(\mathsf{k})$ d'équation** P.

Proposition 5.3.6 Tout ensemble algébrique est une intersection finie d'hypersurface de $\mathbb{A}_n(\mathsf{k})$.

Preuve. Soit $S \subset \mathsf{k}[X_1, \ldots, X_n]$ et $V(S)$ l'ensemble algébrique correspondant. D'après le Corollaire 5.2.8, il existe des polynômes $P_1, \ldots, P_r \in \mathsf{k}[X_1, \ldots, X_n]$ tels que $V(S) = V(P_1, \ldots, P_r)$. Par le Lemme 5.3.1, on a $V(S) = V(P_1) \cap \ldots \cap V(P_r)$ ce qui prouve le résultat. ∎

5.4. Idéal d'un ensemble

Définition 5.4.1 Soit V un sous-ensemble de $\mathbb{A}_n(\mathsf{k})$. **L'idéal de** V est l'ensemble

$$I(V) = \{P \in \mathsf{k}[X_1, \ldots, X_n] \mid P(x) = 0 \text{ pour tout } x \in V\}.$$

Lemme 5.4.2 Soit $V \subset \mathbb{A}_n(\mathsf{k})$. Alors $I(V)$ est un idéal de $\mathsf{k}[X_1, \ldots, X_n]$.

Preuve. Exercice. ∎

Exemple On a $I(\emptyset) = \mathsf{k}[X_1, \ldots, X_n]$.

Lemme 5.4.4 Si $V \subset W \subset \mathbb{A}_n(\mathsf{k})$, alors on a $I(V) \supset I(W)$.

Preuve. Exercice. ∎

Lemme 5.4.5 Soit $V \subset \mathbb{A}_n(\mathsf{k})$ et $I \subset \mathsf{k}[X_1, \cdots, X_n]$ un idéal.

1. On a $V \subset V(I(V))$.

2. On a $I \subset I(V(I))$.

3. On a $I(V) = I(V(I(V)))$.

4. On a $V(I) = V(I(V(I)))$.

Preuve. 1. Soit $x \in V$ et $P \in I(V)$. On a $P(x) = 0$ donc $x \in V(I(V))$. On en déduit $V \subset V(I(V))$.

2. Soit $P \in I$ et $x \in V(I)$. On a $P(x) = 0$ donc $P \in I(V(I))$. On en déduit $I \subset I(V(I))$.

3. Par 1., on a $V \subset V(I(V))$. Par le lemme précédent, on en déduit $I(V) \supset I(V(I(V)))$. Soit maintenant $P \in I(V)$ et soit $x \in V(I(V))$. On a $P(x) = 0$ et donc $P \in I(V(I(V)))$.

4. Par 2., on a $I \subset I(V(I))$. Par le lemme précédent, on en déduit $V(I) \supset V(I(V(I)))$. Soit maintenant $x \in V(I)$ et soit $P \in I(V(I))$. On a $P(x) = 0$ et donc $x \in V(I(V(I)))$. ∎

Lemme 5.4.6 Soit $V \subset \mathbb{A}_n(\mathsf{k})$, on a l'équivalence ($V$ est un ensemble algébrique $\Leftrightarrow$ $V(I(V)) = V$).

Preuve. Si V est algébrique, on a $V = V(I)$ et par le lemme précédent, on en déduit $V = V(I) = V(I(V(I)) = V(I(V))$.

Réciproquement, si $V = V(I(V))$ alors c'est un ensemble algébrique. ∎

Exemple 1. Si V n'est pas algébrique, on a pas l'égalité $V = V(I(V))$. Par exemple, soit

$$V = \{x \in \mathbb{R} = \mathbb{A}_1(\mathbb{R}) \mid 0 < x < 1\}.$$

Alors $I(V) = \{0\}$: un élément $P \in I(V) \subset \mathbb{R}[X]$ a une infinité de racines et est donc nul. Par contre, on a $V(I(V)) = \mathbb{A}_1(\mathbb{R}) = \mathbb{R} \supsetneq V$.

2. L'inclusion $I \subset I(V(I))$ est en général une inclusion stricte. Il y a deux raisons à celà :

(a) Si k n'est pas algébriquement clos, alors les ensembles algébriques ne "voient" pas toutes les solutions. Par exemple soit $\mathsf{k} = \mathbb{R}$ et $I = (X^2 + Y^2 + 1)$. On a $V(I) = V(X^2 + Y^2 + 1) = \emptyset$ et donc $I \subsetneq \mathbb{R}[X, Y] = I(V(I))$.

(b) L'opération $V(-)$ ne "voit" pas les puissances supérieures. Par exemple, soit $I = (X^2) \subset \mathsf{k}[X]$. On a $V(I) = \{0\}$ et $I(V(I)) = (X) \supsetneq (X^2) = I$.

Nous étudierons plus en détail le lien entre I et $I(V(I))$. Ce sera notamment le sujet des différents théorèmes des lieux d'annulation de Hilbert : les fameuse "Hilbert Nullstellensätze".

Proposition 5.4.8 Soit k un corps infini et soit $n \geq 1$. Alors on a $I(\mathbb{A}_n(\mathsf{k})) = (0)$.

Preuve. On procède par récurrence sur n. Pour $n = 1$, soit $P \in I(\mathbb{A}_1(\mathsf{k}))$. Comme k est infini, le polynôme P a une infinité de racines. On a donc $P = 0$.

Supposons le résultat vrai pour $n - 1$ variables. On considède P comme un polynôme en X_n et à coefficients dans $\mathsf{k}[X_1, \ldots, X_{n-1}]$:

$$P = \sum_i r_i X_n^i,$$

avec $r_i \in \mathsf{k}[X_1, \ldots, X_{n-1}]$. Soit $(a_1, \ldots, a_{n-1}) \in \mathsf{k}^{n-1}$. Alors on a un polynôme

$$P_{a_1,\ldots,a_{n-1}}(X_n) = P(a_1, \ldots, a_{n-1}, X_n) = \sum_i r_i(a_1, \ldots, a_{n-1}) X_n^i$$

dans $\mathsf{k}[X_n]$. Pour tout $a_n \in \mathsf{k}^n$, on a $P_{a_1,\ldots,a_{n-1}}(a_n) = P(a_1, \ldots, a_n) = 0$. Le polynôme est donc nul : $P_{a_1,\ldots,a_{n-1}} = 0$ *i.e.* $r_i(a_1, \ldots, a_{n-1}) = 0$ pour tout i et tout $(a_1, \ldots, a_{n-1}) \in \mathsf{k}^{n-1}$. On en déduit $r_i \in I(\mathbb{A}_{n-1}(\mathsf{k}))$ pour tout i. Par récurrence, on a $r_i = 0$ pour tout i et donc $P = 0$. ∎

Exemple L'énoncé précédent est faux pour un corps fini. En effet, soit $\mathsf{k} = \mathbb{F}_q$. On a $X^q - X \in I(\mathbb{A}_1(\mathsf{k}))$.

Exemple 1. Soit $a = (a_1, \ldots, a_n) \in \mathbb{A}_n(\mathsf{k})$. On a

$$I(\{a\}) = (X - a_1, \ldots, X - a_n).$$

L'inclusion $\supset$ est claire. Réciproquement, soit $P \in I(\{a\})$. On a $P \in \mathsf{k}[X_1, \ldots, X_n]$ et $P(a) = 0$. On considère la division euclidienne de P par $X - a_1$. On obtient $P = (X - a_1)Q_1 + R_1$ avec $R_1 \in \mathsf{k}[X_2, \ldots, X_n]$ et $0 = P(a) = R_1(a)$. Par récurrence, on obtient $P = Q + r$ avec $Q \in (X - a_1, \ldots, X - a_n)$ et $r \in \mathsf{k}$. Comme $P(a) = 0$ on obtient $r = 0$ et le résultat.

2. Soit k infini et soit $I = I(V(Y^2 - X^3)) \in \mathsf{k}[X, Y]$. On a $(Y^2 - X^3) \subset I$. Réciproquement, soit $P \in I$. On considère la division de P par $Y^2 - X^3$. Il existe

donc $Q, R \in \mathsf{k}[X,Y]$ avec $\deg_Y(R) < 2$ c'est-à-dire $R(X,Y) = A(X)Y + B(X)$ avec $A, B \in \mathsf{k}[X]$ tels que

$$P = (Y^2 - X^3)Q(X,Y) + A(X)Y + B(X).$$

Pour $t \in \mathsf{k}$, on a $(t^3, t^2) \in V(Y^2 - X^3)$. On en déduit $P(t^3, t^2) = 0$ et donc $A(t^2)t^3 + B(t^2) = 0$. En écrivant $A(X) = \sum_k a_k X^k$ et $B(X) = \sum_j b_j X^j$, on obtient

$$\sum_k a_k t^{2k+3} + \sum_j b_j t^{2j} = 0.$$

Comme k est infini, tous les coefficients doivent s'annuler : $a_k = 0$ et $b_j = 0$ pour tout k et tout j. On en déduit $A = B = 0$ et $P \in (Y^2 - X^3)$.

5.5. Fonctions régulières

Définition 5.5.1 Soit $V \subset \mathbb{A}_n(\mathsf{k})$. La k-algèbre $\Gamma(V) = \mathsf{k}[X_1, \ldots, X_n]/I(V)$ s'appelle **algèbre affine de** V ou encore **algèbre des fonctions régulières sur** V.

Proposition 5.5.2 Soit $V \subset \mathbb{A}_n(\mathsf{k})$, l'anneau $\Gamma(V)$ est réduit ou encore l'idéal $I(V)$ est radical, ou encore $I(V) = \sqrt{I(V)}$.

Preuve. Soit $P \in \mathsf{k}[X_1, \ldots, X_n]$ tel que $[P] \in \Gamma(V)$ est nilpotent. On a donc $P^n \in I(V)$ et donc $P^n(x) = 0$ pour tout $x \in V$. On en déduit $P(x) = 0$ pour tout $x \in V$ et donc $P \in I(V)$ *i.e.* $[P] = 0$. ∎

6. Topologie de Zariski

6.1. Définition

Remarque On peut définir une topologie d'un ensemble M en donnant la famille $\mathcal{T}$ des fermés de cette topologie. Il doivent alors vérifier les axiomes suivants :

(T1) Les ensembles $\emptyset$ et M sont des éléments de $\mathcal{T}'$,

(T2) une union finie d'éléments de $\mathcal{T}$ est encore un élément de $\mathcal{T}$,

(T3) une intersection quelconque d'éléments de $\mathcal{T}$ est encore dans $\mathcal{T}$.

Remarque Soit $\mathcal{T}$ la famille des ensembles algébriques de $\mathbb{A}_n(\mathsf{k})$. D'après l'Exemple 5.1.2, le Lemme 5.3.1 et le Corollaire 5.3.3, les trois axiomes (T1), (T2) et (T3) ci-desus sont vérifés et on a donc une topologie.

Définition 6.1.3 La topologie de Zariski de $\mathbb{A}_n(\mathsf{k})$ est la topologie dont les fermés sont les ensembles algébriques.

Définition 6.1.4 Soit V un sous-ensemble de $\mathbb{A}_n(\mathsf{k})$. **La topologie de Zariski sur** V est la topologie induite par la topologie de Zariski de $\mathbb{A}_n(\mathsf{k})$.

Remarque La topologie de Zariski est très différente de la topologie usuelle. Il y a beaucoup moins d'ouverts et de fermés et les ouverts sont très "gros".

Par exemple, d'arès le Lemme 5.1.3, les fermés de $\mathbb{A}_1(\mathbb{R}) = \mathbb{R}$ sont $\emptyset$, $\mathbb{R}$ et les ensembles finis. L'intervalle $]0, 1[$ n'est ni ouvert ni fermé.

Lemme 6.1.6 Soit $V \subset \mathbb{A}_n(\mathsf{k})$. Alors l'adhérence de V pour la topologie de Zariski est donnée par

$$\overline{V} = V(I(V)).$$

Preuve. On a $V \subset V(I(V))$ et comme $V(I(V))$ est algébrique, il est fermé. On a donc $\overline{V} \subset V(I(V))$. Soit maintenant Z fermé tel que $V \subset Z$. Alors on a $Z = V(I(Z))$ et $I(V) \supset I(Z)$. On en déduit $V(I(V)) \subset V(I(Z)) = Z$ et donc $V(I(V))$ est le plus petit fermé contenant V. ∎

Définition 6.1.7 Soit $P \in \mathsf{k}[X_1, \cdots, X_n]$. Le complémentaire de l'hypersurface $V(P)$ s'appelle **l'ouvert standard défini par** P et se note $D(P)$. On a donc

$$D(P) = \mathbb{A}_n(\mathsf{k}) \setminus V(P) = \{x \in \mathbb{A}_n(\mathsf{k}) \mid P(x) \neq 0\}.$$

Proposition 6.1.8 Un ouvert de la topologie de Zariski est une union finie d'ouverts standards.

Preuve. Soit U un ouvert. Alors $\mathbb{A}_n(\mathsf{k}) \setminus U$ est fermé et donc de la forme $V(S)$. Par le Corollaire 5.2.8, il existe des polynômes $P_1, \cdots, P_r \in \mathsf{k}[X_1, \cdots, X_n]$ tels que $V(S) = V(P_1, \cdots, P_r)$. Par le Lemme 5.3.1, on a $V(S) = V(P_1) \cap \cdots \cap V(P_r)$. On en déduit

$$\begin{aligned} U &= \mathbb{A}_n(\mathsf{k}) \setminus V(S) = \mathbb{A}_n(\mathsf{k}) \setminus (V(P_1) \cap \cdots \cap V(P_r)) \\ &= (\mathbb{A}_n(\mathsf{k}) \setminus V(P_1)) \cup \cdots \cup (\mathbb{A}_n(\mathsf{k}) \setminus V(P_r)) = D(P_1) \cup \cdots \cup D(P_r) \end{aligned}$$

et le résultat en découle. ∎

6.2. Irréductibilité

Lemme 6.2.1 Soit X un espace topologique. Les propositions suivantes sont équivalentes :

1. si $X = F_1 \cup F_2$ avec F_1 et F_2 fermé, alors $X = F_1$ ou $X = F_1$;
2. si U_1 et U_2 sont des ouvert de X tels que $U_1 \cap U_2 = \emptyset$, alors $U_1 = \emptyset$ ou $U_2 = \emptyset$.

Preuve. Il suffit de poser $U_i = F_i^c$ ou $F_i = U_i^c$ pour $i \in [1, 2]$. ∎

Définition 6.2.2 Soit X un espace topologique non vide.

Si X vérifie l'une des deux propositions équivalentes du lemme précédent, alors on dit que X est **irréductible**.

Si X n'est pas irréductible, on dit alors qu'il est **réductible**.

Exemple Pour la topologie usuelle sur $\mathbb{R}$, les sous-ensembles irréductibles sont les points (exercice).

Définition 6.2.4 Un espace topologique X est dit **connexe**, si on a l'implication

$$(U_1 \text{ et } U_2 \text{ ouverts tels que } U_1 \cup U_2 = X \text{ et } U_1 \cap U_2 = \emptyset) \Rightarrow (U_1 = \emptyset \text{ ou } U_2 = \emptyset).$$

Lemme 6.2.5 Si X est irréductible, alors il est connexe.

Preuve. Soient U_1 et U_2 ouverts tels que $U_1 \cup U_2 = X$ et $U_1 \cap U_2 = \emptyset$. Alors on a $U_1 = \emptyset$ ou $U_2 = \emptyset$. ∎

Définition 6.2.6 Soit X un espace topologique. Un sous-ensemble $Y \subset X$ est dit **dense** si on a $Y \cap U \neq \emptyset$ pour tout ouvert non vide U de X.

Proposition 6.2.7 Soit X un espace topologique irréductible et soit U un ouvert non vide. Alors U est dense et irréductible.

Preuve. Soit U' un autre ouvert non vide. Si $U \cap U' = \emptyset$, alors $U = \emptyset$ ou $U' = \emptyset$, une contradiction.

Soient U_1 et U_2 des ouverts de U tels que $U_1 \cap U_2 = \emptyset$. Alors ce sont aussi des ouverts de X tels que $U_1 \cap U_2 = \emptyset$. On a donc $U_1 = \emptyset$ ou $U_2 = \emptyset$. ∎

Proposition 6.2.8 Soit X un espace topologique et Y un sous-ensemble muni de la topologie induite.

1. Si Y est irréductible, alors son adhérence $\overline{Y}$ l'est aussi.

2. Soit U un ouvert de X. Alors l'es applications $Y \mapsto \overline{Y}$ et $Z \mapsto Z \cap U$ forment des bijections réciproques entre les ensembles $\{Y \subset U \mid Y \text{ fermé irréductible de } U\}$ et $\{Z \subset X \mid Z \text{ fermé irréductible de } X \text{ avec } Z \cap U \neq \emptyset\}$.

Preuve. 1. Soient F_1 et F_2 des fermés de $\overline{Y}$ tels que $F_1 \cup F_2 = \overline{Y}$. Par définition, il existe des fermés Z_1 et Z_2 de X tels que $F_i = Z_i \cap \overline{Y}$. On voit donc que F_1 et F_2 sont fermés dans X. Ainsi $F_1 \cap Y$ et $F_2 \cap Y$ sont fermés dans Y tels que $Y = Y \cap \overline{Y} = Y \cap (F_1 \cup F_2) = (Y \cap F_1) \cup (Y \cap F_2)$. Comme Y est irréductible, on a $F_1 \cap Y = Y$ ou $F_2 \cap Y = Y$ et donc $Y \subset F_1$ ou $Y \subset F_2$. On en déduit $\overline{Y} \subset \overline{F_1} = F_1$ ou $\overline{Y} \subset \overline{F_2} = F_2$ et donc $\overline{Y} = F_1$ ou $\overline{Y} = F_2$.

2. Soit $Y \subset U$ fermé et irréductible. Alors $\overline{Y}$ est fermé et irréductible et on a $\emptyset \neq Y \subset \overline{Y} \cap U$.

Soit Z fermé irréductible tel que $Z \cap U \neq 0$. Alors on a que $Y = Z \cap U$ est ouvert dans Z et fermé dans U, il est non vide et d'après la Proposition 6.2.7 il est irréductible.

Les applications ci-dessus sont donc bien définies. Il reste à voir qu'elles sont inverses l'une de l'autre.

Soit $Y \subset U$ fermé et irréductible. On a $Y \subset U \cap \overline{Y}$. Réciproquement, comme Y est fermé dans U, il existe un F fermé de X tel que $Y = F \cap U \subset F$. On a donc $\overline{Y} \subset F$ et $\overline{Y} \cap U \subset F \cap U = Y$. On en déduit $Y = \overline{Y} \cap U$.

Soit Z fermé irréductible de X tel que $Z \cap U \neq \emptyset$. On a $Z \cap U \subset Z$ et comme Z est fermé, on a $\overline{Z \cap U} \subset Z$. Soit $F = Z \setminus (Z \cap U)$. Alors F est fermé dans Z et on a $Z = F \cup \overline{Z \cap U}$. Comme Z est irréductible, on en déduit $F = \emptyset$ ou $\overline{Z \cap U} = \emptyset$. La seconde égalité n'étant pas possible, on a $F = \emptyset$ et $Z = \overline{U \cap Z}$. ∎

Proposition 6.2.9 Soit V un ensemble algébrique, on a les équivalences

$$V \text{ est irréductible } \Leftrightarrow I(V) \text{ est un idéal premier } \Leftrightarrow \Gamma(V) \text{ est un anneau intègre.}$$

Preuve. On a déjà vu que la seconde équivalence est vraie. Montrons la première.

Supposons V irréductible et soient $P_1, P_2 \in \mathsf{k}[X_1, \cdots, X_n]$ tels que $P_1 P_2 \in I(V)$. On pose $F_i = V(P_i) \cap V$ pour $i \in \{1, 2\}$. Les ensembles F_1 et F_2 sont fermés dans V. Soit $x \in V$, on a $P_1(x)P_2(x) = (P_1P_2)(x) = 0$ donc $P_1(x) = 0$ ou $P_2(x) = 0$. On a

donc $x \in V(P_1) = F_1$ ou $x \in V(P_2) = F_2$ *i.e.* $V = (V \cap F_1) \cup (V \cap F_2)$. On en déduit $V \subset F_1 \cup F_2$. mme V est irréductible, on a $V \subset F_1 = V(P_1)$ ou $V \subset F_2 = V(P_2)$. On a donc $P_1 \in I(V)$ ou $P_2 \in I(V)$.

Réciproquement, supposons que $I(V)$ est premier et soient F_1 et F_2 des fermés de V avec $V = F_1 \cup F_2$. Si on a $F_1 \subsetneq V$ et $F_2 \subsetneq V$, alors on a aussi $I(V) \subsetneq I(F_1)$ et $I(V) \subsetneq I(F_2)$ (sinon on aurait $V = V(I(V)) = V(I(F_i)) = F_i$ car ce sont des ensembles algébriques). Soient alors $P_i \in I(F_i) \setminus I(V)$ pour $i \in \{1, 2\}$. On a $P_1 P_2 \in I(F_1 \cup F_2) = I(V)$ et $P_i \notin I(V)$ pour $i \in \{1, 2\}$ ce qui contredit le fait que $I(V)$ est premier. ∎

Corollaire Si k est infini, alors $\mathbb{A}_n(\mathsf{k})$ est irréductible.

Preuve. On a $I(\mathbb{A}_n(\mathsf{k})) = (0)$ et $\Gamma(\mathbb{A}_1(\mathsf{k})) = \mathsf{k}[X_1, \cdots, X_n]$ est un anneau intègre. ∎

Exemple Pour k fini, l'espace affine $\mathbb{A}_n(\mathsf{k})$ est réductibe, c'est la rénion de ses points. Chaque point forme une "composante irréductible" (voir plus loin).

Corollaire (Prolongement des égalités algébriques) Soit k un corps infini et soit $V \subsetneq \mathbb{A}_n(\mathsf{k})$ un ensemble algébrique. Soit $P \in \mathsf{k}[X_1, \cdots, X_n]$ tel que $P(x) = 0$ pour $x \notin V$. Alors on a $P = 0$.

Preuve. On a $\mathbb{A}_n(\mathsf{k}) = V(P) \cup V$. Comme $\mathbb{A}_n(\mathsf{k})$ est irréductible et que $V \subsetneq \mathbb{A}_n(\mathsf{k})$ on doit avoir $V(P) = \mathbb{A}_n(\mathsf{k})$. ∎

Corollaire Soient $A, B \in M_n(\mathsf{k})$, on a $\chi_{AB} = \chi_{BA}$.

Preuve. Soit $P(A, B) = \chi_{AB} - \chi_{BA}$. C'est un polynôme en les coefficients de A et B. Pour B inversible, on a $\chi_{AB} = \chi_{B(AB)B^{-1}} = \chi_{BA}$ donc $P(A, B) = 0$ pour B inversible. Comme l'ensemble des paires (A, B) avec B non inversible est un fermé algébrique (c'est $V(\det(B))$, il est donné par l'annulation du polynôme en B : $\det(B)$), on en déduit $P = 0$. ∎

6.3. Composantes irréductibles

Définition 6.3.1 Un espace topologique X est dit **noethérien** si toute suite décroissante de fermés est stationnaire *i.e.* pour toute suite

$$Z_1 \supset Z_2 \supset \cdots \supset Z_r \supset \cdots$$

avec Z_r fermé, il existe un N tel que $Z_r = Z_N$ pour tout $r \geq N$.

Exemple Le corps $\mathbb{R}$ muni de la topologie usuelle n'est pas noethérien. En effet, la suite décroissante de fermés $[0, \frac{1}{n}]$ n'est pas stationnaire.

Lemme 6.3.3 L'espace affine $\mathbb{A}_n(\mathsf{k})$ muni de la topologie de Zariski est noethérien.

Preuve. Soit $Z_1 \supset Z_2 \supset \cdots \supset Z_r \supset \cdots$ une suite décroissante de fermés de $\mathbb{A}_n(\mathsf{k})$. Alors on a $Z_r = V(I(Z_r))$ et $I(Z_1) \subset I(Z_2) \subset \cdots \subset I(Z_r) \subset \cdots$ est une suite croissante d'idéaux de $\mathsf{k}[X_1, \cdots, X_n]$. Comme cet anneau est noehérien, il existe un N tel que $I(Z_r) = I(Z_N)$ pour $r \geq N$. On a donc $Z_r = V(I(Z_r)) = V(I(Z_N)) = Z_N$ pour $r \geq N$. ∎

Lemme 6.3.4 Soit X un espace topologique noethérien et soit $Y \subset X$. Alors Y est noethérien pour la topologie induite.

Preuve. Soit $Z_1 \supset Z_2 \supset \cdots \supset Z_r \supset \cdots$ une suite décroissante de fermé de Y. Pour tout r, il existe un fermé F_r de X tel que $Z_r = Y \cap F_r$. On pose $Z'_r = F_1 \cap \cdots \cap F_r$. Alors la suite $Z'_1 \supset Z'_2 \supset \cdots \supset Z'_r \supset \cdots$ est une suite décroissante de fermé de X. IL existe donc un N tel que $Z'_r = Z'_N$ pour $r \geq N$. On a donc

$$Z_r = Z_1 \cap \cdots \cap Z_r = (Y \cap F_1) \cap \cdots \cap (Y \cap F_r) = Y \cap (F_1 \cap \cdots \cap F_r) = Y \cap Z'_r.$$

On en déduit $Z_r = Y \cap Z'_r = Y \cap Z'_N = Z_N$. ∎

Corollaire Tout sous-ensemble de $\mathbb{A}_n(\mathsf{k})$ muni de la topologie de ariski est noethérien.

Définition 6.3.6 Soit X un espace topologique. Une **composante irréductible** de X est un fermé irréductible maximal de X.

Exemple 1. Soit k un corps fini et $V \subset \mathbb{A}_n(\mathsf{k})$. Alors les composantes irréductibles de V sont les points de V.

2. Soit k un corps infini et $V = V(XY) \subset \mathbb{A}_2(\mathsf{k})$. Alors les composantes irréductibles de V sont $V(X)$ et $V(Y)$. En effet, soit Z une composante irréductible. Comme Z est irréductible, fermé et maximal, on doit avoir que $I(V) \subset I(Z)$ et que $I(Z)$ est un idéal premier minimal pour cette propriété. On a donc $XY \in I(Z)$ et donc $(X) \subset I(Z)$ ou $(Y) \subset I(Z)$. Comme (X) et (Y) sont des idéaux premiers, on en déduit par minimalité $I(Z) = (X)$ ou $I(Z) = (Y)$ et donc $Z = V(X)$ ou $Z = V(Y)$.

Proposition 6.3.8 Soit $X \neq \emptyset$ un espace topologique noethérien. Alors X est union finie de ses composantes irréductibles $X_1, \cdots, X_r$:

$$X = X_1 \cup \cdots \cup X_r.$$

Preuve. Pour tout sous-ensemble Y de X, on dit que Y vérifie (P) si Y est union finie de fermés iréductibles. Il nous siffit de montrer que X vérifie (P).

Soit $M = \{Y \subset X \mid Y \text{ est non vide, fermé et ne vérifie pas (P)}\}$. Nous allons montrer que M est vide. Supposons que M n'est pas vide. Comme X est noethérien, l'ensemble M admet un élément minimal. En ffet, sinon, on choisit $Z_1 \in M$. Si Z_1 est minimal, on a fini. Sinon, il existe un $Z_2 \subsetneq Z_1$ tel que $Z_2 \in M$. On procède par récurrence. Un

des éléments Z_r ainsi construits doit ître minimal sinon, on a construit une chaine $Z_1 \supset \cdots \supset Z_r \supset \cdots$ non stationnaire.

Soit donc Z minimal dans M. On a $Z \neq \emptyset$ et Z n'est pas irréductible. Il existe donc deux fermés propres F_1 et F_2 de Z tels que $Z = F_1 \cup F_2$. Part minimalité, on a $F_1, F_2 \notin M$ donc F_1 (resp. F_2) est union finie de fermés irréductibles. La même chose est aussi valable pour Z, une contradiction puisque Z ne vérifie pas (P).

Il existe donc un nombre fini de fermés irréductibles $X_1, \cdots, X_r$ de X tels que $X = X_1 \cup \cdots \cup X_r$. Montrons que tout sous-ensemble irréductible de X est contenu dans l'un des X_i. On a

$$Y = Y \cap Y = Y \cap (X_1 \cup \cdots \cup X_r) = (Y \cap X_1) \cup \cdots \cup (Y \cap X_r).$$

Comme tous les $Y \cap X_i$ sont fermés dans Y et que Y est irréductible, il existe un i tel que $Y \subset X_i$. Les éléments maximaux de la famille $(X_i)_{i\in[1,r]}$ sont donc les composantes irréductibles de X. ∎

Corollaire Tout ensemble algébrique a un nombre fini de composantes irréductibles.

Preuve. Comme $V \subset \mathbb{A}_n(\mathsf{k})$ et que $\mathbb{A}_n(\mathsf{k})$ est noethérien, on a le résultat. ∎

6.4. Espaces compacts et séparés

Définition 6.4.1 Un espace topologique X est dit **séoaré ou de Hausdorff** si pour tout $x, x' \in X$ avec $x \neq x'$, il existe des voisinages ouverts U et U' de x et x' tels que $U \cap U' = \emptyset$.

Lemme 6.4.2 Soit V un ensemble algébrique contenant un nombre infini de points. Alors V n'est pas séparé.

Preuve. Comme V n'a qu'un nombre fini de composantes irréductibles, on peut sans restriction supposer que V est irréductible. Soient $x, x' \in V$ avec $x \neq x'$. Si U et U' sont des voisinages de x et x', alors ils sont non vides et ouverts. Ils doivent donc se rencontrer ce qui rend l'égalité $U \cap U' = \emptyset$ impossible. ∎

Exemple Si V est fini, alors chaque point est ouvert et fermé et V est séparé.

Définition 6.4.4 Soit X un espace topologique.

1. Si de tout recouvrement ouvert $(U_\lambda)_{\lambda\in\Lambda}$ on peut extraire un sous-recouvrement fini $(U_{\lambda_i})_{i\in[1,r]}$, alors on dit que X est **quasi-compact**.

2. Si X est séparé et quasi-compact, il est dit **compact**.

Lemme 6.4.5 Un espace topologiue est quasi-compact si et seulement si pour toute famille de fermés $(F_\lambda)_{\lambda\in\Lambda}$ tels que

$$\bigcap_{\lambda\in\Lambda} F_\lambda = \emptyset,$$

il existe une sous-famille finie $(F_{\lambda_i})_{i\in[1,r]}$ telle que

$$\bigcap_{i=1}^{r} F_{\lambda_i} = \emptyset.$$

Preuve. Il suffit de poser $U_\lambda = F_\lambda^c$. ∎

Définition 6.4.6 Soit $V \subset \mathbb{A}_n(\mathsf{k})$ et soit $P \in \mathsf{k}[X_1, \cdots, X_n]$. Les ouverts $D_V(P) = D(P) \cap V$ sont appelés **ouverts standards de** V.

Proposition 6.4.7 Soit V un ensemble algébrique.

1. Tout ouvert de V est union finie d'ouverts standards.

2. L'espace topologique V est quasi-compact.

Preuve. 1. Soit U un ouvert de V et U' un ouvert de $\mathbb{A}_n(\mathsf{k})$ tel que $U = V \cap U'$. Il existe des polynômes $P_1, \cdots, P_r$ tels que $U' = D(P_1) \cup \cdots \cup D(P_r)$ et on a donc $U = D_V(P_1) \cup \cdots \cup D_V(P_r)$.

2. Soit $(U_\lambda)_{\lambda\in\Lambda}$ une famille d'ouverts de V telle que

$$\bigcup_{\lambda\in\Lambda} U_\lambda = V.$$

D'après 1., on peut supposer que tous les U_λ sont des ouverts standards donc $U_\lambda = D_V(P_\lambda)$ avec $P_\lambda \in \mathsf{k}[X_1, \cdots, X_n]$. Soit $I = (P_\lambda \mid \lambda \in \Lambda)$. Comme $\mathsf{k}[X_1, \cdots, X_n]$ est noethérien, il existe une sous-familles $P_{\lambda_1}, \cdots, P_{\lambda_r}$ telle que $I = (P_{\lambda_1}, \cdots, P_{\lambda_r})$.

Montrons que $V = D_V(P_{\lambda_1}) \cup \cdots \cup D_V(P_{\lambda_r})$. Soit $x \in V \setminus (D_V(P_{\lambda_1}) \cup \cdots \cup D_V(P_{\lambda_r}))$. On a $P_{\lambda_i}(x) = 0$ pour tout $i \in [1, r]$. Mais il existe au moins un indice $\lambda \in \Lambda$ tel que $P_\lambda(x) \neq 0$. Comme $P_\lambda \in I$, il existe des polynômes $Q_1, \cdots, Q_r$ tels que $P_\lambda = \sum_{i=1}^r Q_i P_{\lambda_i}$. On obtient $P_\lambda(x) = 0$, une contradiction. ∎

Exemple Soir $X = \mathbb{R}$.

1. X est séparé mais pas quasi-compact pour la topologie usuelle.

2. X n'est pas séparé mais est quasi-compact pour la topologie de Zariski.

7. Nullstellensatz

7.1. Version algébrique

Théorème 7.1.1 (Nullstellensatz 1) Soit k un corps et soit A une algèbre de type fini sur k. Si A est un corps, alors c'est une extension algébrique de k. □

Preuve. Soient $(x_1, \cdots, x_r)$ des générateurs de A. Nous montrons le résultat par récurrence sur r. Si $r = 0$, on a $A = \mathsf{k}$ et le résultat est vrai. Supposons donc $r \geq 1$ et posons $K = \mathsf{k}(x_1)$. Alors A est une K-algèbre et c'est un corps. De plus $(x_2, \cdots, x_r)$ engendrent A sur K. Par récurrence, on a donc que A est une extension algébrique de K. Il existe donc des polynômes $P_2, \cdots, P_r \in K[X]$ de coefficient dominant 1 telq que $P_i(x_i) = 0$ pour tout $i \in [2, r]$. Les coefficients de ces polynômes sont de la forme $\frac{Q(x_1)}{R(x_1)}$ avec $Q, R \in \mathsf{k}[X]$. Soit F le produit de tous les dénominateurs de tous les coefficients des P_i. On pose $a' = \frac{1}{F(x_1)}$ et $A' = \mathsf{k}[x_1, a']$ la sous-algèbre de A engendrée par x_1 et a'. On a alors $P_i \in A'[X]$ pour tout $i \in [2, r]$. Comme $P_i(x_i) = 0$, les éléments x_i sont entiers sur A'. Comme $(x_2, \cdots, x_n)$ engendre A, l'algèbre A' est entière sur A. Comme A est un corps, il en est de même de A'.

Nous utilisons ce fait pour montrer que x_1 est algébrique sur k. Sinon, il est transcendant et on a $A' = \mathsf{k}[x_1, a'] = \mathsf{k}[x_1, \frac{1}{F(x_1)}]$. Montrons que $x = 1 + x_1F(x_1)$ n'a pas d'inverse dans A' (ce qui sera une contradiction puisque A' est un corps. Soit y un inverse dans A', alors il est de la forme

$$y = \frac{P(x_1)}{F(x_1)^m},$$

avec $P \in \mathsf{k}[X]$ et $m \in \mathbb{N}$. Soit m minimal pour qu'une telle expression exist. On a

$$1 = xy = (1 + x_1F(x_1))\frac{P(x_1)}{F(x_1)^m}.$$

Après multiplication par $F(x_1)^m$, on a $(P(X)(1 + F(X)) - F(X)^m)(x_1) = P(x_1)(1 + x_1F(x_1)) - F(x_1)^m = 0$. Comme x_1 est transcendent, on obtient $P(X)(1+XF(X)) = F(X)^m$. Puisque $F(X)$ et $1 + XF(X)$ sont premiers entre eux, on obtient que $F(X)$ doit diviser $P(X)$. Il existe donc un $Q \in \mathsf{k}[X]$. tel que $P(X) = F(X)Q(X)$. On a alors

$$y = \frac{P(x_1)}{F(x_1)^m} = \frac{F(x_1)P(x_1)}{F(x_1)^m} = \frac{Q(x_1)}{F(x_1)^{m-1}},$$

ce qui contredit la minimalité de m.

L'élément x_1 est donc algébrique sur k et l'extension $\mathsf{k} \subset K = \mathsf{k}(x_1)$ est algébrique. Mais on a vu que l'extension $K \subset A$ est aussi algébrique, on a donc que l'extension $\mathsf{k} \subset A$ est algébrique. ∎

7.2. Versions géométriques

Théorème 7.2.1 (Nulstellensatz 2) Soit k un corps algébriquement clos. Les idéaux maximaux de $\mathsf{k}[X_1, \cdots, X_n]$ sont de la forme $(X_1 - a_1, \cdots, X_n - a_n)$ avec $(a_1, \cdots, a_n) \in \mathbb{A}_n(\mathsf{k})$. □

Preuve. Soit $\mathfrak{M} = (X_1 - a_1, \cdots, X_n - a_n)$ et soit $f : \mathsf{k}[X_1, \cdots, X_n] \to \mathsf{k}$ défini par $f(P) = P(a_1, \cdots, a_n)$. Alors f est un morphise de k-algèbres et est surjectif. Par ailleurs, on a $\mathfrak{M} \subset \mathrm{Ker}(f)$ et on peut factoriser f par $\bar{f} : \mathsf{k}[X_1, \cdots, X_n]/\mathfrak{M} \to \mathsf{k}$ tel que $\bar{f}([P]) = f(P) = P(a_1, \cdots, a_n)$. Si maintenant $P \in \mathrm{Ker}(f)$. En faisant la division euclidienne par $X_1 - a_1$ puis $X_2 - a_2, \cdots, X_n - a_n$ on obtient

$$P = (X_1 - a_1)Q_1(X_1, \cdots, X_n) + \cdots (X_n - a_n)Q_n(X_1, \cdots, X_n) + \lambda.$$

Comme $P \in \mathrm{Ker}(f)$, on a doit avoir

$$0 = P(a_1, \cdots, a_n) = \lambda.$$

On en déduit $P \in \mathfrak{M}$ et $\mathrm{Ker}(f) = \mathfrak{M}$. On voit donc que $\mathsf{k}[X_1, \cdots, X_n]/\mathfrak{M} \simeq \mathsf{k}$ et $\mathfrak{M}$ est maximal.

Réciproquement, si $\mathfrak{M}$ est maximal, soit $A = \mathsf{k}[X_1, \cdots, X_n]/\mathfrak{M}$. Alors A est une k-algèbre de type fini et c'est un corps. Par le Nullstellensatz 1, l'extenskion $\mathsf{k} \subset A$ est algébrique. Mais comme k est algébriquement clos, on a $A = \mathsf{k}$. On pose alors $a_i = [X_i] \in A = \mathsf{k}$. On a $[X_i - a_i] = [X_i] - a_i = 0$ donc $X_i - a_i \in \mathfrak{M}$. On a alors $(X_1 - a_1, \cdots, X_n - a_n) \subset \mathfrak{M}$. Comme $(X_1 - a_1, \cdots, X_n - a_n)$ est maximal, on obtient $(X_1 - a_1, \cdots, X_n - a_n) = \mathfrak{M}$. ∎

Exemple Si k n'est pas algébriquement clos, le résultat n'est plus vrai. Par exemple, on a $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$ et $(X^2 + 1)$ est un idéal maximal mais n'est pas de la forme $(X - a) = I(a)$ quelque soit $a \in \mathbb{R} = \mathbb{A}_1(\mathbb{R})$.

Corollaire (Nulstellensatz 3) Soit k algébriquement clos et soit $I \subsetneq \mathsf{k}[X_1, \cdots, X_n]$ un idéal propre. On a $V(I) \neq \emptyset$.

Preuve. Soit $I \subsetneq \mathsf{k}[X_1, \cdots, X_n]$ et soit $\mathfrak{M}$ un idéal maximal tel que $I \subset \mathfrak{M} \subset \mathsf{k}[X_1, \cdots, X_n]$. On a $V(\mathfrak{M}) \subset V(I)$. Par le Nullstellensatz 2, on a $I = (X_1 - a_1, \cdots, X_n - a_n)$. On en déduit $V(I) \supset \{(a_1, \cdots, a_n)\} \neq \emptyset$. ∎

Exemple Si k n'est pas algébriquement clos, le résultat n'est plus vrai. Par exemple, on a $\mathsf{k} = \mathbb{R} : V(X^2 + Y^2 + 1) = \emptyset$.

Corollaire (Nulstellensatz 4) Soit k un corps algébriquement clos et soit $I \subset \mathsf{k}[X_1, \cdots, X_n]$ un idéal. Alors on a

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

Preuve. Soit $P \in \sqrt{I}$. Il existe r tel que $P^r \in I$. Comme $I \subset I(V(I))$, on a $P^r \in I(V(I))$ et donc $P \in \sqrt{I(V(I))}$. Mais $I(V(I)) = \sqrt{I(V(I))}$ donc $P \in I(V(I))$.

Réciproquement, comme $\mathsf{k}[X_1, \cdots, X_n]$ est noethérien, il existe $P_1, \cdots, P_r$ dans l'anneau $\mathsf{k}[X_1, \cdots, X_n]$ tels que $I = (P_1, \cdots, P_r)$. Soit $P \in I(V(I))$, on définit un idéal dans l'anneau $\mathsf{k}[X_1, \cdots, X_n, X_{n+1}]$ des polynômes avec une variable de plus par $J = (P_1, \cdots, P_r, 1 - X_{n+1}P)$. Soit $V = V(J) \subset \mathbb{A}_{n+1}(\mathsf{k})$ et soit $x \in V$. On a $P_1(x) = \cdots = P_r(x) = 0$ et donc $P(x) = 0$. On a aussi $1 - x_{n+1}P(x) = 0$ et donc $1 = 0$, une contradiction. On a donc $V = \emptyset$. Par le Nullstellensatz 3, on a $J = \mathsf{k}[X_1, \cdots, X_n, X_{n+1}]$. En particulier, on a $1 \in J$ et il existe des polynômes $Q_1, \cdots, Q_r, Q_{r+1}$ de $\mathsf{k}[X_1, \cdots, X_n, X_{n+1}]$ tels que

$$1 = P_1Q_1 + \cdots + P_rQ_r + (1 - X_{n+1}P)Q_{r+1}.$$

On pose $X_{n+1} = \frac{1}{P}$. On a alors

$$1 = P_1(X_1, \cdots, X_n)Q_1(X_1, \cdots, X_n, \frac{1}{P}) + \cdots + P_r(X_1, \cdots, X_n)Q_r(X_1, \cdots, X_n, \frac{1}{P}).$$

On écrit Q_i comme polynôme en X_{n+1}. On a $Q_i = \sum_{k=0}^{d_i} R_{i,k}X_{n+1}^k$ avec $R_{i,k} \in \mathsf{k}[X_1, \cdots, X_n]$. On a donc

$$Q_i(X_1, \cdots, X_n, \frac{1}{P}) = \sum_{k=0}^{d_i} \frac{R_{i,k}}{P^k}.$$

Soit $d = \max(d_i)$, on a $P^dQ_i(X_1, \cdots, X_n, \frac{1}{P}) \in \mathsf{k}[X_1, \cdots, X_n]$ pour tout i et on obtient

$$\begin{aligned} P^d = \; & P_1(X_1, \cdots, X_n)P^dQ_1(X_1, \cdots, X_n, \tfrac{1}{P}) + \cdots + \\ & + P_r(X_1, \cdots, X_n)P^dQ_r(X_1, \cdots, X_n, \tfrac{1}{P}) \in (P_1, \cdots, P_r) = I. \end{aligned}$$

On en déduit $P \in \sqrt{I}$. ∎

Exemple Si k n'est pa algébriquement clos, le résultat n'est plus vrai. Par exemple, on a pour $\mathsf{k} = \mathbb{R}$ et $I = (X^2 + Y^2 + 1)$, les égalités $V(I) = \emptyset$ et donc $I(V(I)) = \mathsf{k}[X, Y] \supsetneq \sqrt{I} = I$.

7.3. Conséquences géométriques

Proposition 7.3.1 Soit k un corps algébriquement clos.

Il existe un bijection décroissante (contravariante) définie par $V \mapsto I(V)$ d'application réciproque $I \mapsto V(I)$ entre l'ensemble {ensembles algébriques de $\mathbb{A}_n(\mathsf{k})$} et l'ensemble {I idéal radical de $\mathsf{k}[X_1, \cdots, X_n]$}.

De plus on a

1. V irréductible $\Leftrightarrow$ $I(V)$ premier $\Leftrightarrow$ $\Gamma(V)$ intègre.
2. V a un seul élément $\Leftrightarrow$ $I(V)$ est maximal $\Leftrightarrow$ $\Gamma(V) = \mathsf{k}$.

Preuve. Si V est un ensemble algébrique, on a $V(I(V)) = V$. Si I est un idéal radical, on a par la Nullstellensatz 4 : $I(V(I)) = \sqrt{I} = I$.

1. Voir la Proposition 6.2.9.

2. Soit V un ensemble avec un unique élément et soit I un idéal tel que $I(V) \subset I$. On a $V(I) \subset V(I(V)) = V$. En particulier, $V(I) = V$ ou $V(I) = \emptyset$. Dans le premier cas, on a par le Nullstellensatz 4 : $I(V) = I(V(I)) = \sqrt{I}$ et donc $I \subset I(V)$ et $I = I(V)$. Dans le second cas, on a par le Nullstelensatz 3 : $I = \mathsf{k}[X_1, \cdots, X_n]$. On a donc que $I(V)$ est maximal.

Si V est tel que $I(V)$ est maximal, alors $\Gamma(V)$ est un corps, c'est aussi une k-algèbre de type finie et par le Nullstellensatz 1, on voit que l'extension $\Gamma(V)$ de k est algébrique. Comme k est algebriquement clos, on en déduit $\Gamma(V) = \mathsf{k}$.

Si maintenant $\Gamma(V) = \mathsf{k}$, alors $I(V)$ est un idéal maximal et par le Nullstellensatz 2, on a $I(V) = (X_1 - a_1, \cdots, X_n - a_n)$ pour un $(a_1, \cdots, a_n) \in \mathbb{A}_n(\mathsf{k})$. On en déduit $V = V(I(V)) = \{(a_1, \cdots, a_n)\}$. ∎

Plus généralement, on montre le résultat suivant.

Proposition 7.3.2 Soit k algébriquement clos et soit $V \subset \mathbb{A}_n(\mathsf{k})$ un ensemble algébrique. On a l'équivalence

$$V \text{ est fini } \Leftrightarrow \Gamma(V) \text{ est un espace vectoriel de dimension finie.}$$

Preuve. ($\Rightarrow$). Soit $V = \{v_1, \cdots, v_r\}$ et soit $f : \mathsf{k}[X_1, \cdots, X_n] \to \mathsf{k}^r$ définie par $f(P) = (P(v_1), \cdots, P(v_r))$. On a

$$\begin{aligned} \mathrm{Ker}(f) &= \{P \in \mathsf{k}[X_1, \cdots, X_n] \mid P(v_i) = 0 \text{ pour tout } i \in [1, r]\} \\ &= I(V). \end{aligned}$$

En particulier, f se factorise par $\bar{f} : \Gamma(V) = \mathsf{k}[X_1, \cdots, X_n] \to \mathsf{k}^r$ qui est injective. On a donc $\dim_{\mathsf{k}} \Gamma(V) \leq \dim_{\mathsf{k}} \mathsf{k}^r = r$.

($\Leftarrow$). Soit $[X_i]$ la classe de X_i dans $\Gamma(V)$. Comme $\Gamma(V)$ est de dimension finie, la famille $([1], [X_i], \cdots, [X_i^r], \cdots)$ est liée. Pour tout $i \in [1, n]$, il existe donc des scalaires $a_{i,j}$ tels que

$$a_{i,d_i}[X_i^{d_i}] + a_{i,d_i-1}[X_i^{d_i-1}] + \cdots + a_{i,0}[1] = 0$$

et $a_{i,d_i} \neq 0$. On a alors $P_i = a_{i,d_i}X_i^{d_i} + a_{i,d_i-1}X_i^{d_i-1} + \cdots + a_{i,0}1 \in I(V)$. Si $x = (x_1, , \cdots, x_n) \in V$, alors $P_i(x) = 0$ et donc x_i est une racine de P_i. Il n'existe qu'un nombre fini de telles racines ce qui impose $|V| < \infty$. ∎

Définition 7.3.3 Soit A un anneau.

1. Un élément $r \in A$ est dit **idempotent** si on a $r^2 = r$. Un idempotent est dit **trivial** si $r = 0$ ou $r = 1$.

2. L'anneau A est dit **connexe** si ses seuls éléments idempotents sont triviaux.

Lemme 7.3.4 Un anneau est non connexe si et seulement si il est produit $A_1 \times A_2$ de deux anneaux non nuls. □

Preuve. Si $A = A_1 \times A_2$ avec $A_1 \neq 0 \neq A_2$, alors on pose $r = (1, 0)$. On a $1 \neq r \neq 0$ mais $r^2 = r$ donc l'anneau n'est pas connexe.1.

Réciproquement, soit r un idempotent non trivial. Alors $0 \neq r \neq 1$ et on pose $r' = 1-r$. Le lemme Chinois nous donne alors l'isomorphisme $A \simeq A/(r) \times A/(1-r)$. ∎

Proposition 7.3.5 Soit k un corps algébriquement clos. Un ensemble algébrique $V \subset \mathbb{A}_n(\mathsf{k})$ est connexe si et seulement si $\Gamma(V)$ est connexe.

Preuve. Supposons que V n'est pas connexe et soient V_1 et V_2 des unions de composantes connexes de V telles que $V = V_1 \cup V_2$ et $V_1 \cap V_2 = \emptyset$. Ce sont des fermés de V et sont donc des ensembles algébriques. Par ailleurs, on a $V_1 \cap V_2 = \emptyset$ donc par le Nullstellensatz 3, on a $I(V_1) + I(V_2) = I(V_1 \cap V_2) = \mathsf{k}[X_1, \cdots, X_n]$. Il existe donc $P \in I(V_1)$ et $Q \in I(V_2)$ tels que $P + Q = 1$. On pose $r = [P] \in \Gamma(V)$. On a pour $x \in V$ l'alternative (exclusive) $x \in V_1$ ou $x \in V_2$. Dans le premier cas, on a $P(x) = 0$. Dans le second cas, on a $P(x) = 1 - Q(x) = 1$ et $P(x) = 1$. Dans tous les cas $P(x)^2 = P(x)$ donc $P^2 - P \in I(V)$ ce qui impose $r^2 = r$. Mais $r(x) = 0$ pour $x \in V_1$ et $r(x) = 1$ pour $x \in V_2$ donc r est un idempotent non trivial.

Réciproquement, si $\Gamma(V)$ a un idempotent non trivial r. Soit P un polynôme tel que $r = [P]$ et posons $Q = 1 - P$. On considère $V_1 = V(P) \cap V$ et $V_2 = V(Q) \cap Q$. On voit que si $x \in V_1 \cap V_2$, alors $P(x) = 0$ et $Q(x) = 0$. Mais $1 = P(x) + Q(x) = 0$, une contradiction donc x ne peut exister et $V_1 \cap V_2 = \emptyset$. Si $x \in V$, alors comme $r^2 = r$, on a $P^2 - P \in I(V)$ et donc $P^2(x) - P(x) = 0$. On en déduit $P(x) = 0$ ou $P(x) = 1$ c'est-à-dire $P(x) = 0$ ou $Q(x) = 0$. On a donc $x \in V_1 \cup V_2$ donc $V = V_1 \cap V_2$. Comme r n'est pas trivial, on a $P \in I(V)$ et $Q = 1 - P \notin I(V)$ donc il existe $x \in V$ tel que $P(x) \neq 0$ et $x' \in V$ tel que $Q(x') \neq 0$. On a alors $x \in V \setminus V_1$ et $x' \in V \setminus V_2$. Ainsi V_1 et V_2 sont non vides et V n'est pas connexe. ∎

Définition 7.3.6 Soit V un ensemble algébrique et soit $W \subset V$ un fermé. **L'idéal de W dans V** est l'image de $I(W)$ dans $\Gamma(V)$ par l'application canonique $p_V : \mathsf{k}[X_1, \cdots, X_n] \to \Gamma(V)$.

Remarque On a $I(W) = p_V^{-1}(I_V(W))$. En particulier, on a

1. $I_V(W) = \{f \in \Gamma(V) |\ f(x) = 0 \text{ pour tout } x \in W\}$.
2. $\Gamma(W) \simeq \Gamma(V)/I_V(W)$.

On a donc

3. $I_V(W)$ est radical.
4. $I_W(V)$ premier $\Leftrightarrow$ $I(V)$ premier
5. $I_W(V)$ maximal $\Leftrightarrow$ $I(V)$ maximal.

Proposition 7.3.8 Soit k un corps algébriquement clos et soit $V \subset \mathbb{A}_n(\mathsf{k})$ un ensemble algébrique.

1. Il existe une bijection décroissante (contravariante) $V \mapsto I_V(W)$ d'appllication réciproque $I \mapsto V(p_V^{-1}(I))$ entre les ensembles {sous-ensemble algébriques de V} et {I idéal radical de $\Gamma(V)$}.

De plus on a

2. W irréductible $\Leftrightarrow$ $I_V(W)$ premier $\Leftrightarrow$ $\Gamma(W)$ intègre.
3. W a un seul élément $\Leftrightarrow$ $I_V(W)$ maximal $\Leftrightarrow$ $\Gamma(W) = \mathsf{k}$.
4. W est fini $\Leftrightarrow$ $\dim_{\mathsf{k}} \Gamma(W) < \infty$.
4. W est connexe $\Leftrightarrow$ $\Gamma(W)$ est connexe.

Preuve. On a une bijection

$$\{W \subset \mathbb{A}_n(\mathsf{k}) \mid W \text{ algébrique } \} \leftrightarrow \{I(W) \mid I(W) \text{ radical}\}.$$

On peut restreindre cette bijection à

$$\{W \subset V \mid W \text{ algébrique } \} \leftrightarrow \{I(W) \supset I(V) \mid I(W) \text{ radical } \}.$$

Comme on a ($I(W)$ radical $\Leftrightarrow$ $I_V(W)$ radical), on obtient une bijection

$$\{I(W) \supset I(V) \mid I(W) \text{ radical } \} \leftrightarrow \{I_V(W) \subset \Gamma(V) \mid I_V(W) \text{ radical } \}.$$

On en déduit les assertions 2,3,4 et 5. ∎

Corollaire Soit V un ensemble algébrique. On a des bijections

$$V \leftrightarrow \{\text{idéaux maximaux de } \Gamma(V)\} \leftrightarrow \mathrm{Hom}_{\mathsf{k}-\mathrm{Alg}}(\Gamma(V), \mathsf{k}).$$

Remarque L'ensemble $\mathrm{Hom}_{\mathsf{k}-\mathrm{Alg}}(\Gamma(V), \mathsf{k})$ est l'ensemble des morphismes de k-algèbres. En particulier, pour $f \in \mathrm{Hom}_{\mathsf{k}-\mathrm{Alg}}(\Gamma(V), \mathsf{k})$ on a $f(1) = 1$ et f n'est pas nulle.

Définition 7.3.11 Soit $v \in V$. On écrira $\mathfrak{M}_v$ pour l'idéal maximal de $\Gamma(V)$ défini par $\mathfrak{M}_v = I_V(\{v\})$.

8. Morphismes

Définition 8.0.1 Soient $V \subset \mathbb{A}_n(\mathsf{k})$ et $W \subset \mathbb{A}_m(\mathsf{k})$ des ensembles algébriques et soit $\varphi : V \to W$ une application.

1. L'appllication φ est de la forme $\varphi = (\varphi_1, \cdots, \varphi_m)$ avec $\varphi_i : V \to \mathsf{k}$ pour tout $i \in [1, m]$. Les applications φ_i sont **les composantes de** φ

2. L'application φ est dite **regulière** s'il existe $[P_i] \in \Gamma(V)$ tel que $\varphi_i(x) = P_i(x)$ pour tout $i \in [1, r]$ et tout $x \in V$.

3. L'ensemble des applications régulières de V dans W est noté $\mathrm{Reg}(V, W)$.

4. Une application régulière $\varphi : V \to W$ est appelé **isomorphisme** s'il existe une application régulière $\psi : W \to V$ telle que $\varphi \circ \psi = \mathrm{Id}_W$ et $\psi \circ \varphi = \mathrm{Id}_V$.

Exemple Soit $V \subset \mathbb{A}_n(\mathsf{k})$ un ensemble algébrique.

1. Les éléments $\varphi \in \Gamma(V)$ induisent des applications régulières $\varphi : V \to \mathsf{k} = \mathbb{A}_1(\mathsf{k})$.

2. Si on écrit les éléments $x \in \mathsf{k}^n = \mathbb{A}_n(\mathsf{k})$ comme des vecteurs en colonne

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

et si $M \in M_n(\mathsf{k})$ est une matrice carrée de taille n, alors $\varphi_M : \mathbb{A}_n(\mathsf{k}) \to \mathbb{A}_n(\mathsf{k})$ définie par $\varphi(x) = Mx$ est une application régulière. On a

— φ_M isomorphisme $\Leftrightarrow$ $M \in \mathrm{GL}_n(\mathsf{k})$

— Dans ce cas $\varphi_{M^{-1}}$ est l'inverse.

3. Soit $V \subset \mathbb{A}_n(\mathsf{k})$ et soit $\varphi : V \to \mathsf{k}^m$ avec $m \leq n$ la projection définie par $\varphi_n) = (x_1, \cdots, x_m)$. Alors φ est régulière.

Plus généralement, pour $\{i_1, \cdots, i_m\} \subset [1, n]$, la projection $\varphi(x) = (x_{i_1}, \cdots, x_{i_m})$ est une application régulière.

4. Soit $V = V(Y - X^2)$ et soit $\varphi : V \to \mathbb{A}_1(\mathsf{k})$ définie par $\varphi(x, y) = x$. Alors φ est un isomorphisme d'inverse $\psi : \mathbb{A}_1(\mathsf{k}) \to V$ défini par $\psi(x) = (x, x^2)$.

5. L'application $\varphi : \mathbb{A}_1(\mathsf{k}) \to V(X^3 + Y^2 - X^2)$ définie par $\varphi(t) = (t^2 - 1, t(t^2 - 1))$ est une application régulière mais n'est pas un isomorphisme (elle n'est pas injective).

6. L'application $\varphi : \mathbb{A}_1(\mathsf{k}) \to V(X^3 - Y^2)$ définie par $\varphi(t) = (t^2, t^3)$ est une application régulière, elle est bijective mais ce n'est pas un isomorphisme (voir Exemple 8.1.14).

8.1. Le foncteur Γ

Nous avons défini une application $V \mapsto \Gamma(V)$, nous allons voir que c'est en fait un foncteur contravariant : si on a une application régulière $\varphi : V \to W$ alors on définit un morphisme de k-algèbres $\Gamma(\varphi) = \varphi^* : \Gamma(W) \to \Gamma(V)$.

Définition 8.1.1 Soit $\varphi : V \to W$ une application régulière et soit $f \in \Gamma(W)$. On pose $\Gamma(\varphi)(f) = \varphi^*(f) = f \circ \varphi$.

Remarque Comme $f \in \Gamma(W)$ défini une fonction $f : W \to \mathsf{k}$, alors $\Gamma(\varphi)(f) = \varphi^*(f)$ définit aussi une fonction $\Gamma(\varphi)(f) = \varphi^*(f) : V \to \mathsf{k}$.

Lemme 8.1.3 Soit $\varphi : V \to W$ une application régulière et soit $f \in \Gamma(W)$. On a $\Gamma(\varphi)(f) = \varphi^*(f) \in \Gamma(V)$.

Preuve. On a $f = [P] \in \Gamma(W)$ pour un $P \in \mathsf{k}[Y_1, \cdots, Y_m]$. Soient $P_1, \cdots, P_m \in \mathsf{k}[X_1, \cdots, X_n]$ tels que $\varphi_i = [P_i] \in \Gamma(V)$. On a donc

$$\begin{aligned} \Gamma(\varphi)(f)(v_1, \cdots, v_n) &= f(\varphi_1(v_1, \cdots, v_n), \cdots, \varphi_m(v_1, \cdots, v_n)) \\ &= P(P_1(v_1, \cdots, v_n), \cdots, P_m(v_1, \cdots, v_n)). \end{aligned}$$

On en déduit $\Gamma(\varphi)(f) = [P(P_1, \cdots, P_m)]$ avec $P(P_1, \cdots, P_m) \in \mathsf{k}[X_1, \cdots, X_n]$. On obtient $F(\varphi)(f) \in \Gamma(V)$. ∎

Corollaire Une application régulière est continue pour la topologie de Zariski.

Preuve. Soit $\varphi : V \to W$ une application régulière et soit $U \subset W$ un ouvert, on veut montrer que $\varphi^{-1}(U)$ est ouvert. Comme les ouverts standards forment une base de la topologie, on peut supposer que U est standard de la forme $U = D_W(f)$ avec $f \in \Gamma(W)$. On a alors $D_W(f) = \{w \in W \mid f(w) \neq 0\}$. Soit maintenant $g = f \circ \varphi = \varphi^* f = \Gamma(\varphi)(f) : V \to \mathsf{k}$. On a

$$\begin{aligned} \varphi^{-1}(D_W(f)) &= \{v \in V \mid \varphi(v) \in D_W(f)\} \\ &= \{v \in V \mid f(\varphi(v)) \neq 0\} \\ &= \{v \in V \mid g(v) \neq 0\}. \end{aligned}$$

Comme $g \in \Gamma(V)$, on obtient $\varphi^{-1}(V) = D_V(g)$ qui est un ouvert standard. ∎

Exemple Toute les applications continues pour la topologie de Zariski ne sont pas régulières. Par exemple, $\exp : \mathbb{R} \to \mathbb{R}$ est continue mais pas régulière. Il est claire qu'elle n'est pas réguli/'ere : l'exponentielle n'est pas un polynôme. On vérifie qu'elle est continue. Les fermés V de $\mathbb{R}$ sont $V = \emptyset$, $V = \mathbb{R}$ ou $|V| < \infty$. On a donc $\exp^{-1}(V) = \emptyset$, $\exp^{-1}(V) = \mathbb{R}$ ou $|\exp^{-1}(V)| < \infty$. L'ensemble $\exp^{-1}(V)$ est donc fermé et exp est continue.

Lemme 8.1.6 Soit $\varphi : V \to W$ une application régulière et soit $f \in \Gamma(W)$.

L'application $\Gamma(\varphi) : \Gamma(W) \to \Gamma(V)$ est un morphisme de k-algèbre. □

Preuve. L'application est bien définie par le Lemme 8.1.3. On a $\Gamma(\varphi)(f + f') = (f+f')\circ\varphi = f\circ\varphi+f'\circ\varphi = \Gamma(\varphi)(f)+\Gamma(\varphi)(f')$. De même on a $\Gamma(\varphi)(ff') = (ff')\circ\varphi = (f \circ \varphi)(f' \circ \varphi) = \Gamma(\varphi)(f)\,\Gamma(\varphi)(f')$ et $\Gamma(\varphi)(\lambda f) = (\lambda f) \circ \varphi = \lambda(f \circ \varphi) = \lambda\,\Gamma(\varphi)(f)$. ■

Exemple Soit k un corps.

1. Soit $V = V(P)$ avec $P \in \mathsf{k}[X, Y]$, soit $W = \mathbb{A}_1(\mathsf{k})$ et soit $\varphi : V \to \mathsf{k} = \mathbb{A}_1(\mathsf{k})$ la première projection définie par $\varphi(x, y) = x$. On a

$$\Gamma(\varphi) : \Gamma(\mathbb{A}_1(\mathsf{k})) = \mathsf{k}[X] \to \Gamma(V) = \mathsf{k}[X, Y]/(P),\ Q(X) \mapsto [Q(X)].$$

2. Soit $V = \mathbb{A}_1(\mathsf{k})$, $W = V(X^3 - Y^3)$ et $\varphi : V \to W$ définie par $\varphi(t) = (t^2, t^3)$. On a

$$\Gamma(\varphi) : \Gamma(W) = \mathsf{k}[X, Y]/(X^3 - Y^2) \to \Gamma(W) = \mathsf{k}[T],\ [Q(X, Y)] \mapsto Q(T^2, T^3).$$

Lemme 8.1.8 Γ est un foncteur contravariant de la catégorie **Ens-Alg** des ensembles algébriques (dont les morphismes sont les applications régulières) vers la catégorie k**-Alg** des k-algèbres *i.e* on a

1. Pour $\varphi \in \mathrm{Reg}(V, W)$ et $\psi \in \mathrm{Reg}(W, X)$, on a $\psi \circ \varphi \in \mathrm{Reg}(V, X)$ et
$$\Gamma(\psi \circ \varphi) = \Gamma(\varphi) \circ \Gamma(\psi).$$
2. On a $\Gamma(\mathrm{Id}_V) = \mathrm{Id}_{\Gamma(V)}$. □

Preuve. 1. La première assertion vient du fait que la composée de deux polynômes est encore un polynôme. De plus, pour $f \in \Gamma(X)$, on a

$$\Gamma(\psi \circ \varphi)(f) = f \circ \psi \circ \varphi = \Gamma(\psi)(f) \circ \varphi = \Gamma(\varphi)(\Gamma(\psi)(f)) = (\Gamma(\varphi) \circ \Gamma(\psi))(f).$$

2. C'est clair. ■

Lemme 8.1.9 Soit $\varphi : V \to W$ une application régulère et soit $v \in V$. On a

$$\Gamma(\varphi)^{-1}(\mathfrak{M}_v) = \mathfrak{M}_{\varphi(v)}.$$

Preuve. On a $\Gamma(\varphi)^{-1}(\mathfrak{M}_v) = \{f \in \Gamma(W) \mid f(\varphi(v)) = 0\} = \mathfrak{M}_{\varphi(v)}$. ■

Remarque Une conséquence du lemme précédent est que l'application $\Gamma(\varphi)$ détermine l'aplication φ.

Proposition 8.1.11 L'application $\Gamma : \mathrm{Reg}(V, W) \to \mathrm{Hom}_{\mathsf{k}-\mathrm{Alg}}(\Gamma(W), \Gamma(V))$ est bijective.

Remarque On dit alors que le fonction Γ est **pleinement fidèle**.

Preuve. Soient $\varphi, \psi \in \mathrm{Reg}(V, W)$ tels que $\Gamma(\varphi) = \Gamma(\psi)$. On a $\varphi = (\varphi_1, \cdots, \varphi_m)$ et $\psi = (\psi_1, \cdots, \psi_m)$. Soit $f_j = [Y_j] \in \Gamma(W)$, on a

$$\Gamma(\varphi)(f_j)(x_1, \cdots, x_n) = f_j(\varphi(x_1, \cdots, x_n)) = \varphi_j(x_1, \cdots, x_n).$$

En particulier, on a $\varphi_j = \Gamma(\varphi)(f_j) = \Gamma(\psi)(f_j) = \psi_j$. On an déduit $\varphi = \psi$.

Soit $\theta : \Gamma(W) \to \Gamma(V)$ un morphisme de k-algèbre. Posons $\varphi_j = \theta([Y_j])\,\Gamma(V)$ pour tout $j \in [1, m]$. On définit $\varphi = (\varphi_1, \cdots, \varphi_m)$.

Montrons que φ est une application de V dans W. Soit donc $v \in V$, nous montrons que $\varphi(v) \in W$. Comme $W = V(I(W))$, il suffit de montrer que $P(\varphi(v)) = 0$ pour tout $P \in I(W)$. On a

$$\begin{array}{lll}
P(\varphi(v)) & = P(\varphi_1(v), \cdots, \varphi_m(v)) & \\
& = P(\theta([X_1]), \cdots, \theta([X_m])) & \\
& = \theta(P([X_1], \cdots, [X_m])) & \theta \text{ est un morphisme de } \mathsf{k}\text{-algèbre} \\
& = \theta([P]) & P \mapsto [P] \text{ est un morphisme de } \mathsf{k}\text{-algèbre} \\
& = \theta(0) & [P] = 0 \text{ dans } \Gamma(W) \text{ car } P \in I(W) \\
& = 0. &
\end{array}$$

On a donc $\varphi \in \mathrm{Reg}(V, W)$ et il reste /'a montrer que $\Gamma(\varphi) = \theta$. Comme $\Gamma(\varphi$ et θ sont des morphismes de k-algèbre, il suffit de montrer que ces deux applications coincident sur des générateurs, par exemple les $[Y_j]$. Il suffit donc de montrer que $\Gamma(\varphi)([Y_j]) = \theta([Y_j))$ pour tout $j \in [1, m]$. On a

$$\Gamma(\varphi)([X_j]) = [X_j](\varphi) = \varphi_j = \theta([X_j])$$

d'où le résultat. ∎

Corollaire Une application régulière $\varphi \in \mathrm{Reg}(V, W)$ est un isomorphisme si et seulement si $\Gamma(\varphi)$ est un isomorphisme.

Preuve. Soit $\psi : W \to V$ une application régulière tell que $\psi \circ \varphi = \mathrm{Id}_V$ et $\varphi \circ \psi = \mathrm{Id}_W$. On a $\Gamma(\varphi) \circ \Gamma(\psi) = \Gamma(\psi \circ \varphi) = \Gamma(\mathrm{Id}_V) = \mathrm{Id}_{\Gamma(V)}$ et $\Gamma(\psi) \circ \Gamma(\varphi) = \Gamma(\varphi \circ \psi) = \Gamma(\mathrm{Id}_X) = \mathrm{Id}_{\Gamma(W)}$.

Réciproquement, si $\Gamma(\varphi) : \Gamma(W) \to \Gamma(V)$ est un isomorphisme, soit $\theta = \Gamma(\varphi)^{-1} : \Gamma(V) \to \Gamma(W)$ son inverse. Il existe une (unique) application régulière $\psi : W \to V$ telle que $\Gamma(\psi) = \theta$. On a alors $\Gamma(\varphi \circ \psi) = \Gamma(\psi) \circ \Gamma(\varphi) = \mathrm{Id}_{\Gamma(W)} = \Gamma(\mathrm{Id}_W)$. On obtient $\varphi \circ \psi = \mathrm{Id}_W$. De même, on a $\psi \circ \varphi = \mathrm{Id}_V$ et φ est un isomorphisme. ∎

Exemple Soit k infini. L'application régulière $\varphi : V = \mathbb{A}_1(\mathsf{k}) \to W = V(Y^2 - X^3)$ définie par $\varphi(t) = (t^2, t^3)$ est bijective mais n'est pas un isomorphisme. En effet,

si φ était un isomorphisme, l'application $\Gamma(\varphi) : \Gamma(W) \to \Gamma(V)$ serait aussi un isomorphisme. Mais on a (car k est infini) ist) $I(W) = (Y^2 - X^3)$ et

$$\Gamma(\varphi) : \mathsf{k}[X,Y]/(Y^2 - X^3) \to \mathsf{k}[T],\ \Gamma(\varphi)(P) = P(T^2, T^3).$$

Pour un P quelconque, si on écrit $P = \sum_{i,j} a_{i,j} X^i Y^j$, on a

$$\Gamma(\varphi)(P) = P(T^2, T^3) = \sum_{i,j \geq 0} a_{i,j} T^{2i+3j}.$$

En particulier, on a $T \notin \mathrm{Im}(\Gamma(\varphi))$ et $\Gamma(\varphi)$ n'est pas surjective donc n'est pas un isomorphsme.

Définition 8.1.15 Un foncteur $F : \mathcal{C} \to \mathcal{D}$ est appelé **équivalence de catégories** si F est pleinenement fidèle et **essentiellement surjektif** *i.e.* pour tout $B \in \mathrm{Obj}(\mathcal{D})$ il existe un $A \in \mathrm{Obj}(\mathcal{C})$ tel que $F_{\mathrm{Obj}}(A) \simeq B$.

Théorème 8.1.16 Soit k un corps algébriquement clos.

Le foncteur Γ est une équivalence entre la catégorie **Ens-Alg** des ensembles algébriques avec pour morphismes les applications régulières et la catégorie **red-k-Alg** des k-alèbres réduites de type fini. □

Preuve. Nous savons déjà par la Proposition 8.1.11) que Γ est pleinement fidèle. Il reste /'a montrer qu'il est essentiellement surjectif. Soit donc A une k-alèbre réduite de type fini. Comme elle est de type fini, il existe des générateurs $(x_1, \cdots, x_n)$ et donc un morphisme surjetif de k-alèbres $f : \mathsf{k}[X_1, \cdots, X_n] \to A, P \mapsto P(x_1, \cdots, x_n)$. Soit $I = \mathrm{Ker}(f)$. On a $A \simeq \mathsf{k}[X_1, \cdots, X_n]/I$ et comme A est réduite, l'idéal I est radical. Par le Nullstellensatz 4, on a $I = \sqrt{I} = I(V(I))$. On obtient $A \simeq \Gamma(V(I))$. ■

Index