I. ANNEAUX ET MODULES, LOCALISATION

Séances du 25 et 26/9

Introduction

Le lecteur a déjà rencontré les corps $\mathbb{R}$ et $\mathbb{C}$, et les espaces vectoriels sur ces corps. Si l'on remplace ces corps par un anneau A, par exemple $\mathbb{Z}$ ou $\mathbb{C}[X]$, l'analogue de la notion d'espace vectoriel est celle de A-module. L'un des aspects de ce cours est donc une généralisation de **l'algèbre linéaire**. D'autre part, le lecteur aura aussi déjà rencontré les anneaux

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et vu le théorème des restes chinois, par exemple :

$$\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/84\mathbb{Z}$$

(mais $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \not\simeq \mathbb{Z}/12\mathbb{Z}$). Ainsi, un autre aspect du cours est lié à **l'arithmétique** (questions de divisibilité, étude d'équations algébriques). Signalons aussi que la théorie de la réduction des matrices $B \in M_n(\mathbb{C})$ (espaces caractéristiques, réduction de Jordan), s'obtient comme conséquence de l'étude des modules sur l'anneau $\mathbb{C}[X]$.

1. Anneaux et modules

1.1. Anneaux. —

Définition 1.1. — Un **anneau** A est un ensemble non vide muni de deux lois, $+$ (addition) et $\cdot$ (multiplication), telles que :

1) $(A, +)$ est un groupe abélien, c.-à-d.,

(0) Version du 28/9/06

(i) + est associative, c.-à-d., $a+(b+c)=(a+b)+c$, pour tout $a,b,c\in \mathrm{A}$.
(ii) + est commutative, c.-à-d., $a+b=b+a$, pour tout $a,b\in \mathrm{A}$.
(iii) A possède un élément 0 tel que $0+a=a$ pour tout $a\in \mathrm{A}$.
(iv) Tout $a\in \mathrm{A}$ admet un opposé noté $-a$, tel que $a+(-a)=0$.

2) La loi $\cdot$ est associative (c.-à-d., $a(bc)=(ab)c$ pour tout $a,b,c\in \mathrm{A}$), et A admet un élément neutre 1 tel que $1\cdot a=a=a\cdot 1$, pour tout a.

3) La loi $\cdot$ est distributive (à gauche et à droite) sur l'addition, c.-à-d., pour tout $a,b,c\in \mathrm{A}$, on a :

$$a(b+c)=ab+ac, \qquad (b+c)a=ba+ca.$$

(Ici, comme c'est l'usage, on a omis le signe $\cdot$ et écrit ab au lieu de $a\cdot b$, etc.).

Un sous-ensemble de A est un **sous-anneau** si c'est un sous-groupe pour l'addition, et s'il est stable par multiplication et contient l'élément unité 1_{A}.

Enfin, on dit que A est un **anneau commutatif** si, de plus, la loi $\cdot$ est commutative.

Remarque 1.2. — 1) Il résulte des propriétés 1) et 3) que

$$a\cdot 0=a\cdot(0+0)=(a\cdot 0)+(a\cdot 0),$$

de sorte que $a\cdot 0=0$, et de même $0\cdot a=0$, pour tout a.

2) On n'exclut pas la possibilité que $1=0$. Si c'est le cas, alors $a=a\cdot 1=a\cdot 0=0$ pour tout a, et donc A se réduit au singleton $\{0\}$, appelé l'anneau nul. Ce cas ne présente aucun intérêt et pourrait être exclu en ajoutant la condition $1\neq 0$. Toutefois, il est commode de s'autoriser à considérer l'anneau nul ; une raison est de ne pas avoir à exclure le cas $\mathrm{I}=\mathrm{A}$ lorsqu'on définira l'anneau quotient A/I pour un idéal I de A, voir plus loin.

3) Dans ce cours, on considérera quasi-exclusivement des anneaux commutatifs, à une exception près : les anneaux de matrices $\mathrm{M}_n(\mathbb{C})$ et certaines de leurs généralisations s'introduisent naturellement, même si l'on s'intéresse à un anneau commutatif A.

Définition 1.3. — Soit A un anneau. On dit qu'un élément $a\in \mathrm{A}\setminus\{0\}$ est **inversible** s'il existe $a'\in \mathrm{A}$ tel que $aa'=1=a'a$. Un tel a', s'il existe, est nécessairement unique et est alors noté a^{-1} ou $1/a$. On note $\mathrm{A}^\times$ l'ensemble des éléments inversibles de A ; c'est un groupe pour la multiplication.

Exercice 1.4. — Quels sont les éléments inversibles de $\mathbb{Z}$? Et de l'anneau

$$\mathbb{Z}[i]=\{a+ib\in\mathbb{C}\mid a,b\in\mathbb{Z}\}?$$

Définition 1.5. — Un **corps** est un anneau commutatif $k\neq\{0\}$ dans lequel tout élément non nul est inversible.

Définition 1.6. — On dit que l'anneau A est **intègre** (en anglais : A is a domain) s'il est non nul et vérifie : $a, b \in \mathrm{A} \setminus \{0\} \Rightarrow ab \neq 0$.

Il est clair que tout sous-anneau d'un anneau intègre est intègre.

Exemples 1.7. — Exemples d'anneaux intègres : tout corps k, $\mathbb{Z}$, l'anneau de polynômes $k[\mathrm{X}]$ lorsque k est un corps.

Exemples d'anneaux non intègres : $\mathrm{M}_2(\mathbb{R})$, mais il est non commutatif ; exemple commutatif : $\mathbb{Z}/6\mathbb{Z}$.

1.1.1. Morphismes. — Quelques généralités sur les morphismes.

Remarque 1.8. — Soient M, N deux groupes abéliens. Un **morphisme de groupes abéliens** $f : \mathrm{M} \to \mathrm{N}$ est une application $\mathrm{M} \to \mathrm{N}$ qui respecte la structure de groupe, c.-à-d., vérifie $f(x+y) = f(x) + f(y)$, $f(-x) = -f(x)$ et $f(0) = 0$. Ceci est le cas si, et seulement si, $f(x+y) = f(x) + f(y)$ pour tout $x, y \in \mathrm{M}$.

En effet, $f(0) = f(0+0) = f(0) + f(0)$ donne $f(0) = 0$, puis

$$0 = f(0) = f(-x+x) = f(-x) + f(x)$$

donne $f(-x) = -f(x)$.

Définition 1.9. — Soient A, B deux anneaux, non nécessairement commutatifs. Un **morphisme d'anneaux** $f : \mathrm{A} \to \mathrm{B}$ est une application qui respecte la structure d'anneau, c.-à-d., la structure de groupe abélien, la multiplication, et l'élément unité 1. On a déjà vu que, pour que f soit un morphisme de groupes abéliens, il suffit que f préserve l'addition. Donc, f est un morphisme d'anneaux si et seulement si il vérifie les trois conditions suivantes :

(i) $f(a+b) = f(a) + f(b)$, pour tout $a, b \in \mathrm{A}$;
(ii) $f(ab) = f(a)f(b)$, pour tout $a, b \in \mathrm{A}$;
(iii) $f(1) = 1$.

Remarque 1.10. — 1) La condition (iii) n'est pas conséquence de (i) et (ii). Par exemple, considèrons l'anneau $\mathbb{Z}^2$, muni de la multiplication composante par composante :

$$(a, b) \cdot (c, d) = (ac, bd);$$

son élément neutre est $(1, 1)$. L'application $\mathbb{Z} \to \mathbb{Z}^2$, $n \mapsto (n, 0)$ vérifie (i) et (ii) mais pas (iii).

2) Si A est un sous-anneau de B, alors l'inclusion $\mathrm{A} \subseteq \mathrm{B}$ est un morphisme d'anneaux. Réciproquement, si $f : \mathrm{A} \to \mathrm{B}$ est un morphisme d'anneaux injectif, alors on peut identifier A à son image $f(\mathrm{A})$, qui est un sous-anneau de B.

Définition 1.11. — Soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux. On dit que f est un **isomorphisme** d'anneaux s'il existe un morphisme d'anneaux $g : \mathrm{B} \to \mathrm{A}$ tel que $gf = \mathrm{id}_\mathrm{A}$ et $fg = \mathrm{id}_\mathrm{B}$.

Proposition 1.1. — *Soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux. Si f est bijectif, son inverse g est un morphisme d'anneaux. Par conséquent, f est un isomorphisme si, et seulement si, f est bijectif.*

Démonstration. — Laissée au lecteur. □

Convention On convient que dans la suite le mot anneau signifie anneau commutatif, sauf mention explicite du contraire.

1.2. A-modules. — Soit A un anneau.

Définition 1.12. — Un **A-module** est un groupe abélien M muni d'une application $\mathrm{A} \times \mathrm{M} \to \mathrm{M}$, notée $(a, m) \mapsto am$, vérifiant les trois propriétés suivantes (où $a, b \in \mathrm{A}$, $m, m' \in \mathrm{M}$) :

1) (bi-additivité) : $a(m + m') = am + am', \quad (a + a')m = am + a'm$;
2) ("associativité") : $a(bm) = (ab)m$;
3) ("unité") : $1m = m$.

Un **sous-A-module** de M est un sous-groupe N tel que $\mathrm{AN} = \mathrm{N}$, c.-à-d., tel que $an \in \mathrm{N}$ pour tout $a \in \mathrm{A}$, $n \in \mathrm{N}$.

Remarque 1.13. — D'après 1), on a $0m = (0+0)m = 0m+0m$ et donc $0m = 0$, pour tout $m \in \mathrm{M}$.

Détaillons ce qu'est un A-module dans les trois cas suivants : $\mathrm{A} = k$ un corps, $\mathrm{A} = \mathbb{Z}$, $\mathrm{A} = \mathbb{C}[\mathrm{X}]$.

Exemple 1.14. — Si k est un corps, un k-module est la même chose qu'un k-espace vectoriel, et un morphisme de k-modules n'est autre qu'une application k-linéaire.

Lemme 1.15. — *Un $\mathbb{Z}$-module est « la même chose » qu'un groupe abélien. Plus précisément, si* M *est un $\mathbb{Z}$-module, l'action de $\mathbb{Z}$ est entièrement déterminée par la structure de groupe abélien. Réciproquement, si* M *est un groupe abélien, il possède une unique structure de $\mathbb{Z}$-module, définie par*

$$n \cdot x = x + \cdots + x \quad (n \textit{ fois}), \quad \forall\, n \geqslant 0.$$

Démonstration. — Soit M un groupe abélien. Pour tout $x \in \mathrm{M}$ et $n \in \mathbb{N}^*$, on pose

$$(*) \qquad \begin{cases} n \cdot x = x + \cdots + x \ \ (n \text{ fois}), \\ (-n) \cdot x = -(n \cdot x) = -x - \cdots - x \ \ (n \text{ fois}), \\ 0 \cdot x = 0. \end{cases}$$

(où le zéro est celui de $\mathbb{Z}$ à gauche, et celui de M à droite). On vérifie facilement que l'application $\mathbb{Z} \times \mathrm{M} \to \mathrm{M}$, $(n, x) \mapsto n \cdot x$, fait de M un $\mathbb{Z}$-module.

Réciproquement, si M est un $\mathbb{Z}$-module, il résulte des axiomes qu'on a : $0 \cdot x = 0$ et $1 \cdot x = x$, puis, pour $n \geqslant 1$

$$n \cdot x = (1 + \cdots + 1) \cdot x = x + \cdots + x \quad (n \text{ fois}),$$

puis $0 = (n - n) \cdot x = n \cdot x + (-n) \cdot x$, d'où

$$(-n) \cdot x = -(n \cdot x) = -x - \cdots - x \quad (n \text{ fois}),$$

c.-à-d., la structure de $\mathbb{Z}$-module est définie par $(*)$ ci-dessus. Ceci montre qu'un $\mathbb{Z}$-module « est la même chose » qu'un groupe abélien. □

Proposition 1.16. — *Un* $\mathbb{C}[\mathrm{X}]$*-module « est la même chose » qu'un* $\mathbb{C}$*-espace vectoriel* V *muni d'un endomorphisme* $u \in \mathrm{End}_{\mathbb{C}}(\mathrm{V})$.

Avant de démontrer cette proposition, introduisons la définition suivante.

Définition 1.17 **(Restriction des scalaires)**. — Soit $\phi : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux et soit M un B-module. Alors M est aussi un A-module via ϕ, c.-à-d., l'action $a \cdot m = \phi(a)m$ fait de M un A-module.

Exemples 1.18. — 1) Le lecteur aura déja rencontré le cas où ϕ est l'inclusion $\mathbb{R} \subset \mathbb{C}$: tout $\mathbb{C}$-espace vectoriel V est de façon naturelle, par restriction des scalaires, un $\mathbb{R}$-espace vectoriel. (Et si $\dim_{\mathbb{C}} \mathrm{V} = n$, alors $\dim_{\mathbb{R}} \mathrm{V} = 2n$.)

2) Considérons l'inclusion $\phi : \mathbb{C} \subset \mathbb{C}[\mathrm{X}]$. Ceci montre que tout $\mathbb{C}[\mathrm{X}]$-module M est de façon naturelle un $\mathbb{C}$-espace vectoriel, l'action de $z \in \mathbb{C}$ étant égale à celle du polynôme constant $z \cdot 1$.

On peut maintenant démontrer la proposition 1.16. Soit M un $\mathbb{C}[\mathrm{X}]$-module. Alors M est un $\mathbb{C}$-espace vectoriel, et pour tout $z \in \mathbb{C}$, $m \in \mathrm{M}$, on a

$$\mathrm{X}(zm) = (\mathrm{X}z)m = (z\mathrm{X})m = z(\mathrm{X}m),$$

ce qui montre que $m \mapsto \mathrm{X}m$ est un endomorphisme $\mathbb{C}$-linéaire de M ; notons-le u. Alors, la structure de $\mathbb{C}[\mathrm{X}]$-module est entièrement déterminée par u ; en effet, pour tout $\mathrm{P} = a_0 + a_1\mathrm{X} + \cdots + a_d\mathrm{X}^d$, on a

$$(*) \qquad \mathrm{P}m = a_0 m + a_1 u(m) + \cdots + a_d u^d(m),$$

où u^d désigne $u \circ \cdots \circ u$ (d fois). Réciproquement, si V est un $\mathbb{C}$-espace vectoriel muni d'un endomorphisme u, on vérifie que l'application $\mathbb{C}[\mathrm{X}] \times \mathrm{V} \to \mathrm{V}$ définie par $(*)$ fait de V un $\mathbb{C}[\mathrm{X}]$-module. La proposition est démontrée. □

Définition 1.19. — Soit A un anneau commutatif. Évidemment, la multiplication fait de A un A-module. Un **idéal** I de A est un sous-A-module de A, c.-à-d., un sous-groupe I qui est stable par multiplication par tout élément de A, c.-à-d. : $ax \in \mathrm{I}$ pour tout $x \in \mathrm{I}$, $a \in \mathrm{A}$.

Remarque 1.20. — Si k est un corps, ses seuls idéaux sont $\{0\}$ et k.

Définition 1.21. — Pour tout $a \in \mathrm{A}$, on note

$$(a) = \mathrm{A}a = \{ab \mid b \in \mathrm{B}\},$$

l'ensemble des multiples de a. On voit facilement que c'est un idéal de A ; on l'appelle l'idéal **principal** engendré par a. Pour $a = 0$, on obtient l'idéal nul (0), et si $a = 1$, l'idéal (1) égale A.

Exemples 1.22. — 1) Soit $\mathrm{A} = \mathbb{Z}$. Les $n\mathbb{Z}$ sont des idéaux de $\mathbb{Z}$.

2) Soit $\mathrm{A} = \mathbb{R}[\mathrm{X}]$ et soit P un polynôme non nul. Alors (P) est un idéal de $\mathbb{R}[\mathrm{X}]$.

3) Soit $\mathrm{A} = \mathbb{C}[\mathrm{X}, \mathrm{Y}]$, l'anneau des polynômes en deux variables. Alors

$$\mathfrak{m} = \{\mathrm{PX} + \mathrm{QY} \mid \mathrm{P}, \mathrm{Q} \in \mathrm{A}\} = \{\mathrm{R} \in \mathrm{A} \mid \mathrm{R}(0,0) = 0\}$$

est un idéal de A. On l'appelle l'idéal engendré par X et Y et on le note (X, Y). On peut montrer qu'il n'est pas principal, c.-à-d., ne peut pas être engendré par un seul élément.

Définition 1.23. — Soient M, N deux A-modules. Un **morphisme de A-modules** $f : \mathrm{M} \to \mathrm{N}$ est un morphisme de groupes abéliens tel que $f(am) = af(m)$ pour tout $a \in \mathrm{A}, m \in \mathrm{M}$.

On dit que f est un **isomorphisme** s'il existe un morphisme de A-modules $g : \mathrm{N} \to \mathrm{M}$ tel que $gf = \mathrm{id}_{\mathrm{M}}$ et $fg = \mathrm{id}_{\mathrm{N}}$.

Proposition 1.2. — *Soit $f : \mathrm{M} \to \mathrm{N}$ un morphisme de* A*-modules. Si f est bijectif, son inverse g est un morphisme de* A*-modules. Par conséquent, f est un isomorphisme si, et seulement si, f est bijectif.*

Démonstration. — Il suffit de montrer la première assertion. Supposons f bijectif et soit g l'application inverse. Soient $n, n' \in \mathrm{N}$ et $m = g(n)$, $m' = g(n')$. Alors,

$$f(am + a'm') = af(m) + a'f(m') = an + a'n'.$$

Appliquant g, on obtient

$$g(an + a'n') = am + a'm' = ag(n) + a'g(n').$$

Ceci prouve que g est un morphisme de A-modules. □

À l'anneau $\mathbb{Z}$ et l'idéal $n\mathbb{Z}$, on a associé l'anneau $\mathbb{Z}/n\mathbb{Z}$. Ceci se généralise : pour tout sous-module N d'un A-module M, on peut construire le A-module quotient M/N ; de plus, si I est un idéal I de A, alors A/I est un anneau. Ceci est l'objet de la section suivante.

2. Modules et anneaux quotients, théorèmes de Noether

2.1. Définition des modules quotients. — Soient A un anneau, M un A-module et N un sous-A-module de M. On construit le A-module quotient M/N de la façon suivante.

D'abord, ses éléments sont les classes d'équivalence dans M pour la relation

$$x \sim y \Leftrightarrow x - y \in \mathrm{N}.$$

La classe d'un élément $x \in \mathrm{M}$ est désignée par $x + \mathrm{N}$.

On définit ensuite l'addition par

$$(x + \mathrm{N}) + (y + \mathrm{N}) = x + y + \mathrm{N}. \tag{1}$$

Bien sûr, il faut vérifier que la formule ci-dessus a bien un sens, c.-à-d., que si x' (resp. y') est un autre élément de la classe $x + \mathrm{N}$ (resp. $y + \mathrm{N}$) alors la classe de $x' + y'$ est la même que celle de $x + y$.

Ceci est bien le cas, car si $x' = x + n$ et $y' = y + n'$, où $n, n' \in \mathrm{N}$, alors

$$x' + y' = x + n + y + n' = x + y + n + n'.$$

Ayant ainsi vérifié que la formule (1) fait sens, on obtient aussitôt que l'addition est associative et commutative, et que

$$(0 + \mathrm{N}) + (x + \mathrm{N}) = x + \mathrm{N}, \qquad (-x + \mathrm{N}) + (x + \mathrm{N}) = 0 + \mathrm{N},$$

pour tout $x \in \mathrm{M}$. Par conséquent, l'ensemble quotient M/N est un groupe abélien, et l'application naturelle

$$\pi : \mathrm{M} \longrightarrow \mathrm{M/N}, \quad x \mapsto x + \mathrm{N}$$

(appelée la projection canonique de M sur M/N) est un morphisme de groupes abéliens.

De même, on définit une action de A sur M/N par la formule

$$a(x + \mathrm{N}) = ax + \mathrm{N}. \tag{2}$$

À nouveau, il faut vérifier que cette formule fait sens, c.-à-d., que si x' est un autre élément de la classe $x + \mathrm{N}$ alors la classe de ax' est la même que celle de ax. Mais ceci est clair, car si $x' - x \in \mathrm{N}$ alors $ax' - ax = a(x' - x)$ appartient aussi à N, puisque N est un sous-A-module de M.

On obtient alors facilement que (2) munit M/N d'une structure de A-module, telle que la projection $\pi : \mathrm{M} \to \mathrm{M/N}$ soit un morphisme de A-modules.

De plus, cette condition détermine uniquement la structure de A-module de M/N. En effet, sous cette condition, on doit avoir :

$$(x + \mathrm{N}) + a(x' + \mathrm{N}) = \pi(x) + a\pi(x') = \pi(x + ax') = x + ax' + \mathrm{N},$$

ce qui montre que l'addition et l'action de A sont définies par (1) et (2).

Soit maintenant I un idéal de A. On dispose déjà du A-module quotient A/I, avec la projection canonique $\pi : \mathrm{A} \to \mathrm{A/I}$. On va munir A/I d'une structure d'anneau, de sorte que π soit un morphisme d'anneaux.

Pour que ceci soit vérifié, la multiplication dans A/I doit nécessairement être définie par la formule

$$(a + \mathrm{I})(b + \mathrm{I}) = ab + \mathrm{I}, \tag{3}$$

pour tout $a, b \in \mathrm{A}$. Pour vérifier que cette formule fait sens, il faut, à nouveau, vérifier que si a' (resp. b') est un autre représentant de la classe $a + \mathrm{I}$ (resp. $b + \mathrm{I}$), alors la classe de $a'b'$ est la même que celle de ab. C'est bien le cas car si $a' = a + h$ et $b' = b + h'$, avec $h, h' \in \mathrm{I}$, alors

$$a'b' = (a + h)(b + h') = ab + ah' + hb + hh',$$

et chacun des trois produits ah', hb, et hh' appartient à I. Ceci montre que la formule (3) fait sens. On vérifie alors aussitôt, en utilisant cette formule, que la multiplication est associative, commutative et distributive sur l'addition, que la classe $1 + \mathrm{I}$ est l'élément unité, et que π est un morphisme d'anneaux.

On a donc démontré le théorème suivant.

Théorème 2.1. — (a) *Il existe une unique structure de* A*-module sur* M/N *telle que la projection* $\pi : \mathrm{M} \to \mathrm{M/N}$ *soit un morphisme de* A*-modules.*

(b) *De plus, si* I *est un idéal de* A*, il existe sur* A/I *une unique structure d'anneau telle que la projection canonique* $\pi : \mathrm{A} \to \mathrm{A/I}$ *soit un morphisme d'anneaux.*

Exemple 2.2 **(Très important)**. — Soit k un corps, par exemple $k = \mathbb{R}$, et soit $\mathrm{P} \in k[\mathrm{X}]$ non nul, de degré n. Alors, le $k[\mathrm{X}]$-module quotient est de dimension n comme k-espace vectoriel : pour tout $\lambda \in k$, il admet une base formée par les images des monômes $\{1, \mathrm{X} - \lambda, \dots, (\mathrm{X} - \lambda)^{n-1}\}$.

En effet, en faisant un changement de variable $\mathrm{X}' = \mathrm{X} + \lambda$, il suffit de faire la démonstration dans le cas où $\lambda = 0$. Pour $\mathrm{S} \in k[\mathrm{X}]$ arbitraire, on peut faire la division euclidienne de S par P :

$$\mathrm{S} = \mathrm{PQ} + \mathrm{R}, \quad \text{avec } \mathrm{R} = 0 \text{ ou } \deg \mathrm{R} < n.$$

Écrivant $\mathrm{R} = \sum_{i=0}^{n-1} a_i \mathrm{X}^i$, on obtient que $\overline{\mathrm{S}} = \overline{\mathrm{R}} = \sum_{i=0}^{n-1} a_i \overline{\mathrm{X}^i}$. Ceci montre que les $\overline{\mathrm{X}^i}$, pour $i = 0, \dots, n-1$, engendrent $k[\mathrm{X}]/(\mathrm{P})$ comme espace vectoriel. De plus, ces images sont linéairement indépendantes sur k : si on a une égalité $0 = \sum_{i=0}^{n-1} a_i \overline{\mathrm{X}^i}$, avec $a_i \in k$, alors le polynôme $\mathrm{R} = \sum_{i=0}^{n-1} a_i \mathrm{X}^i$ appartient à (P), donc $\mathrm{R} = \mathrm{PQ}$ pour un certain $\mathrm{Q} \in k[\mathrm{X}]$; comme

$$\deg \mathrm{P} = n > \deg \mathrm{R},$$

ceci n'est possible que si $\mathrm{Q} = 0$, d'où $a_i = 0$ pour tout i.

Remarque 2.3. — On montrera plus loin que tout $\mathbb{C}[X]$-module qui est de dimension finie sur $\mathbb{C}$ est une somme directe de modules

$$V_n(\lambda) = \mathbb{C}[X]/(X-\lambda)^{n+1}, \quad \text{où } \lambda \in \mathbb{C}, n \in \mathbb{N}.$$

Considérons la base $\{\overline{1}, \ldots, \overline{(X-\lambda)^n}\}$ de $V_n(\lambda)$. Comme $X = (X-\lambda) + \lambda \cdot 1$, la matrice dans cette base de la multiplication par X est :

$$J_{n+1}(\lambda) = \begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & \lambda & 0 \\ 0 & \cdots & 0 & 1 & \lambda \end{pmatrix}.$$

On retrouve donc ainsi la décomposition en somme directe d'espaces propres généralisés, et la décomposition de Jordan des endomorphismes.

Exercice 2.4. — Soient A un anneau, I un idéal, M un A-module. On désigne par IM l'ensemble des sommes finies

$$x_1 m_1 + \cdots + x_r m_r,$$

où $r \in \mathbb{N}$, $x_i \in I$, $m_i \in M$. Montrer que IM est un sous-A-module de M, puis que M/IM est un A/I-module.

Ainsi, partant d'un sous-module N de M, resp. d'un idéal I de A, on a construit le module M/N, resp. l'anneau A/I. Il est naturel de se demander quels sont les sous-modules de M/N, et les idéaux de A/I. Ceci est l'objet du prochain théorème.

Pour tout sous-module L de M/N, posons

$$\pi^{-1}(L) = \{x \in M \mid \pi(x) \in L\}.$$

On voit facilement que c'est un sous-module de M contenant N. De plus, comme π est surjectif, on a $\pi(\pi^{-1}(L)) = L$.

Réciproquement, soit M′ un sous-module de M contenant N. Alors $\pi(M')$ est l'ensemble des classes $y+N$, où $y \in M'$, donc s'identifie au module quotient M′/N. Il est clair que

$$M' \subseteq \pi^{-1}(\pi(M')). \tag{†}$$

Réciproquement, soit $x \in \pi^{-1}(\pi(M'))$. Alors $\pi(x) \in \pi(M')$ donc il existe $y \in M'$ tel que $\pi(x) = \pi(y)$, d'où $x - y \in N$. Or $N \subseteq M'$ et donc $x = y + n \in M'$. Ceci montre que l'inclusion (†) est une égalité.

On a donc démontré que les applications $L \mapsto \pi^{-1}(L)$ et $M' \mapsto \pi(M') = M'/N$ sont des bijections réciproques entre l'ensemble des sous-modules de M/N et l'ensemble des sous-modules de M contenant N.

Si I est un idéal de A, les idéaux de A/I ne sont autres que les sous-A-modules de A/I (le vérifier !), et correspondent donc bijectivement aux idéaux de A contenant I. On a donc obtenu le théorème suivant.

Théorème 2.5. — *Les sous-modules de* M/N *sont les* M′/N*, pour* M′ *sous-module* M′ *de* M *contenant* N*, et les idéaux de* A/I *sont les* J/I*, pour* J *idéal de* A *contenant* I*.*

Remarque 2.6. — Les deux théorèmes précédents s'appliquent en particulier au cas des groupes abéliens (c.-à-d., le cas $A = \mathbb{Z}$).

Remarque 2.7. — 1) Il ne faut pas être rebuté par l'aspect abstrait de la définition des quotients. Dans la pratique, on ne pense jamais à A/I comme à un ensemble de classes d'équivalence ; on voit plutôt les éléments de A/I comme « des éléments de A », avec lesquels on calcule « modulo I ». Comme exemples de base, on peut penser aux anneaux $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{R}[X]/(X^n)$.

2) De plus, cette façon de « négliger » (c.-à-d., de rendre nuls) les éléments de I permet dans bien des cas de travailler avec un anneau A/I plus simple que A, et d'en déduire des résultats pour A lui même. Un exemple frappant est le théorème de l'invariance du rang d'un A-module libre de type fini (voir plus loin).

3) On peut aussi obtenir des résultats négatifs sur A, c.-à-d., montrer que A n'a pas telle ou telle propriété, en montrant que cette propriété entraîne une contradiction facile à détecter dans un certain anneau quotient de A. Le lecteur intéressé pourra étudier, par exemple, [**Pe1**, Chap.II, § 5], où des arguments de ce type sont utilisés pour montrer que les anneaux $\mathbb{Z}[(1 + i\sqrt{19})/2]$ et $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ ne sont pas euclidiens, bien que principaux (voir plus loin pour la définition et l'étude de ces anneaux).

4) Les anneaux quotients d'anneaux de polynômes $\mathbb{C}[X_1, \ldots, X_n]$ apparaissent de façon naturelle quand on considère les fonctions polynomiales sur un sous-ensemble de $\mathbb{C}^n$ défini par des équations polynomiales, voir par exemple [**Pe2**] ou [**Die**].

2.2. A-modules simples et idéaux maximaux. — Soit M un A-module.

Définition 2.8. — 1) On dit que M est un A-module **simple** si $M \neq (0)$ et si M n'a pas de sous-module autre que (0) et M.

2) On dit que M est un A-module **cyclique** (ou **monogène**) s'il peut être engendré par un seul élément, c.-à-d., s'il existe $x \in M$ tel que $M = Ax$.

Remarque 2.9. — Évidemment, si M est simple, il est engendré par tout $x \in M$ non nul, car alors le sous-module Ax est non nul, donc égal à M.

Mais attention, un module cyclique n'est pas nécessairement simple ! Par exemple, $\mathrm{A} = \mathrm{A} \cdot 1$ est un A-module cyclique, mais n'est pas simple, sauf si A est un corps.

Définition 2.10. — Soit I un idéal de A. On dit que I est un idéal **maximal** si $\mathrm{I} \neq \mathrm{A}$ et si A est le seul idéal contenant strictement J. Ceci équivaut à dire que si J est un idéal contenant I, alors $\mathrm{J} = \mathrm{I}$ ou $\mathrm{J} = \mathrm{A}$, c.-à-d., le A-module A/I est simple.

D'après le lemme ci-dessous, ceci équivaut à dire que l'anneau quotient A/I est un corps.

Lemme 2.11. — *Soit* B *un anneau commutatif, n'ayant pas d'idéaux autres que* (0) *et* B. *Alors* B *est un corps.*

Démonstration. — Soit $x \in \mathrm{B}$ non nul. Alors, l'idéal $\mathrm{B}x$ est non nul, donc égale B. Donc il existe $b \in \mathrm{B}$ tel que $bx = 1$. Ceci montre que tout $x \neq 0$ est inversible, donc B est un corps. □

Définition 2.12. — Soit $x \in \mathrm{M}$; on définit son **annulateur**

$$\mathrm{Ann}(x) = \mathrm{Ann}_{\mathrm{A}}(x) = \{a \in \mathrm{A} \mid ax = 0\}.$$

C'est un idéal de A, et l'on a : $x = 0 \Leftrightarrow \mathrm{Ann}(x) = (1)$. On définit aussi l'annulateur de M :

$$\mathrm{Ann}(\mathrm{M}) = \bigcap_{x \in \mathrm{M}} \mathrm{Ann}(x) = \{a \in \mathrm{A} \mid a\mathrm{M} = (0)\}.$$

Proposition 2.1. — *Soient* $x \in \mathrm{M}$ *et* $\mathrm{I} = \mathrm{Ann}_{\mathrm{A}}(x)$. *L'application* $a + \mathrm{I} \mapsto ax$ *est un isomorphisme de* A*-modules*

$$\mathrm{A/I} \xrightarrow{\sim} \mathrm{A}x \subseteq \mathrm{M}.$$

Démonstration. — Laissée au lecteur (ou bien, voir le paragraphe suivant). □

Corollaire 2.13. — *Soit* M *un* A*-module simple. Alors* $\mathrm{M} \simeq \mathrm{A/I}$*, où* I *est un idéal maximal.*

Démonstration. — Soit $x \in \mathrm{M}$ non nul. Alors $\mathrm{M} = \mathrm{A}x$. Posant $\mathrm{I} = \mathrm{Ann}(x)$, on obtient, d'après la proposition précédente,

$$\mathrm{A/I} \simeq \mathrm{A}x = \mathrm{M}.$$

Comme M est simple, ceci entraîne que I est maximal. □

2.3. Noyaux et théorèmes de Noether. —

Définition 2.14. — 1) Soit $f : \mathrm{M} \to \mathrm{M}'$ un morphisme de A-modules. Son noyau et son image :

$$\mathrm{Ker}(f) = \{x \in \mathrm{M} \mid f(x) = 0\}, \qquad \mathrm{Im}(f) = f(\mathrm{M}) = \{f(x) \mid x \in \mathrm{M}\};$$

sont des sous-modules de M et M′ respectivement.

2) Soit $f : \mathrm{A} \to \mathrm{B}$ un morphisme d'anneaux, avec B non nécessairement commutatif. Alors $\mathrm{Ker}(f)$ est un idéal de A, et

$$f(\mathrm{A}) = \{f(a) \mid a \in \mathrm{A}\}$$

est un sous-anneau commutatif de B.

Remarque 2.15. — 1) Une application d'ensembles $f : \mathrm{X} \to \mathrm{Y}$ est bijective si, et seulement si, elle est injective et surjective.

2) Soit $f : \mathrm{M} \to \mathrm{M}'$ un morphisme de A-modules. Alors f est surjectif $\Leftrightarrow \mathrm{Im}(f) = \mathrm{M}'$, et f est injectif $\Leftrightarrow \mathrm{Ker}(f) = 0$. Par conséquent, f est un isomorphisme si et seulement si $\mathrm{Ker}(f) = 0$ et $\mathrm{Im}(f) = \mathrm{M}'$.

Théorème 2.16. — 1) *Soit* $f : \mathrm{M} \to \mathrm{M}'$ *un morphisme de* A*-modules et soit* N *un sous-module de* M *contenu dans* $\mathrm{Ker}(f)$. *Notons* π *la projection* $\mathrm{M} \to \mathrm{M/N}$. *Alors,* f *se factorise de façon unique à travers* M/N, *c.-à-d., il existe un unique morphisme de* A*-modules*

$$\overline{f} : \mathrm{M/N} \longrightarrow \mathrm{Im}(f) \subseteq \mathrm{M}'$$

tel que $\overline{f} \circ \pi = f$, *et l'on a* $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/\mathrm{N}$. *En particulier, pour* $\mathrm{N} = \mathrm{Ker}(f)$ *on obtient un isomorphisme de* A*-modules*

$$\overline{f} : \mathrm{M}/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f).$$

2) *Soit* $f : \mathrm{A} \to \mathrm{B}$ *un morphisme d'anneaux, avec* B *non nécessairement commutatif, et soit* J *un idéal de* A *contenu dans* $\mathrm{Ker}(f)$. *Notons* π *la projection* $\mathrm{A} \to \mathrm{A/J}$. *Alors,* f *se factorise de façon unique à travers* A/J, *c.-à-d., il existe un unique morphisme d'anneaux*

$$\overline{f} : \mathrm{A/J} \longrightarrow f(\mathrm{A}) \subseteq \mathrm{B}$$

tel que $\overline{f} \circ \pi = f$, *et l'on a* $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/\mathrm{J}$. *En particulier, pour* $\mathrm{J} = \mathrm{Ker}(f)$ *on obtient un isomorphisme d'anneaux*

$$\overline{f} : \mathrm{A}/\mathrm{Ker}(f) \xrightarrow{\sim} f(\mathrm{A}).$$

Démonstration. — 1) On remarque que f prend la même valeur sur tout élément d'une classe $m + \mathrm{N}$, car si $m' = m + x$ avec $x \in \mathrm{N} \subseteq \mathrm{Ker}(f)$ alors $f(m') = f(m)$. On peut donc définir $\overline{f} : \mathrm{M/N} \to \mathrm{Im}(f) \subseteq \mathrm{P}$ par la formule

$$\overline{f}(m + \mathrm{N}) = f(m).$$

Alors, par définition, l'on a $\overline{f} \circ \pi = f$. De plus, $\overline{f}$ est un morphisme de A-modules. En effet, soient $\overline{x}, \overline{y} \in \overline{\mathrm{M}} := \mathrm{M}/\mathrm{N}$ et soient $x, y \in \mathrm{M}$ tels que $\pi(x) = \overline{x}$ et $\pi(y) = \overline{y}$. Alors, d'après la définition de la structure de groupe abélien et de A-module de $\overline{\mathrm{M}}$, et la définition de $\overline{f}$, l'on a

$$\overline{f}(\overline{x} + a\overline{y}) = \overline{f}(\pi(x + ay)) = f(x + ay) = f(x) + af(y) = \overline{f}(\overline{x}) + a\overline{f}(\overline{y}).$$

Ceci prouve que $\overline{f}$ est un morphisme de A-modules. Montrons de plus que

$$\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/\mathrm{N}.$$

L'inclusion $\supseteq$ est claire. Réciproquement, soit $m + \mathrm{N} \in \mathrm{Ker}(\overline{f})$. Alors $0 = \overline{f}(\overline{m}) = f(m)$ donc $m \in \mathrm{Ker}(f)$.

Dans le cas particulier où $\mathrm{N} = \mathrm{Ker}(f)$, on obtient donc un morphisme

$$\overline{f} : \mathrm{M}/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$$

qui est surjectif et injectif, donc un isomorphisme.

2) La preuve de 2) est tout-à-fait analogue à celle de 1) et est laissée au lecteur. Montrons seulement que $\overline{f}$ est un morphisme d'anneaux : avec des notations évidentes, on a

$$\overline{f}(\overline{a}\overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a)f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b}).$$

□

Exemples 2.17. — 1) Comme $12\mathbb{Z} \subseteq 4\mathbb{Z}$, le morphisme morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ se factorise par $\mathbb{Z}/12\mathbb{Z}$.

2) Comme $(\mathrm{X}^3) \subseteq (\mathrm{X}^2)$ dans $\mathbb{R}[\mathrm{X}]$, le morphisme d'anneaux $\mathbb{R}[\mathrm{X}] \to \mathbb{R}[\mathrm{X}]/(\mathrm{X}^2)$ se factorise à travers $\mathbb{R}[\mathrm{X}]/(\mathrm{X}^3)$.

Le théorème précédent admet les deux corollaires suivants. Soient M, N deux sous-modules d'un A-module E. On pose

$$\mathrm{M} + \mathrm{N} = \{x + y \mid x \in \mathrm{M},\ y \in \mathrm{N}\},$$

c'est un sous-module de E, appelé la somme des sous-modules M et N.

Corollaire 2.18 **(1er théorème d'isomorphisme)**. — *L'inclusion* $\mathrm{M} \hookrightarrow \mathrm{M}+\mathrm{N}$ *induit un isomorphisme de* A*-modules :*

$$\frac{\mathrm{M}}{\mathrm{M} \cap \mathrm{N}} \xrightarrow{\sim} \frac{\mathrm{M} + \mathrm{N}}{\mathrm{N}}.$$

Démonstration. — Notons ϕ la composée $\mathrm{M} \hookrightarrow \mathrm{M} + \mathrm{N} \twoheadrightarrow (\mathrm{M} + \mathrm{N})/\mathrm{N}$. On a $\mathrm{Ker}(\phi) = \mathrm{M} \cap \mathrm{N}$ et ϕ est surjective car tout élément de $(\mathrm{M} + \mathrm{N})/\mathrm{N}$ est de la forme $m+\mathrm{N}$, avec $m \in \mathrm{M}$. Donc le corollaire résulte du théorème précédent. □

***Corollaire 2.19* (2ème théorème d'isomorphisme).** — *Soient* $\mathrm{M} \supseteq \mathrm{N} \supseteq \mathrm{P}$ *des* A*-modules. Alors :*

1) *On a un morphisme surjectif de* A*-modules* $\phi : \mathrm{M/P} \to \mathrm{M/N}$, $m + \mathrm{P} \mapsto m + \mathrm{N}$, *et son noyau est le sous-module* N/P.

2) *La projection* ϕ *induit un isomorphisme de* A*-modules :*

$$(\mathrm{M/P})/(\mathrm{N/P}) \xrightarrow{\sim} \mathrm{M/N}.$$

3) *Dans le cas où* $\mathrm{J} \subseteq \mathrm{I}$ *sont des idéaux de* A, *on a un isomorphisme d'anneaux*

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

Démonstration. — Considérons les projections $\pi_{\mathrm{N}} : \mathrm{M} \to \mathrm{M/N}$ et $\pi_{\mathrm{P}} : \mathrm{M} \to \mathrm{M/P}$. Comme $\mathrm{P} \subseteq \mathrm{N} = \mathrm{Ker}(\pi_{\mathrm{N}})$, alors π_{N} induit l'application

$$\phi : \mathrm{M/P} \twoheadrightarrow \mathrm{M/N}, \qquad m + \mathrm{P} \mapsto m + \mathrm{N},$$

telle que $\phi \circ \pi_{\mathrm{P}} = \pi_{\mathrm{N}}$. Le noyau de ϕ est l'ensemble des classes $m + \mathrm{P}$ telles que $m + \mathrm{N} = 0$, c.-à-d., telles que $m \in \mathrm{N}$; c'est donc le sous-module N/P de M/P. Ceci prouve le point 1), et les points 2) et 3) résultent alors du théorème précédent. □

3. Construction de modules ou d'idéaux

3.1. Sous-module ou idéal engendré. —

Soit M un A-module.

***Proposition 3.1*.** — *Soit* S *une partie non-vide de* M, *finie ou infinie. L'ensemble de toutes les sommes* **finies** *de la forme*

$$(*) \qquad \sum_{i=1}^{n} a_i x_i, \quad \text{où} \quad n \geqslant 1, x_i \in \mathrm{S}, a_i \in \mathrm{A},$$

est un sous-module de M, *et c'est le plus petit sous-module de* M *contenant* S. *On l'appelle le sous-module* **engendré par** S *et on le note* (S).

Si $\mathrm{M} = \mathrm{A}$, *on dit que* (S) *est l'idéal engendré par* S.

Démonstration. — Il est clair que l'ensemble considéré contient S (et est donc non vide) et est stable par addition, soustraction et multiplication par un élément arbitraire de A. C'est donc un sous-module de M contenant S. Notons-le (S).

Réciproquement, soit N un sous-module de M contenant S. Alors N contient toute somme de la forme $(*)$, et donc N contient (S). Ceci prouve que (S) est le plus petit sous-module de M contenant S. □

Remarque 3.1. — 1) Lorsque $M = A$ et $S = \{0\}$, (0) est l'idéal nul, tandis que pour $S = \{1\}$ on a $(1) = A$. Ceci justifie les notations introduites précédemment.

2) Revenons au cas M arbitraire. Si S est un ensemble fini, disons $S = \{x_1, \ldots, x_r\}$, on désignera (S) aussi par

$$Ax_1 + \cdots + Ax_r \quad \text{ou} \quad \sum_{i=1}^{r} Ax_i.$$

Plus généralement, si $S = \{x_i\}_{i\in I}$, où I est un ensemble d'indices arbitraire, on écrira aussi

$$(S) = \sum_{i\in I} Ax_i,$$

étant entendu que le terme de droite désigne l'ensemble des sommes finies de termes $a_i x_i$.

Exercice 3.2. — Soit $\lambda \in \mathbb{C}$. Montrer que l'idéal $I_\lambda = \{P \in \mathbb{C}[X] \mid P(\lambda) = 0\}$ est l'idéal engendré par le polynôme $X - \lambda$. (Utiliser la division euclidienne par $X - \lambda$).

3.2. Sommes de sous-modules et sommes directes. — Soient $M_1, \ldots, M_n$ des sous-modules d'un A-module M.

***Définition 3.3* (Somme de sous-modules)**. — On note $M_1 + \cdots + M_n$ ou $\sum_{i=1}^{n} M_i$ le sous-module de M engendré par $M_1 \cup \cdots \cup M_n$. Il résulte de la proposition 3.1 que $M_1 + \cdots + M_n$ est l'ensemble des éléments de la forme

$$x_1 + \cdots + x_n,$$

avec $x_i \in M_i$ pour $i = 1, \ldots, n$.

Définition et proposition 3.4. — *On dit que les sous-modules* $M_1, \ldots, M_n$ *de* M *sont en* **somme directe** *si tout élément* $x \in \sum_{i=1}^{n} M_i$ *s'écrit de façon* **unique** *sous la forme*

$$x = x_1 + \cdots + x_n, \quad \text{où} \quad x_i \in M_i.$$

Ceci est le cas si, et seulement si, on a :

$$(*) \qquad \forall\, i = 1, \ldots, n, \qquad M_i \cap \sum_{j\neq i} M_j = \{0\}.$$

Démonstration. — Supposons $(*)$ vérifiée et considérons deux décompositions

$$x = x_1 + \cdots + x_n = x'_1 + \cdots + x'_n,$$

avec $x_j, x'_j \in M_j$. Alors, pour tout i, on a

$$x_i - x'_i = \sum_{j\neq i} (x'_j - x_j),$$

et donc $x_i - x_i' = 0$ d'après l'hypothèse $(*)$. Ceci prouve l'unicité de l'écriture. Réciproquement, supposons l'unicité vérifiée et soit $x_i \in \mathrm{M}_i \cap \sum_{j\neq i} \mathrm{M}_j$. Alors on peut écrire $-x_i = \sum_{j\neq i} x_j$, avec $x_j \in \mathrm{M}_j$, d'où

$$0 = \sum_{j=1}^{n} x_j,$$

et donc $x_i = 0$ par unicité de l'écriture. Ceci montre que $(*)$ est vérifiée. □

D'autre part, étant donnés des A-modules arbitraires $\mathrm{M}_1, \ldots, \mathrm{M}_n$, on peut définir leur somme directe « externe », comme suit.

Définition 3.5. — Le groupe abélien

$$\mathrm{M}_1 \times \cdots \times \mathrm{M}_n = \{(m_1, \ldots, m_n) \mid m_i \in \mathrm{M}_i\}$$

(où l'addition est définie composante par composante), est muni d'une structure de A-module définie par

$$a(m_1, \ldots, m_n) = (am_1, \ldots, am_n).$$

On l'appelle **somme directe** (externe) des M_i et on le note

$$\mathrm{M}_1 \oplus \cdots \oplus \mathrm{M}_n \quad \text{ou} \quad \bigoplus_{i=1}^{n} \mathrm{M}_i.$$

Si l'on pose $\mathrm{S} = \bigoplus_{j=1}^{n} \mathrm{M}_j$ et si l'on identifie chaque $m_i \in \mathrm{M}_i$ au n-uplet

$$(0, \ldots, 0, m_i, 0, \ldots, 0)$$

où, bien sûr, m_i se trouve à la i-ème place, alors M_i s'identifie à un sous-module de S, et l'on vérifie sans peine que S est la somme directe de ses sous-modules M_i.

Notation 3.6. — Si tous les M_i sont égaux à un même A-module M, la somme directe $\mathrm{M} \oplus \cdots \oplus \mathrm{M}$ (n copies) sera désignée par M^n ou $\mathrm{M}^{\oplus n}$.

3.3. Sommes et produits d'idéaux. — Soient $\mathrm{I}_1, \ldots, \mathrm{I}_n$ des idéaux de A.

Définition 3.7. — 1) On note $\mathrm{I}_1 + \cdots + \mathrm{I}_n$ l'idéal engendré par $\mathrm{I}_1 \cup \cdots \cup \mathrm{I}_n$. D'après la proposition 3.1, c'est l'ensemble des éléments $x_1 + \cdots + x_n$, avec $x_k \in \mathrm{I}_k$.

2) On note $\mathrm{I}_1 \cdots \mathrm{I}_n$ l'idéal engendré par tous les produits $x_1 \cdots x_n$, avec $x_k \in \mathrm{I}_k$. Attention, l'ensemble de ces produits n'est pas stable par addition ! Il résulte de 3.1 que $\mathrm{I}_1 \cdots \mathrm{I}_n$ est l'ensemble de toutes les sommes finies

$$a_1 \cdots a_n + b_1 \cdots b_n + \cdots + z_1 \cdots z_n,$$

avec $a_k, b_k, \ldots, z_k \in \mathrm{I}_k$.

3) En particulier, lorsque $\mathrm{I}_1 = \cdots = \mathrm{I}_n = \mathrm{I}$, on note I^n l'idéal engendré par tous les produits $x_1 \cdots x_n$, avec $x_k \in \mathrm{I}$, c.-à-d., l'ensemble de toutes les sommes finies de produits de n éléments de I.

Attention ! I^n n'est pas égal à l'idéal engendré par les x^n, pour $x \in \mathrm{I}$.

Exemple 3.8. — Soient $\mathrm{A} = \mathbb{C}[\mathrm{X}, \mathrm{Y}]$ et $\mathfrak{m} = (\mathrm{X}, \mathrm{Y})$, l'idéal engendré par X et Y. Alors XY appartient à $(\mathrm{X}, \mathrm{Y})^2$ mais n'est pas un carré dans $\mathbb{C}[\mathrm{X}, \mathrm{Y}]$.

Remarque 3.9. — Si M est un A-module, on note M^n la somme directe $\mathrm{M} \oplus \cdots \oplus \mathrm{M}$. Ainsi, lorsque M est un idéal I, la notation I^n peut *a priori* faire référence ou bien au A-module $\mathrm{I} \oplus \cdots \oplus \mathrm{I}$ (somme directe externe de n copies de I), ou bien à l'idéal produit $\mathrm{I} \cdots \mathrm{I}$ (n facteurs). En dépit de ce conflit apparent de notation, aucune confusion n'en résulte en pratique ; il est toujours clair d'après le contexte si l'on fait référence à la somme directe de modules, ou au produit d'idéaux. En tout cas, lorsqu'on parle de *l'idéal* I^n il s'agit toujours, bien entendu, du produit $\mathrm{I} \cdots \mathrm{I}$.

Lemme 3.10. — *Soient* I, J *deux idéaux de* A. *Si* I, *resp.* J, *est engendré par des éléments* $x_1, \ldots, x_m$, *resp.* $y_1, \ldots, y_n$, *alors* IJ *est engendré par les produits*

$$x_i y_j, \quad \textit{pour } i = 1, \ldots, m,\ j = 1, \ldots, n.$$

En particulier, lorsque $\mathrm{I} = (x)$ *et* $\mathrm{J} = (y)$, *on a :* $(x)(y) = (xy)$.

Démonstration. — Laissée au lecteur. □

4. Idéaux premiers et localisation

4.1. Idéaux premiers. —

Définition 4.1. — Soit P un idéal de A. On dit que P est **premier** si l'anneau quotient A/P est intègre. Comme un anneau intègre est $\neq \{0\}$, par définition, ceci équivaut à dire que : $\mathrm{P} \neq \mathrm{A}$ et P vérifie l'une des conditions équivalentes suivantes : soient $a, b \in \mathrm{A}$ et I, J deux idéaux ;

- si $a \notin \mathrm{P}$ et $b \notin \mathrm{P}$ alors $ab \notin \mathrm{P}$;
- si $ab \in \mathrm{P}$ alors $a \in \mathrm{P}$ ou $b \in \mathrm{P}$;
- si $\mathrm{IJ} \subseteq \mathrm{P}$ alors $\mathrm{I} \subseteq \mathrm{P}$ ou $\mathrm{J} \subseteq \mathrm{P}$;
- si $\mathrm{I} \not\subseteq \mathrm{P}$ et $\mathrm{J} \not\subseteq \mathrm{P}$, alors $\mathrm{IJ} \not\subseteq \mathrm{P}$.

En particulier, comme un corps est un anneau intègre, tout idéal maximal de A est premier.

On note Spec(A), resp. Max(A), l'ensemble des idéaux premiers, resp. maximaux, de A.

On laisse au lecteur le soin de vérifier l'équivalence des conditions ci-dessus. De plus, le lemme suivant est très utile dans la pratique.

Lemme 4.2. — *Soit* $\mathrm{P} \in \mathrm{Spec}(\mathrm{A})$*, et soient* $\mathrm{I}_1, \ldots, \mathrm{I}_n$ *des idéaux de* A.

1) *Si* $\mathrm{I}_1 \cdots \mathrm{I}_n \subseteq \mathrm{P}$*, alors* P *contient l'un des* I_k.

2) *Si* $\bigcap_{k=1}^n \mathrm{I}_k \subseteq \mathrm{P}$*, alors* P *contient l'un des* I_k.

Démonstration. — Le point 1) se démontre par récurrence sur n. Le point 2) en découle, car le produit $\mathrm{I}_1 \cdots \mathrm{I}_n$ est contenu dans l'intersection $\bigcap_{k=1}^n \mathrm{I}_k$. □

Remarque 4.3. — Les idéaux premiers d'un anneau A jouent un rôle extrêmement important.

a) En arithmétique, si A est un anneau de nombres, ses idéaux premiers généralisent la notion usuelle de nombre premier dans $\mathbb{Z}$, voir par exemple [**Sa**].

b) En géométrie algébrique, les idéaux premiers de l'anneau $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ correspondent aux **sous-variétés algébriques irréductibles** de $\mathbb{C}^n$: une **sous-variété algébrique** de $\mathbb{C}^n$ est un sous-ensemble X de $\mathbb{C}^n$ défini par des équations polynomiales $f_1, \ldots, f_m$, c.-à-d., X égale

$$\mathrm{V}(f_1, \ldots, f_m) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid f_j(x_1, \ldots, x_n) = 0,\ \forall\, j = 1, \ldots, m\}.$$

On observe que $\mathrm{V}(f_1, \ldots, f_m) = \mathrm{V}(\mathrm{I})$, où I désigne l'idéal engendré par $f_1, \ldots, f_m$.

D'autre part, à un tel X, on associe l'idéal

$$\mathrm{I}(\mathrm{X}) = \{f \in \mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \mid f(x) = 0,\ \forall\, x \in \mathrm{X}\}.$$

Enfin, on dit que X est **irréductible** s'il n'est pas réunion de deux sous-variétés algébriques plus petites, c.-à-d., s'il vérifie la propriété suivante : si J, K sont des idéaux de $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tels que $\mathrm{X} = \mathrm{V}(\mathrm{J}) \cup \mathrm{V}(\mathrm{K})$, alors $\mathrm{V}(\mathrm{J}) = \mathrm{X}$ ou $\mathrm{V}(\mathrm{K}) = \mathrm{X}$. *Exercice* : Montrez que X est irréductible $\Leftrightarrow$ I(X) est un idéal premier. Les lecteurs intéressés pourront consulter, par exemple, [**Die**] ou [**Pe2**].

Soit $\phi : \mathrm{A} \to \mathrm{K}$ un morphisme d'anneaux, où K est un corps. Alors $\mathrm{A}/\operatorname{Ker}(\phi)$ est isomorphe à $\phi(\mathrm{A}) \subseteq \mathrm{K}$, qui est intègre. Donc $\operatorname{Ker}(\phi)$ est un idéal premier.

Réciproquement, on va montrer que tout $\mathrm{P} \in \mathrm{Spec}(\mathrm{A})$ peut être obtenu de cette façon. On va montrer que tout anneau intègre B se plonge dans un corps K, appelé le corps des fractions de B, et qu'on peut décrire comme l'ensemble des fractions a/b, avec $a, b \in \mathrm{B}$, $b \neq 0$, et les égalités usuelles

$$\frac{a}{b} = \frac{c}{d} \quad \text{si} \quad ad = bc.$$

Ceci est l'objet du paragraphe suivant, qui développe la « construction des fractions » en toute généralité.

4.2. Anneaux et modules de fractions. — Soit A un anneau commutatif.

Définition 4.4. — Une **partie multiplicative** de A est un sous-ensemble S contenant 1, stable par multiplication et ne contenant pas 0.

Exemples 4.5. — 1) Si A est intègre, alors $A \setminus \{0\}$ est une partie multiplicative. Plus généralement, si P est un idéal premier, son complémentaire $S = A \setminus P$ est une partie multiplicative.

2) Un élément $x \in A$ est dit nilpotent s'il existe $n \geqslant 1$ tel que $x^n = 0$. Pour tout $f \in A$ non nilpotent, l'ensemble $\{f^n \mid n \in \mathbb{N}\}$ (avec la convention $f^0 = 1$), est une partie multiplicative.

Soit M un A-module. On veut construire un A-module $S^{-1}M$, formé de « fractions »

$$\frac{m}{s}, \qquad m \in M,\ s \in S,$$

et sur lequel l'action de tout $s \in S$ soit inversible. On veut de plus que les règles usuelles d'addition et de multiplication des fractions soient vérifiées. En particulier, pour tout $x, y \in M$ et $s, t, u \in S$ on doit avoir :

$$(*) \qquad u(tx - sy) = 0 \Rightarrow \frac{x}{s} - \frac{y}{t} = \frac{u(tx - sy)}{ust} = 0.$$

Ceci conduit à définir $S^{-1}M$ comme suit.

Sur l'ensemble $M \times S$ on considère la relation suivante. On pose :

$$(m, s) \sim (m', t) \Leftrightarrow \quad \text{il existe } u \in S \text{ tel que } u(tm - sm') = 0.$$

Cette relation est clairement réflexive et symétrique. Elle est aussi transitive. En effet, si

$$(x, s) \sim (y, t) \sim (z, u),$$

il existe $v, v' \in S$ tels que $v(tx - sy) = 0 = v'(uy - tz)$. Alors

$$vv'utx = svv'uy = svv'tz, \qquad \text{d'où } vv't(ux - sz) = 0,$$

et $tvv' \in S$ puisque S est stable par multiplication. Ceci montre que $(x, s) \sim (z, u)$ et donc $\sim$ est une relation d'équivalence.

On note $S^{-1}M$ l'ensemble des classes d'équivalence et, pour tout $(m, s) \in M \times S$, on désigne par m/s son image dans $S^{-1}M$. On définit sur $S^{-1}M$ une addition par la formule suivante :

$$(1) \qquad \frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}.$$

Il faut vérifier que cette formule fait sens. Supposons que x'/s' soit un autre représentant de la classe x/s, et montrons que

$$(*) \qquad \frac{tx' + s'y}{s't} = \frac{tx + sy}{st}.$$

Par hypothèse, il existe $u \in \mathrm{S}$ tel que $us'x = usx'$, alors

$$u\left(st(tx' + s'y) - s't(tx + sy)\right) = t^2u(sx' - s'x) = 0$$

et donc l'égalité $(*)$ a lieu. Ceci montre que, dans (1), le terme de droite ne dépend que de la classe x/s (et non du couple (x, s)). De même, ce terme ne dépend que de la classe y/t. Ceci montre que l'addition (1) est bien définie.

On vérifie alors facilement qu'elle est associative et commutative, que $0/1$ est un élément 0, et que $-m/1$ est l'opposé de $m/1$. Donc, $\mathrm{S}^{-1}\mathrm{M}$ est un groupe abélien, et l'application

$$\tau_{\mathrm{M}} : \mathrm{M} \longrightarrow \mathrm{S}^{-1}\mathrm{M}, \qquad m \mapsto m/1$$

est un morphisme de groupes abéliens.

De plus, lorsque $\mathrm{M} = \mathrm{A}$, on définit sur $\mathrm{S}^{-1}\mathrm{A}$ une multiplication par la formule suivante :

$$\frac{x}{s}\frac{y}{t} = \frac{xy}{st}. \tag{2}$$

À nouveau, il faut vérifier que cette formule fait sens, c.-à-d., que si x'/s' est un autre représentant de la classe x/s, on a :

$$\frac{x'y}{s't} = \frac{xy}{st}. \tag{$**$}$$

Par hypothèse, il existe $u \in \mathrm{S}$ tel que $us'x = usx'$, alors

$$u(s'txy - stx'y) = tyu(s'x - sx') = 0,$$

d'où $(**)$. Ceci montre que, dans (2), le terme de droite ne dépend que de la classe x/s ; de même, il ne dépend que de la classe y/t. Ceci montre que la multiplication (2) est bien définie. On vérifie alors facilement qu'elle est associative, distributive sur l'addition, et que $1/1$ est un élément unité. Donc, $\mathrm{S}^{-1}\mathrm{A}$ est un anneau, et l'application

$$\tau_{\mathrm{A}} : \mathrm{A} \longrightarrow \mathrm{S}^{-1}\mathrm{A}, \qquad a \mapsto a/1$$

est un morphisme d'anneaux.

Enfin, revenant à M arbitraire, on définit une action de $\mathrm{S}^{-1}\mathrm{A}$ sur $\mathrm{S}^{-1}\mathrm{M}$ par la formule

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}. \tag{3}$$

On vérifie, comme précédemment, que ceci est bien défini et fait de $\mathrm{S}^{-1}\mathrm{M}$ un $\mathrm{S}^{-1}\mathrm{A}$-module.

En particulier, $\mathrm{S}^{-1}\mathrm{M}$ est un A-module par restriction des scalaires via $\tau_{\mathrm{A}} : \mathrm{A} \to \mathrm{S}^{-1}\mathrm{A}$, c.-à-d., pour $a \in \mathrm{A}$, $m \in \mathrm{M}$, on a

$$a \cdot \frac{m}{1} = \frac{a}{1} \cdot \frac{m}{1} = \frac{am}{1}.$$

Ceci montre que l'application $\tau_{\mathrm{M}} : \mathrm{M} \to \mathrm{S}^{-1}\mathrm{M}$, $m \mapsto m/1$, est un morphisme de A-modules. Attention, ce morphisme n'est en général pas injectif ! Plus précisément, il résulte de la construction que

$$\operatorname{Ker} \tau_{\mathrm{M}} = \{m \in \mathrm{M} \mid \exists\, s \in \mathrm{S} \text{ tel que } sm = 0\}.$$

En résumé, on a donc obtenu le théorème suivant.

Théorème 4.6. — 1) $\mathrm{S}^{-1}\mathrm{A}$ *est un anneau, et* $\tau_{\mathrm{A}} : \mathrm{A} \to \mathrm{S}^{-1}\mathrm{A}$, $a \mapsto a/1$ *est un morphisme d'anneaux ; son noyau est l'idéal*

$$\operatorname{Ker} \tau_{\mathrm{A}} = \{a \in \mathrm{A} \mid \exists\, s \in \mathrm{S} \textit{ tel que } sa = 0\}.$$

2) $\mathrm{S}^{-1}\mathrm{M}$ *est un* $\mathrm{S}^{-1}\mathrm{A}$*-module, et* $\tau_{\mathrm{M}} : \mathrm{M} \to \mathrm{S}^{-1}\mathrm{M}$, $m \mapsto m/1$ *est un morphisme de* A*-modules. Son noyau est le sous-*A*-module*

$$\operatorname{Ker} \tau_{\mathrm{M}} = \{m \in \mathrm{M} \mid \exists\, s \in \mathrm{S} \textit{ tel que } sm = 0\}.$$

4.2.1. Le cas intègre. — Dans le cas où A est intègre, la construction de $\mathrm{S}^{-1}\mathrm{A}$ se simplifie un peu, pour deux raisons. D'une part, la relation d'équivalence sur $\mathrm{A} \times \mathrm{S}$ est définie, plus simplement, par

$$(*) \qquad (a, s) \sim (b, t) \Leftrightarrow at = bs.$$

Notant a/s l'image de (a, s) dans l'ensemble quotient $\mathrm{S}^{-1}\mathrm{A}$, la structure d'anneau est définie, comme précédemment, par

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st}, \qquad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}.$$

(Le fait que ces formules font sens résulte du calcul fait dans le cas général, où se vérifie directement par un calcul analogue, un peu plus simple.)

D'autre part, le morphisme d'anneaux $\mathrm{A} \to \mathrm{S}^{-1}\mathrm{A}$, $a \mapsto a/1$ est **injectif**. En effet, si $a/1 = 0 = 0/1$ alors $(*)$ et l'intégrité de A entraînent $a = 0$. On peut donc, cette fois, considérer A comme un sous-anneau de $\mathrm{S}^{-1}\mathrm{A}$.

De plus, comme A est intègre, on peut prendre comme partie multiplicative $\mathrm{S} = \mathrm{A} \setminus \{0\}$; dans ce cas, l'anneau $\mathrm{S}^{-1}\mathrm{A}$ obtenu, que nous noterons K, est un corps. En effet, tout élément non nul de K est de la forme as^{-1}, avec $a \neq 0$, donc admet sa^{-1} pour inverse. On appelle K le **corps des fractions de** A.

Exemples 4.7. — 1) $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$.

2) Soit k un corps et soit $\mathrm{A} = k[\mathrm{X}]$ l'anneau des polynômes à coefficients dans k ; c'est un anneau intègre, puisque si P, Q sont non nuls alors

$$\deg(\mathrm{PQ}) = \deg(\mathrm{P}) + \deg(\mathrm{Q}).$$

Son corps des fractions est le corps des fractions rationnelles

$$k(\mathrm{X}) = \left\{ \frac{\mathrm{P}(\mathrm{X})}{\mathrm{Q}(\mathrm{X})} \;\middle|\; \mathrm{P}, \mathrm{Q} \in k[\mathrm{X}],\, \mathrm{Q} \neq 0 \right\}.$$

TABLE DES MATIÈRES

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[ChL] A. Chambert-Loir, Algèbre corporelle, Presses de l'École polytechnique, 2005.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Ne04] J. Nekovàř, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekovar/co/ln

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.

[Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.