2 Anneaux, idéaux, modules, propriétés de finitude, anneaux de polynômes

Version du 23 octobre 2005

5 Anneaux et idéaux

5.1 Anneaux et corps

Définition 5.1.1 *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.,*

(i) *$+$ est associative, c.-à-d., $a + (b + c) = (a + b) + c$, pour tout $a, b, c \in A$.*

(ii) *$+$ est commutative, c.-à-d., $a + b = b + a$, pour tout $a, b \in A$.*

(iii) *A possède un élément 0 tel que $0 + a = a$ pour tout $a \in A$.*

(iv) *Tout $a \in A$ 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 $a, b, c \in A$), 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 $a, b, c \in A$, 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...).

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

Remarque 5.1.2 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 parfois commode de s'autoriser à considérer l'anneau nul (une raison est de ne pas avoir à exclure le cas $I = A$ 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 $M_n(\mathbb{C})$ et certaines de leurs généralisations s'introduisent naturellement, même si l'on s'intéresse à un anneau commutatif A.

Exemple 5.1.3 Soit A un anneau commutatif et soit $n \geq 2$. On note $M_n(A)$ l'ensemble des matrices à coefficients dans A, muni des lois usuelles d'addition et de multiplication des matrices. Montrez que $M_n(A)$ est un anneau non-commutatif.

Définition 5.1.4 *Soit A un anneau. On dit qu'un élément $a \in A \setminus \{0\}$ est* **inversible** *s'il existe $a' \in A$ 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 $A^\times$ l'ensemble des éléments inversibles de A.*

Exercice 5.1.1 Quels sont les éléments inversibles de $\mathbb{Z}$, de $\mathbb{Z}[i]$, de $M_n(\mathbb{C})$?

Définition 5.1.5 *Un* **corps** *est un anneau commutatif $k \neq \{0\}$ dans lequel tout élément non nul est inversible.*

Définition 5.1.6 *On dit que l'anneau A est* **intègre** *(en anglais : A is a domain) s'il est non nul et vérifie : $a, b \in A \setminus \{0\} \Rightarrow ab \neq 0$.*

Convention Dans ce cours, tous les anneaux considérés seront supposés commutatifs, à une exception près (les anneaux d'endomorphismes, qui seront brièvement considérés). On convient donc que dans la suite le mot anneau signifie anneau commutatif, sauf mention explicite du contraire.

5.2 Idéaux

Soit A un anneau (commutatif, comme convenu plus haut).

Définition 5.2.1 *Un* **idéal** I *de* A *est un sous-ensemble non-vide qui est un sous-groupe pour l'addition (c.-à-d.,* $x, y \in I \Rightarrow x - y \in I$*) et qui est stable par multiplication par tout élément de* A*, c.-à-d. :*

$$\forall x \in I, \forall a \in A, \quad ax \in I.$$

Deux exemples immédiats sont : l'idéal nul, noté (0), et l'anneau A tout entier, qu'on désignera parfois par (1), voir ci-dessous. Voici d'autres exemples.

Exemples 5.2.2 1) Soit $A = \mathbb{Z}$, et k un entier. On note $(k) = \{nk \mid n \in \mathbb{Z}\}$. C'est un idéal de $\mathbb{Z}$.

2) Soient $A = \mathbb{C}[X]$ et $\lambda \in \mathbb{C}$. On pose $I_\lambda = \{P \in \mathbb{C}[X] \mid P(\lambda) = 0\}$. C'est un idéal de $\mathbb{C}[X]$.

Proposition 5.2.3 *Soit* S *une partie non-vide de* A*. L'ensemble de toutes les sommes finies de la forme*

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

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

Réciproquement, soit I un idéal de A contenant S. Alors I contient toute somme de la forme $(*)$, et donc I contient (S). Ceci prouve que (S) est le plus petit idéal de A contenant S, et on l'appellera l'idéal engendré par S. □

Pour $S = \{0\}$, (0) est l'idéal nul, et pour $S = \{1\}$ on a $(1) = A$. Ceci justifie les notations introduites plus haut. D'autre part, si S est un ensemble fini, disons $S = \{x_1, \ldots, x_r\}$, on désignera (S) aussi par

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

Exercice 5.2.1 On suppose connue la division euclidienne dans $\mathbb{C}[X]$. 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 $X - \lambda$).

Définition 5.2.4 (Somme et produit d'idéaux) *Soient I, J des idéaux de A.*

1) On désigne par $I + J$ l'idéal engendré par $I \cup J$. Il résulte de la proposition 5.2.3 que $I + J$ est l'ensemble des éléments $x + y$, avec $x \in I$ et $y \in J$.

2) On désigne par IJ l'idéal engendré par les produits xy, pour $x \in I$ et $y \in J$. Il résulte de la proposition 5.2.3 que IJ est l'ensemble de toutes les sommes finies

$$\sum_{i=1}^{n} x_i y_i,$$

pour $n \geq 1$, $x_i \in I$, $y_i \in J$. (Attention, en général l'ensemble des produits xy, avec $x \in I$ et $y \in J$, n'est pas stable par addition !)

6 Modules

6.1 Groupes abéliens et $\mathbb{Z}$-modules

Définition 6.1.1 *Soit M un groupe abélien. Pour tout $x \in M$ et $n \in \mathbb{N}^*$, on pose*

$$\begin{aligned} nx &= x + \cdots + x \quad (n \text{ fois}), \\ (-n)x &= -(nx) = -x - \cdots - x \quad (n \text{ fois}). \end{aligned}$$

On pose aussi $0x = 0$ (où le zéro est celui de $\mathbb{Z}$ à gauche, et celui de M à droite). On vérifie facilement que l'application $\mathbb{Z} \times M \to M$, $(n, x) \mapsto nx$, ainsi définie, vérifie les trois propriétés suivantes :

1) (bi-additivité) : $n(x + x') = nx + nx'$, $(n + n')x = nx + n'x$;
2) ("associativité") : $n(n'x) = (nn')x$;
3) ("unité") : $1x = x$.

Par conséquent, un groupe abélien est un $\mathbb{Z}$-module, au sens de la définition introduite dans le paragraphe suivant.

6.2 A-modules et sous-A-modules

Soit A un anneau, toujours supposé commutatif.

Définition 6.2.1 *Un* A**-module** *est un groupe abélien* M *muni d'une application* $A \times M \to M$, *notée* $(a, m) \mapsto am$, *vérifiant les trois propriétés suivantes (où* $a, b \in A$, $m, m' \in M$*) :*

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

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

Remarque 6.2.2 D'après 1), on a $0m = (0 + 0)m = 0m + 0m$ et donc $0m = 0$, pour tout $m \in M$.

Exemples 6.2.3 1) A est un A-module, et ses sous-modules sont les idéaux.

2) Si $A = \mathbb{Z}$, un $\mathbb{Z}$-module n'est rien d'autre qu'un groupe abélien.

3) Si $A = k$ est un corps, un k-module n'est rien d'autre qu'un k-espace vectoriel.

Proposition 6.2.4 *Soit* M *un* A*-module et soit* S *un sous-ensemble de* M. *L'ensemble de toutes les sommes finies de la forme*

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

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* S *est un ensemble fini, disons* $S = \{x_1, \ldots, x_r\}$, *on désignera* (S) *aussi par*

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

Démonstration. Analogue à celle pour les idéaux (Prop. 5.2.3), et laissée au lecteur. □

Définition 6.2.5 (Somme de sous-modules)
Soient $M_1, \ldots, M_n$ *des sous-modules de* M. *On désigne par* $M_1 + \cdots + M_n$, *ou* $\sum_{i=1}^{n} M_i$, *le sous-module engendré par* $M_1 \cup \cdots \cup M_n$. *Il résulte de la proposition 6.2.4 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 6.2.6 *Soient $M_1, \ldots, M_n$ des sous-modules de M. On dit qu'ils 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 $x_i \in M_i \cap \sum_{j \neq i} M_j$. Alors on peut écrire $-x_i = \sum_{j \neq i} x_j$, avec $x_j \in M_j$, d'où

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

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

Le lemme suivant est important et sera utilisé de façon répétée.

Lemme 6.2.7 *Soit $M_0 \subseteq M_1 \subseteq \cdots$ une suite croissante de sous-A-modules de M. Alors, leur réunion*

$$\bigcup_{i \geq 0} M_i$$

est un sous-A-module de M.

Démonstration. On fait la démonstration sous une hypothèse un peu plus générale : il suffit de supposer que la famille de sous-modules $\{M_i\}_{i \in \mathbb{N}}$ est **filtrante**, c.-à-d., vérifie la propriété suivante :

$$(\text{filt}) \qquad \forall i, j, \quad \exists \ell \geq i, j \ \text{ tel que } \ M_i + M_j \subseteq M_\ell.$$

(Bien sûr, toute suite croissante est une famille filtrante ; il suffit de prendre $\ell = \max\{i, j\}$). Sous cette hypothèse, montrons que $U := \bigcup_{i\in\mathbb{N}} M_i$ est un sous-A-module de M.

Soient $a \in A$ et $x, y \in U$. Alors, il existe $i, j \in \mathbb{N}$ tels que $x \in M_i$ et $y \in M_j$ et donc, comme la famille est filtrante, il existe ℓ tel que $x, y \in M_\ell$. Comme M_ℓ est un sous-module, on a $x + ay \in M_\ell$, et donc $x + ay \in U$. Ceci prouve le lemme. □

6.3 Construction de modules (I) : sommes directes finies

Soient $M_1, \ldots, M_n$ des A-modules.

Définition 6.3.1 *Le groupe abélien*

$$M_1 \times \cdots \times M_n = \{(m_1, \ldots, m_n) \mid m_i \in M_i\}$$

(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*

$$M_1 \oplus \cdots \oplus M_n \quad \textit{ou} \quad \bigoplus_{i=1}^{n} M_i.$$

Remarque 6.3.2 Posons $S = \bigoplus_{j=1}^{n} M_j$. Si on identifie chaque $m_i \in M_i$ 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.

Définition 6.3.3 *Si tous les M_i sont égaux à un même A-module M, la somme directe $M \oplus \cdots \oplus M$ (n copies) sera désignée par M^n ou $M^{\oplus n}$.*

6.4 Morphismes et isomorphismes

L'identification, faite plus haut, de M_i à un sous-module de $\bigoplus_{j=1}^{n} M_j$ est un cas particulier de morphisme (et ici, isomorphisme) de A-modules.

Définition et proposition 6.4.1 *Soient M, N deux groupes abéliens. Un* **morphisme de groupes abéliens** *$f : M \to N$ est une application $M \to N$ 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 $x, y \in M$.*

Démonstration. $f(0) = f(0+0) = f(0) + f(0)$ donne $f(0) = 0$, puis

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

donne $f(-x) = -f(x)$. □

Définition 6.4.2 *Soient M, N deux A-modules. Un* **morphisme de A-modules** *$f : M \to N$ est un morphisme de groupes abéliens tel que $f(am) = af(m)$ pour tout $a \in A, m \in M$.*

Définition 6.4.3 *Soit $f : M \to N$ un morphisme de A-modules. On dit que f est un* **isomorphisme** *s'il existe un morphisme de A-modules $g : N \to M$ tel que $gf = \mathrm{id}_M$ et $fg = \mathrm{id}_N$.*

Proposition 6.4.4 *Soit $f : M \to N$ 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 $n, n' \in N$ 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. La proposition est démontrée. □

6.5 Modules de type fini

Définition 6.5.1 *On dit qu'un A-module M est* **de type fini** *s'il est engendré par un nombre fini d'éléments, c.-à-d., s'il existe $x_1, \ldots, x_n \in M$ tels que*

$$M = Ax_1 + \cdots + Ax_n,$$

c.-à-d., si tout $m \in M$ s'écrit $m = a_1x_1 + \cdots + a_nx_n$, avec $a_i \in A$.

Exemples 6.5.2 1) Le A-module A est de type fini : il est engendré par l'élément 1 puisque $a = a1$ pour tout $a \in A$.

2) Plus généralement, pour tout $n \geq 1$, la somme directe

$$A^n = \{(a_1, \ldots, a_n) \mid a_i \in A\}$$

est un A-module de type fini. En effet, introduisons les éléments

$$e_1 = (1, 0, \ldots, 0), \quad \cdots \quad , e_n = (0, \ldots, 0, 1).$$

(Si $A = k$ est un corps, alors les e_i sont simplement les vecteurs de la base canonique de k^n.) Alors, tout élément $\underline{a} = (a_1, \ldots, a_n)$ de A^n s'écrit (de façon unique)

$$\underline{a} = a_1 e_1 + \cdots + a_n e_n.$$

3) Le $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ est de type fini, puisqu'il est engendré par l'élément $\dot{1}$. Par contre, ici, l'écriture n'est pas unique puisque $a\dot{1} = b\dot{1}$ si $a - b \in n\mathbb{Z}$.

Remarque 6.5.3 Attention, un sous-module d'un module de type fini n'est pas nécessairement de type fini. Cette "pathologie" ne se produit pas pour les anneaux et modules noethériens, qu'on va étudier dans la section suivante.

On connaît déjà un exemple d'anneau non noethérien : l'anneau $\mathcal{A}$ des entiers algébriques de $\mathbb{C}$. Et en effet, si $\alpha_0 \in \mathcal{A}$ est un élément non inversible (par exemple, $\alpha_0 = 2$), et si α_n désigne une racine 2^n-ème de α, la suite d'idéaux

$$(*) \qquad (\alpha_0) \subset (\alpha_1) \subset (\alpha_2) \subset \cdots$$

est strictement croissante. En effet, si on avait $(\alpha_{n-1}) = (\alpha_n)$, il existerait β tel que

$$\alpha_n = \beta \alpha_{n-1} = \beta \alpha_n^2,$$

donc α_n serait inversible, et $\alpha_0 = \alpha_n^{2^n}$ aussi, une contradiction. Il en résulte que l'idéal

$$I = \bigcup_{n \geq 0} (\alpha_n)$$

n'est pas de type fini. En effet, s'il était engendré par un nombre fini d'éléments $x_1, \ldots, x_r$, ces éléments seraient tous dans un certain (α_n), et la suite $(*)$ serait stationnaire à partir du cran n, une contradiction.

Cette contradiction montre que l'idéal I de $\mathcal{A}$ n'est pas de type fini, bien que ce soit un sous-$\mathcal{A}$-module de $\mathcal{A}$ (qui est engendré comme $\mathcal{A}$-module par l'élément 1).

Exercice 6.5.1 On suppose que $A = k$ est un corps. Soit V un k-espace vectoriel. Montrer que V est un k-module de type fini ssi $\dim_k V < \infty$.

7 Modules et anneaux noethériens

7.1 Modules noethériens

Soit A un anneau commutatif et M un A-module.

Proposition 7.1.1 *Les conditions suivantes sont équivalentes.*

1) *Tout sous-module de M est de type fini ;*

2) *Toute suite croissante de sous-modules de M est stationnaire, c.-à-d., pour toute suite croissante de sous-modules*

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$

il existe un entier k tel que $N_k = N_i$ pour tout $i \geq k$.

3) *Toute famille non-vide de sous-modules de M admet un élément maximal.*

Démonstration. 1) $\Rightarrow$ 2) Supposons 1) vérifiée et soit

$$(*) \qquad N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$

une suite croissante de sous-modules. Posons $N = \bigcup_{i\geq 0} N_i$; c'est un sous-module de M. Par hypothèse, il est engendré par un nombre fini d'éléments $x_1, \ldots, x_k$. Alors, il existe un entier r tel que $x_1, \ldots, x_k$ appartiennent tous à N_r. Donc $N = N_r$ et la suite $(*)$ est stationnaire à partir du cran r.

2) $\Rightarrow$ 3) Supposons qu'une famille non-vide $\mathcal{F}$ de sous-modules de M ne possède pas d'élément maximal. Soit N_0 un élément de $\mathcal{F}$. Comme il n'est pas maximal, il est contenu strictement dans un élément N_1 de $\mathcal{F}$. Ce dernier n'étant pas maximal, par hypothèse, il est contenu strictement dans un élément N_2 de $\mathcal{F}$. On construit ainsi une suite strictement croissante

$$N_0 \subset N_1 \subset N_2 \subset \cdots$$

de sous-modules de M, en contradiction avec l'hypothèse 2).

3) $\Rightarrow$ 1) Soit N un sous-module de M et soit $\mathcal{F}$ la famille des sous-modules de type fini de N. Elle est non-vide, car elle contient le sous-module (0). Donc, elle possède un élément maximal N'. Soit $n \in N$ arbitraire. Alors $N' + An$ est un sous-module de N de type fini (car il est engendré par n et un système de générateurs de N'). Par maximalité de N', on a $N' = N' + An$, d'où $n \in N'$. Ceci montre que $N' = N$, et donc N est de type fini. La proposition est démontrée. □

Définition 7.1.2 *On dit que M est un module* **noethérien** *s'il vérifie les conditions équivalentes de la proposition précédente. (Ceci entraîne, en particulier, que M soit de type fini).*

7.2 Anneaux et modules noethériens

Soit A un anneau commutatif.

Définition 7.2.1 *On dit que A est* **noethérien** *s'il est noethérien comme A-module, c.-à-d., si tout idéal de A est de type fini.*

Proposition 7.2.2 *Supposons A noethérien et soit M un A-module de type fini. Alors M est noethérien.*

Démonstration. Par hypothèse, M est engendré comme A-module par un nombre fini d'éléments $x_1, \ldots, x_r$. On procède par récurrence sur r. Si $r = 0$, alors $M = \{0\}$ et il n'y a rien à montrer. Soit $r \geq 1$ et supposons avoir montré que le sous-module

$$M' = Ax_2 + \cdots + Ax_r$$

est noethérien. Soit N un sous-module arbitraire de M.

Posons $N' = N \cap M'$. C'est un sous-module de M' donc, par l'hypothèse de récurrence, il est engendré par un nombre fini d'éléments $y_1, \ldots, y_t$.

D'autre part, notons I l'ensemble des $a \in A$ tels qu'il existe $n \in N$ tel que $n = ax_1 + \sum_{i=2}^{r} c_i x_i$, c.-à-d., tel que $n - ax_1 \in M'$. On voit facilement que I est un idéal de A. Donc, comme A est noethérien, I est engendré par un nombre fini d'éléments $\alpha_1, \ldots, \alpha_s$. Par définition, il existe $n_1, \ldots, n_s \in N$ tels que

$$n_i - \alpha_i x_1 \in M', \quad \forall i = 1, \ldots, s. \tag{1}$$

Maintenant, soit $n \in N$ arbitraire. Comme $M = Ax_1 + \cdots + Ax_r$, il existe $a \in A$ tel que

$$n - ax_1 \in M'; \tag{2}$$

alors $a \in I$ et donc il existe $b_1, \ldots, b_s \in A$ tels que $a = b_1\alpha_1 + \cdots + b_s\alpha_s$. Or, on déduit de (1) que $b_i n_i - b_i \alpha_i x_1 \in M'$, pour tout $i = 1, \ldots, s$, d'où

$$\sum_{i=1}^{s} b_i n_i - ax_1 \in M'. \tag{2}$$

Soustrayant (2) de (1), on obtient que $n - \sum_{i=1}^{s} b_i n_i$ appartient à M'. Il appartient aussi à N, donc à $M' \cap N = N'$, donc, d'après l'hypothèse de récurrence, on a

$$n - \sum_{i=1}^{s} b_i n_i = c_1 y_1 + \cdots + c_t y_t,$$

pour certains $c_j \in A$. On a donc

$$n = \sum_{i=1}^{s} b_i n_i + \sum_{j=1}^{t} c_j y_t,$$

et comme n était arbitrairement choisi dans N, ceci montre que les éléments $b_1 n_1, \ldots, b_s n_s$ et $y_1, \ldots, y_t$ engendrent N. Donc N est de type fini. La proposition est démontrée. □

Remarque 7.2.3 On disposera d'une démonstration plus facile lorsqu'on disposera du concept de module quotient. En effet, dire que M est de type fini équivaut à dire que c'est un quotient de A^n, pour un certain $n \geq 1$. Or on peut montrer que tout module quotient d'un module noethérien est noethérien, et que A^n est noethérien (voir Corollaire 9.3.4 plus loin).

8 Anneaux de polynômes et théorème de transfert de Hilbert

Dans cette section, A est un anneau commutatif.

8.1 L'anneau de polynômes $A[X]$

De la même façon qu'on a défini $\mathbb{C}[X]$, on peut définir l'anneau de polynômes $A[X]$.

Définition 8.1.1 *L'anneau $A[X]$ est le groupe abélien formé de toutes les sommes finies $\sum_{i=0}^{d} a_i X^i$, où $d \in \mathbb{N}$ et $a_i \in A$, muni de la multiplication définie par :*

$$(*) \qquad \left(\sum_{i=0}^{d} a_i X^i\right)\left(\sum_{j=0}^{f} b_j X^j\right) = \sum_{\ell=0}^{d+f}\left(\sum_{\substack{i,j\geq 0\\ i+j=\ell}} a_i b_j\right) X^\ell.$$

En particulier, $(a1)(b1) = (ab)1$ *et donc* A *s'identifie à un sous-anneau de* $A[X]$ *et* $A[X]$ *est un* A*-module.*

De plus, tout élément $P \neq 0$ *dans* $A[X]$ *s'écrit de façon unique* $P = a_n X^n + \cdots + a_0$*, avec* $a_n \neq 0$*. On dit que* n *est le degré de* P *(noté* $\deg P$*), et que* a_n *est le coefficient dominant de* P*.*

Proposition 8.1.2 *Pour tout* $P, Q \in A[X]\setminus\{0\}$*, on a* $\deg(PQ) \leq \deg(P) + \deg(Q)$*, et on a l'égalité si* A *est intègre.*

En particulier, $A[X]$ *est intègre si* A *l'est.*

Démonstration. Écrivons $P = \sum_{i=0}^{d} a_i X^i$ et $Q = \sum_{j=0}^{f} b_j X^j$, avec $a_d \neq 0$ et $b_f \neq 0$. L'inégalité $\deg(PQ) \leq d + f$ résulte de la formule $(*)$ définissant le produit PQ. De plus, le coefficient dans PQ de X^{d+f} est $a_d b_f$, qui est $\neq 0$ si A est intègre. Ceci prouve la proposition. □

Exercice 8.1.1 Supposons A intègre. Montrez que les seuls éléments inversibles de $A[X]$ sont les éléments inversibles de A (si P est inversible, considérer le degré de PP^{-1}).

Théorème 8.1.3 (Division euclidienne dans $A[X]$ **par un polynôme unitaire)**

Soit $U \in A[X]\setminus\{0\}$ *un polynôme dont le coefficient dominant est* **inversible**. *Alors, on peut faire dans* $A[X]$ *la division euclidienne par* U*, c.-à-d., pour tout* $P \in A[X]$*, il existe un unique couple* (Q, R) *d'éléments de* $A[X]$ *tels que* $P = UQ + R$ *et* $\deg R < \deg U$*.*

On appelle Q *et* R *le quotient et le reste de la division euclidienne de* P *par* U*.*

Démonstration. **Unicité** Soient (Q, R) et (Q', R') deux couples vérifiant les propriétés ci-dessus. Alors, on a

$$(*) \qquad U(Q - Q') = R' - R.$$

Si $Q - Q'$ était non nul, disons de degré n, alors, puisque le coefficient dominant de U est inversible, $U(Q - Q')$ serait de degré $n + \deg U \geq \deg U$. Or, $R' - R$ est, par hypothèse, de degré $< \deg U$. Donc, nécessairement, $Q = Q'$ et $R = R'$. Ceci prouve l'unicité.

Existence Écrivons $U = \alpha X^d + a_{d-1} X^{d-1} + \cdots + a_0$. Par hypothèse, le coefficient dominant α est inversible dans A. Montrons l'existence par récurrence sur $n = \deg P$.

Si $n < d$, on peut prendre $Q = 0$ et $R = P$. On peut donc supposer $n \geq d$ et l'existence démontrée pour tout polynôme de degré $< n$. Écrivons

$$P = b_n X^n + \cdots + b_0.$$

Alors, $P - b_n \alpha^{-1} U X^{n-d}$ est de degré $< n$. Donc, par hypothèse de récurrence, il existe $Q_0, R \in A[X]$, avec $\deg R < d$ tels que

$$P - b_n \alpha^{-1} U X^{n-d} = UQ_0 + R.$$

Alors, $P = U(Q_0 + b_n \alpha^{-1} X^{n-d}) + R$. Ceci montre l'existence. Le théorème est démontré. □

On en déduit, en particulier, le théorème suivant.

Théorème 8.1.4 (Division euclidienne dans $k[X]$) *Soit k un corps.*

1) *$k[X]$ est intègre et, pour tout $U \in k[X] \setminus \{0\}$, on peut faire la division euclidienne par U.*

2) *Tout idéal de $k[X]$ est* **principal**, *c.-à-d., engendré par un élément. Plus précisément, soit I un idéal non nul de $k[X]$ et soit $U \in I$ un polynôme de degré minimal. Alors $I = (U)$. En particulier, $k[X]$ est noethérien.*

3) *$k[X]$ est un anneau factoriel.*

Démonstration. Le point 1) résulte de ce qui précède, et le point 2) en découle, comme dans la démonstration de 1.2.2.

De plus, tout élément de $k[X]$ s'écrit comme un produit fini d'éléments irréductibles : ceci peut se voir directement, par récurrence sur le degré, ou se déduire de la proposition 2.6.4.

Enfin, comme tout idéal de $k[X]$ est principal, tout élément irréductible vérifie le Lemme d'Euclide (voir la preuve de 1.2.5). Par conséquent, $k[X]$ est factoriel. □

Remarque 8.1.5 Pour décrire $A[X]$ comme A-module, on est conduit à introduire la notion de A-module libre sur un ensemble de générateurs arbitraire (c.-à-d., non nécessairement fini), voir plus loin.

8.2 Le théorème de transfert de Hilbert

Théorème 8.2.1 (Théorème de transfert de Hilbert) *Si A est noethérien, $A[X]$ l'est aussi.*

Démonstration. Soit I un idéal non nul de $A[X]$. Soit D le sous-ensemble de A formé de 0 et des coefficients dominants des polynômes $\neq 0$ appartenant à I. On voit facilement que D est un idéal de A. Par hypothèse, il est engendré par des éléments $\alpha_1, \ldots, \alpha_r$.

Pour tout $i = 1, \ldots, r$, soit P_i un élément de I dont le coefficient dominant est α_i, et soit $d_i = \deg P_i$. Soit d le plus grand des d_i, et soit M le sous-A-module de $A[X]$ engendré par les monômes $1, X, \ldots, X^{d-1}$. Alors M est noethérien, d'après la proposition 7.2.2.

Soit $N = M \cap I$; c'est un sous-A-module de M. Alors N est de type fini, donc engendré comme A-module par des éléments $Q_1, \ldots, Q_s$. Alors, I est égal à l'idéal J engendré par

$$P_1, \ldots, P_r, Q_1, \ldots, Q_s.$$

En effet, montrons par récurrence sur n que tout élément $P \neq 0$ de I, de degré n, appartient à J. C'est clair si $n < d$, car dans ce cas $P \in N$ donc est combinaison A-linéaire de $Q_1, \ldots, Q_s$. Soit donc $n \geq d$ et supposons l'assertion établie pour tout $n' < n$. Soit $P \in I \setminus \{0\}$, de degré n, et soit α son coefficient dominant. Alors $\alpha \in D$ donc il existe $a_1, \ldots, a_r \in A$ tels que

$$\alpha = a_1\alpha_1 + \cdots + a_r\alpha_r.$$

Alors,

$$a_1\alpha_1 X^{n-d_1} P_1 + \cdots + a_r\alpha_r X^{n-d_r} P_r$$

a pour terme dominant αX^n, et donc

$$P - \sum_{i=1}^{r} a_i\alpha_i X^{n-d_i} P_i$$

est un élément de I de degré $< n$. Il appartient donc à J, par hypothèse de récurrence. Enfin, comme les P_i sont dans I, on a aussi $P \in J$. Ceci prouve le théorème. □

Remarque 8.2.2 En anglais, le théorème précédent est appelé "Hilbert's Basis Theorem".

8.3 Construction de modules (II) : modules libres

Définition 8.3.1 *Soit M un A-module et soit B un sous-ensemble de M. On dit que B est une* **partie libre** *de M si les éléments de B sont linéairement indépendants sur A, c.-à-d., si la propriété suivante est vérifiée :*

Pour tout $n \geq 1$, si $\beta_1, \ldots, \beta_n \in B$ sont deux à deux distincts et si $a_1\beta_1 + \cdots + a_n\beta_n = 0$, alors $a_i = 0$ pour tout $i = 1, \ldots, n$.

(Noter que, même si B est un ensemble infini, la condition ci-dessus ne fait intervenir qu'un nombre fini d'éléments de B.)

Définition 8.3.2 *Soit M un A-module. On dit qu'un sous-ensemble B de M est une* **base** *de M s'il vérifie les deux propriétés suivantes :*

1) B engendre M, c.-à-d., tout $m \in M$ s'écrit comme combinaison A-linéaire d'un nombre fini d'éléments de B, c.-à-d., sous la forme

$$m = \sum_{i=1}^{n} a_i\beta_i,$$

avec $n \in \mathbb{N}^*$, $\beta_i \in B$ et $a_i \in A$.

2) B est une partie libre de M.

Il résulte de 1) et 2) que tout $m \neq 0$ dans M s'écrit de façon **unique** *comme une somme finie*

$$m = \sum_{i=1}^{n} a_i\beta_i,$$

où $n \geq 1$, $\beta_i \in B$ et $a_i \neq 0$ pour tout $i = 1, \ldots, n$.

Définition 8.3.3 *On dit que M est un A-module* **libre** *s'il possède une base.*

Exemples 8.3.4 1) Le A-module A possède la base $\{1\}$. Donc A est un A-module libre.

2) Plus généralement, pour tout $n \geq 1$, le A-module

$$A^n = \{(a_1, \ldots, a_n) \mid a_i \in A\}$$

est un A-module libre. En effet, il possède la base $B = (e_1, \ldots, e_n)$, où :

$$e_1 = (1, 0, \ldots, 0), \quad \cdots \quad , e_n = (0, \ldots, 0, 1).$$

3) Le A-module $A[X]$ possède la base $\{X^n\}_{n\geq 0}$. Donc $A[X]$ est un A-module libre.

4) Considérons l'anneau $A = \mathbb{Z}$ et le $\mathbb{Z}$-module $M = \mathbb{Z}/n\mathbb{Z}$ (où $n > 1$). Alors M ne possède pas de base comme $\mathbb{Z}$-module. En effet, pour tout $x \in M$ on a $nx = 0$, et donc la condition 2) de la définition n'est vérifiée pour aucun sous-ensemble B de M. Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module libre.

Réciproquement, pour tout ensemble I, il existe un A-module $A^{(I)}$ ayant une base paramétrée par I. On le construit en deux étapes, de la façon suivante.

Définition 8.3.5 *Soit A^I l'ensemble* **produit**, *c.-à-d.,*

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

est l'ensemble des familles paramétrées par I d'éléments de A. C'est un groupe abélien, l'addition étant définie composante par composante. C'est aussi un A-module, pour la loi

$$a \cdot (b_i)_{i\in I} = (ab_i)_{i\in I}.$$

Pour tout $i \in I$, notons e_i la famille $(\delta_{ij})_{j\in I}$, où δ_{ij} est le symbole de Kronecker, *c.-à-d.,*

$$\delta_{ij} = \begin{cases} 1 & \text{si } j = i; \\ 0 & \text{sinon.} \end{cases}$$

Lemme 8.3.6 *Les éléments e_i, pour $i \in I$, sont linéairement indépendants sur A.*

Démonstration. C'est clair. □

Définition 8.3.7 *On note $A^{(I)}$ le sous-A-module de A^I engendré par les éléments e_i, pour $i \in I$. Alors, d'après le lemme précédent, l'ensemble $B = \{e_i, i \in I\}$ est une base de $A^{(I)}$.*

Proposition 8.3.8 *$A^{(I)}$ est l'ensemble de toutes les sommes finies*

$$\sum_{j\in J} a_j e_j,$$

où J est un sous-ensemble **fini** *de I, et $a_j \in A$.*

Démonstration. C'est la définition du sous-A-module engendré par $B = \{e_i, i \in I\}$. □

Remarque 8.3.9 1) Si $I = \{1, \ldots, n\}$ alors $A^{(I)}$ égale A^I et s'identifie au A-module A^n déjà considéré, de base $(e_1, \ldots, e_n)$.

2) Si $I = \mathbb{N}$, on peut identifier le A-module libre $A^{(\mathbb{N})}$, avec sa base $\{e_i\}_{i\in\mathbb{N}}$, au A-module libre $A[X]$, avec sa base $\{X^i\}_{i\in\mathbb{N}}$.

Remarque 8.3.10 Toute partie libre X de A est nécessairement réduite à un seul élément. En effet, entre deux éléments distincts $a, b \in A$ on a toujours la relation de dépendance linéaire non triviale :

$$b \cdot a - a \cdot b = 0.$$

Remarque 8.3.11 Si k est un corps et V un k-espace vectoriel, on sait que les bases de V sont aussi caractérisées comme étant les parties libres maximales, ou les parties génératrices minimales. Dans le cas d'un anneau, ces deux propriétés sont strictement plus faibles que le fait d'être une base, comme le montrent les deux exemples suivants. Prenons $A = \mathbb{Z}$.

1) La partie $\{2\}$ est libre, car si $0 = n \cdot 2 = 2n$ alors $n = 0$. (Plus généralement, dans un anneau intègre A, tout singleton $\{a\}$ avec $a \neq 0$ est une partie libre). La partie $\{2\}$ est libre maximale, d'après la remarque précédente. Pourtant $\{2\}$ n'engendre pas $\mathbb{Z}$: le sous-module engendré est $2\mathbb{Z}$, l'idéal formé des entiers pairs.

2) La partie $\{2, 3\}$ est génératrice, car l'idéal engendré contient $1 = 3 - 2$ donc est égal à $\mathbb{Z}$. Comme aucune des sous-parties $\{2\}$ ou $\{3\}$ n'engendre $\mathbb{Z}$, alors $X = \{2, 3\}$ est une partie génératrice minimale. Mais ce n'est pas une base, car elle n'est pas libre, d'après la remarque précédente. (On a $3 \cdot 2 - 2 \cdot 3 = 0$).

8.4 Anneaux de polynômes en plusieurs variables

Soit A un anneau commutatif. On va généraliser la construction de l'anneau de polynômes $A[X]$, au cas de n indéterminées $X_1, \ldots, X_n$. Commençons par le cas $n = 2$, c.-à-d., le cas de deux indéterminées X et Y.

Définition 8.4.1 *Soit $A[X, Y]$ le A-module libre de base les monômes $X^r Y^s$, pour $(r, s) \in \mathbb{N}^2$. On définit le degré d'un tel monôme comme étant $r + s$.*

Tout élément non nul $P \in A[X, Y]$ est une somme finie de termes $a_{r,s} X^r Y^s$, avec $a_{r,s} \in A$, et le plus grand des degrés $r + s$ tel que $a_{r,s} \neq 0$ s'appelle le degré de P et se note $\deg P$ *; ainsi P peut s'écrire comme somme finie*

$$P = \sum_{\substack{(r,s)\in\mathbb{N}^2 \\ r+s\leq n}} a_{r,s} X^r Y^s,$$

où $n = \deg P$. *On munit* $A[X,Y]$ *de la multiplication définie par*

$$\left(\sum_{\substack{(r,s)\in\mathbb{N}^2\\ r+s\le m}} a_{r,s}X^rY^s\right)\left(\sum_{\substack{(t,u)\in\mathbb{N}^2\\ t+u\le n}} b_{t,u}X^tY^u\right) = \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^2\\ \alpha+\beta\le m+n}}\left(\sum_{\substack{(r,s),(t,u)\in\mathbb{N}^2\\ r+t=\alpha,\, s+u=\beta}} a_{r,s}b_{t,u}\right)X^\alpha Y^\beta.$$

Ceci se généralise de façon évidente au cas de n variables. Toutefois, pour alléger l'écriture, il est utile d'observer que $\mathbb{N}^n$ est muni de l'addition définie composante par composante par

$$(\nu_1,\dots,\nu_n)+(\eta_1,\dots,\eta_n)=(\nu_1+\eta_1,\dots,\nu_n+\eta_n).$$

De plus, pour tout $\nu=(\nu_1,\dots,\nu_n)$ dans $\mathbb{N}^n$, on pose $|\nu|=\nu_1+\cdots+\nu_n$ et l'on note X^ν le monôme

$$X_1^{\nu_1}\cdots X_n^{\nu_n};$$

il est de degré $|\nu|$. On peut alors définir l'anneau de polynômes $A[X_1,\dots,X_n]$ comme suit.

Proposition 8.4.2 *Soit* $A[X_1,\dots,X_n]$ *le* A*-module libre de base les monômes*

$$X^\nu := X_1^{\nu_1}\cdots X_n^{\nu_n},$$

pour $\nu\in\mathbb{N}^n$, *un tel monôme étant de degré* $|\nu|$.

Tout élément $P\in A[X_1,\dots,X_n]$ *est une somme finie de termes* $a_\nu X^\nu$, *avec* $a_\nu\in A$, *et le plus grand des degrés* $|\nu|$ *tels que* $a_\nu\neq 0$ *s'appelle le degré de* P *et se note* $\deg P$ *; ainsi* P *peut s'écrire comme somme finie*

$$P=\sum_{\substack{\nu\in\mathbb{N}^r\\ |\nu|\le n}} a_\nu X^\nu,$$

où $n=\deg P$. *On munit* $A[X_1,\dots,X_n]$ *de la multiplication définie par*

$$\left(\sum_{\substack{\nu\in\mathbb{N}^r\\ |\nu|\le m}} a_\nu X^\nu\right)\left(\sum_{\substack{\eta\in\mathbb{N}^r\\ |\eta|\le n}} b_\eta X^\eta\right)=\sum_{\substack{\mu\in\mathbb{N}^r\\ |\mu|\le m+n}}\left(\sum_{\substack{\nu,\eta\in\mathbb{N}^r\\ \nu+\eta=\mu}} a_\nu b_\eta\right)X^\mu.$$

Exercice 8.4.1 Soit $A = \mathbb{C}[X, Y]$. Montrer que l'idéal (X, Y) de A n'est pas un A-module libre. (S'il était libre alors, d'après la remarque 8.3.10, il serait engendré par un unique élément $a \in A$. Écrivant $X = aP$ et $Y = aQ$, considérer les degrés de a, P, Q et obtenir une contradiction.)

8.5 Morphismes d'anneaux et A-algèbres

Définition 8.5.1 *Soient A, B deux anneaux, non nécessairement commutatifs. Un* **morphisme d'anneaux** *$f : A \to B$ 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* $a, b \in A$ *;*
(ii) $f(ab) = f(a)f(b)$*, pour tout* $a, b \in A$ *;*
(iii) $f(1) = 1$*.*

Remarque 8.5.2 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)*.

Définition 8.5.3 *Soit B un anneau. Un sous-ensemble A de B 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_B ; dans ce cas, l'inclusion $A \subseteq B$ est un morphisme d'anneaux. Réciproquement, si $f : A \to B$ est un morphisme injectif, alors on peut identifier A à son image $f(A)$, qui est un sous-anneau de B.*

Définition 8.5.4 *Soit $f : A \to B$ un morphisme d'anneaux. On dit que f est un* **isomorphisme** *d'anneaux s'il existe un morphisme d'anneaux $g : B \to A$ tel que $gf = \mathrm{id}_A$ et $fg = \mathrm{id}_B$.*

Proposition 8.5.5 *Soit $f : A \to B$ 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. Analogue à celle de la Proposition 6.4.4. □

La notion de morphisme d'anneaux vaut pour des anneaux non nécessairement commutatifs. Par contre, pour la notion de A-algèbre introduite ci-dessous, on se limite exclusivement à des anneaux **commutatifs**.

Définition 8.5.6 *Soient A, B deux* **anneaux commutatifs**. *On dit que B est une A-***algèbre** *si l'on s'est donné un morphisme d'anneaux $\phi : A \to B$. Dans ce cas, B est aussi un A-module, via*

$$a \cdot b = \phi(a)b, \qquad \forall a \in A, b \in B.$$

Exemple 8.5.7 Si A est un sous-anneau de B, alors B est une A-algèbre. Par exemple, l'anneau de polynômes $A[X_1, \ldots, X_n]$ est une A-algèbre.

Exemple 8.5.8 Soit B un anneau commutatif. L'application $\mathbb{Z} \to B$, $n \mapsto n1_B$ est un morphisme d'anneaux. Par conséquent, tout anneau commutatif est une $\mathbb{Z}$-algèbre.

Remarque 8.5.9 Soit $n > 1$. Le morphisme composé

$$\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})[X]$$

fait de $(\mathbb{Z}/n\mathbb{Z})[X]$ une $\mathbb{Z}$-algèbre, et ϕ n'est ni injectif ni surjectif.

Définition 8.5.10 *Soient $\phi : A \to B$ et $\psi : A \to C$ deux A-algèbres. Un* **morphisme de A-algèbres** *$f : B \to C$ est un morphisme d'anneaux tel que $f \circ \phi = \psi$.*

Se rappelant que ϕ (resp. ψ) fait de B (resp. C) un A-module via $a \cdot b = \phi(a)b$ (resp. $a \cdot c = \psi(a)c$), la seconde condition équivaut à dire que f est A-linéaire, c.-à-d., vérifie $f(a \cdot b) = a \cdot f(b)$, pour tout $a \in A$, $b \in B$.

Remarque 8.5.11 Si A est un sous-anneau de B et de C, un morphisme de A-algèbres $f : B \to C$ est simplement un morphisme d'anneaux $f : B \to C$ tel que $f(a) = a$, pour tout $a \in A$.

8.6 A-algèbres et propriété universelle des algèbres de polynômes

Soit A un anneau commutatif.

Théorème 8.6.1 (Propriété universelle de $A[X_1, \ldots, X_n]$)
Soit $\rho : A \to B$ une A-algèbre. Pour tout n-uplet $(b_1, \ldots, b_n)$ d'éléments de B, il existe un unique morphisme de A-algèbres

$$\phi : A[X_1, \ldots, X_n] \to B$$

prolongeant ρ et tel que $\phi(X_i) = b_i$, pour $i = 1, \ldots, n$.

Démonstration. Un tel morphisme, s'il existe, doit vérifier, pour tout $P = \sum_{|\nu| \leq \deg P} a_\nu X^\nu$,

$$(*) \qquad \phi(P) = \sum_{|\nu| \leq \deg P} \rho(a_\nu) b_1^{\nu_1} \cdots b_n^{\nu_n}.$$

Réciproquement, l'application $\phi : A[X_1, \ldots, X_n] \to B$ définie par la formule $(*)$ est A-linéaire et vérifie $\phi(1) = 1$. Il reste à vérifier que $\phi(PQ) = \phi(P)\phi(Q)$, pour tout $P, Q \in A[X_1, \ldots, X_n]$. Par bilinéarité, il suffit de le vérifier lorsque $P = X^\nu$ et $Q = X^\eta$ sont des monômes. Mais alors c'est clair, car

$$\phi(X^{\nu+\eta}) = b_1^{\nu_1+\eta_1} \cdots b_n^{\nu_n+\eta_n} = b_1^{\nu_1} \cdots b_n^{\nu_n} \cdot b_1^{\eta_1} \cdots b_n^{\eta_n}.$$

Ceci prouve le théorème. □

Exercice 8.6.1 Montrer que l'on a un isomorphisme de A-algèbres

$$A[X_1, \ldots, X_n] \cong (A[X_1, \ldots, X_{n-1}])[X_n].$$

9 Modules et anneaux quotients, théorèmes d'isomorphisme de Noether

9.1 Définition des modules quotients

Soit A un anneau commutatif. Soient 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

$$x \sim y \Leftrightarrow x - y \in N.$$

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

On définit ensuite l'addition par

$$(*) \qquad (x + N) + (y + N) = x + y + N.$$

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 $x+N$ (resp. $y+N$) 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 $n,n'\in N$, alors

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

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

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

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

$$\pi : M\to M/N,\quad x\mapsto x+N$$

(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

$$(**)\qquad a(x+N)=ax+N.$$

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

On obtient alors facilement que $(**)$ munit M/N d'une structure de A-module, telle que la projection $\pi : M\to M/N$ 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 :

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

ce qui montre que l'addition et l'action de A sont définies par $(*)$ et $(**)$. On a donc démontré le théorème suivant.

Théorème 9.1.1 *Il existe une unique structure de A-module sur M/N telle que la projection $\pi : M\to M/N$ soit un morphisme de A-modules.*

De plus, 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. D'autre part, il est clair que

$$(\dagger) \qquad M' \subseteq \pi^{-1}(\pi(M')).$$

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 le théorème suivant.

Théorème 9.1.2 *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.*

En d'autres termes, tout sous-module L de M/N s'écrit $L = M'/N$, pour un unique sous-module M' de M contenant N, et l'on a $M' = \pi^{-1}(L)$.

Remarque 9.1.3 Les deux théorèmes précédents s'appliquent en particulier au cas des groupes abéliens (c.-à-d., le cas $A = \mathbb{Z}$).

9.2 Noyaux et images, théorèmes de Noether

Définition et proposition 9.2.1 *Soit $f : M \to N$ un morphisme de A-modules. Le* **noyau** *de f est*

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

*c'est un sous-module de M. L'***image** *de f est*

$$\mathrm{Im}(f) = f(M) = \{f(x) \mid x \in M\};$$

c'est un sous-module de N.

Démonstration. On voit facilement que $\mathrm{Ker}(f)$ est un sous-module de M. Soient $a \in A$ et $y, y' \in \mathrm{Im}(f)$. Il existe $x, x' \in M$ tels que $f(x) = y$ et $f(x') = y'$; alors $y + ay'$ égale $f(x + ax')$ donc appartient à $\mathrm{Im}(f)$. Ceci montre que $\mathrm{Im}(f)$ est un sous-module de N. □

Remarque 9.2.2 1) Une application d'ensembles $f : X \to Y$ est bijective si, et seulement si, elle est injective et surjective.

2) Soit $f : M \to N$ un morphisme de A-modules. Alors

f est surjectif $\Leftrightarrow \mathrm{Im}(f) = N$;
f est injectif $\Leftrightarrow \mathrm{Ker}(f) = 0$.

Le premier point est clair, ainsi que l'implication $\Rightarrow$ du second. Réciproquement, supposons $\mathrm{Ker}(f) = 0$ et soient $x, x' \in M$ tels que $f(x) = f(x')$. Alors $f(x - x') = 0$ et donc $x - x' = 0$.

Corollaire 9.2.3 *Soit $f : M \to N$ un morphisme de A-modules. Alors f est un isomorphisme ssi* $\mathrm{Ker}(f) = 0$ *et* $\mathrm{Im}(f) = N$.

Démonstration. Ceci résulte de la remarque précédente et de la proposition 6.4.4. □

Théorème 9.2.4 (Propriété universelle de M/N)
Soient M un A-module et N un sous-module. Notons π la projection $M \to M/N$. Le module quotient M/N possède la propriété universelle suivante :

> *Soit $f : M \to P$ un morphisme de A-modules tel que $f(N) = 0$, c.-à-d., $N \subseteq \mathrm{Ker}(f)$. Alors, f se factorise de façon unique à travers M/N, c.-à-d., il existe un unique morphisme de A-modules*
>
> $$\bar{f} : M/N \to \mathrm{Im}(f) \subseteq P$$
>
> *tel que $\bar{f} \circ \pi = f$.*

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

$$\bar{f}(m + M') = f(m).$$

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

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

Ceci prouve que $\bar{f}$ est un morphisme de A-modules. □

Théorème 9.2.5 (Théorème fondamental d'isomorphisme) (*pour les A-modules*)
Soit $f : M \to N$ un morphisme de A-modules. Alors, f induit un isomorphisme de A-modules

$$\bar{f} : M/\operatorname{Ker}(f) \xrightarrow{\sim} \operatorname{Im}(f).$$

Démonstration. D'après le théorème précédent appliqué à $N = \operatorname{Ker}(f)$, on obtient un morphisme surjectif

$$\bar{f} : M/\operatorname{Ker}(f) \twoheadrightarrow \operatorname{Im}(f).$$

Donc, d'après le corollaire 9.2.3, il reste à voir que $\bar{f}$ est injectif. Soit $\overline{m} = m + \operatorname{Ker}(f) \in \operatorname{Ker}(\bar{f})$. Alors

$$0 = \bar{f}(\overline{m}) = f(m)$$

donc $m \in \operatorname{Ker}(f)$ et $\overline{m} = 0$. Ceci prouve le théorème. □

Corollaire 9.2.6 (1er théorème d'isomorphisme)
Soient M, N deux sous-modules d'un A-module E. L'inclusion $M \hookrightarrow M + N$ induit un isomorphisme de A-modules :

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

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

Corollaire 9.2.7 (2ème théorème d'isomorphisme)
Soient $M \supseteq N \supseteq P$ des A-modules. Alors :

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

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

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

Démonstration. Considérons les projections $\pi_N : M \to M/N$ et $\pi_P : M \to M/P$. Comme $P \subseteq N = \operatorname{Ker}(\pi_N)$, alors π_N induit l'application

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

telle que $\phi \circ \pi_P = \pi_N$. Le noyau de ϕ est l'ensemble des classes $m + P$ telles que $m + N = 0$, c.-à-d., telles que $m \in N$; c'est donc le sous-module N/P de M/P. Ceci prouve le point 1), et le point 2) résulte alors du théorème fondamental d'isomorphisme 9.2.5. □

9.3 Applications des modules quotients

Proposition 9.3.1 *Soient M un A-module et N un sous-module.*

1) *Si M est de type fini, M/N l'est aussi.*

2) *Si N et M/N sont de type fini, alors M l'est aussi.*

Démonstration. Notons π la projection $M \to M/N$.
1) Supposons M engendré par des éléments $x_1, \ldots, x_n$. Alors tout $m \in M$ s'écrit

$$m = a_1 x_1 + \cdots + a_n x_n,$$

et donc $\pi(m) = a_1\pi(x_1) + \cdots + a_n\pi(x_n)$. Ceci montre que M/N est engendré par $\pi(x_1), \ldots, \pi(x_n)$, donc de type fini.

2) On suppose N et M/N de type fini. Soient $y_1, \ldots, y_s \in N$ des générateurs de N et soient $x_1, \ldots, x_r \in M$ dont les images engendrent M/N. Soit $m \in M$ arbitraire. Alors, il existe $a_1, \ldots, a_r \in A$ tels que

$$\pi(m) = a_1\pi(x_1) + \cdots + a_r\pi(x_r),$$

d'où $m - \sum_{i=1}^r a_i x_i \in N$.

Donc, il existe $b_1, \ldots, b_s \in A$ tels que

$$m - \sum_{i=1}^{r} a_i x_i = b_1 y_1 + \cdots + b_s y_s.$$

Par conséquent, $m = \sum_{i=1}^r a_i x_i + \sum_{j=1}^s b_j y_j$. Comme m était arbitrairement choisi dans M, ceci montre que M est engendré par $x_1, \ldots, x_r, y_1, \ldots, y_s$. La proposition est démontrée. □

Proposition 9.3.2 *Soient M un A-module, N un sous-module, et $Q = M/N$ le module quotient.*

1) *Si M est noethérien, N et Q le sont aussi.*

2) *Réciproquement, si N et Q sont noethériens, M l'est aussi.*

Démonstration. 1) Supposons M noethérien et soit N', resp. Q', un sous-module de N, resp. Q. Comme N' est un sous-module de M, il est de type

fini. D'autre part, on a $Q' = M'/N$, où $M' = \pi^{-1}(Q')$ est un sous-module de M. Par hypothèse, M' est de type fini, donc Q' l'est aussi, d'après la proposition précédente.

2) Supposons N et $Q = M/N$ noethériens et notons π la projection $M \to Q$. Soit M' un sous-module arbitraire de M. Alors $M' \cap N$ est un sous-module de N, donc est de type fini. D'autre part,

$$\frac{M'}{M' \cap N} \cong \pi(M')$$

est un sous-module de Q, donc est de type fini. Par conséquent, d'après la proposition précédente, M' est de type fini. Ceci montre que M est noethérien. □

Corollaire 9.3.3 *Soit $M_1, \cdots, M_n$ un nombre fini de modules noethériens. Alors $M_1 \oplus \cdots \oplus M_n$ est noethérien.*

Démonstration. Supposons d'abord $n = 2$. Alors M_1 est un sous-module de $M_1 \oplus M_2$ et, d'après le 1er théorème d'isomorphisme (corollaire 9.2.6), le module quotient $(M_1 \oplus M_2)/M_1$ est isomorphe à M_2. Donc, dans ce cas, le corollaire résulte du point 2) de la proposition précédente.

Enfin, le cas général s'en déduit par récurrence, puisque pour tout $n \geq 3$ l'on a

$$M_1 \oplus \cdots \oplus M_n \cong (M_1 \oplus \cdots \oplus M_{n-1}) \oplus M_n.$$

Le corollaire est démontré. □

On peut maintenant obtenir une démonstration plus conceptuelle, et peut-être plus simple à retenir, de la proposition 7.2.2.

Corollaire 9.3.4 *Soient A un anneau noethérien et M un A-module de type fini. Alors M est noethérien.*

Démonstration. Par hypothèse, il existe $x_1, \ldots, x_n \in M$ tels que

$$M = Ax_1 + \cdots + Ax_n.$$

Alors, l'application $\phi : A^n \to M$ définie par

$$\phi(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n$$

est un morphisme surjectif de A-modules. Donc, d'après le théorème fondamental d'isomorphisme 9.2.5, M s'identifie au module quotient $A^n/\operatorname{Ker}(\phi)$.

Or, d'après le corollaire précédent, A^n est noethérien, et donc M l'est aussi, d'après le point 1) de la proposition 9.3.2. □

9.4 Anneaux quotients

Dans ce paragraphe, on considère des anneaux non nécessairement commutatifs.

Définition 9.4.1 *Soit $\phi : A \to B$ un morphisme d'anneaux, non nécessairement commutatifs. Son noyau*

$$\mathrm{Ker}(\phi) = \{a \in A \mid \phi(a) = 0\}$$

est un **idéal bilatère** *de A, c.-à-d., un sous-groupe abélien I qui vérifie $AI = I$ et $IA = A$ (c.-à-d., $ax \in I$ et $xa \in I$; pour tout $x \in I$ et $a \in A$).*

D'autre part, l'image $\phi(A) = \{\phi(a) \mid a \in A\}$ est un sous-anneau de B.

Remarque 9.4.2 Si A est un anneau commutatif, un idéal bilatère n'est rien d'autre qu'un idéal.

Soit I un idéal bilatère arbitraire de A. On construit l'anneau quotient A/I de la façon suivante. D'abord, on dispose du groupe abélien quotient A/I, avec la projection canonique $\pi : A \to A/I$. 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

$$(a + I)(b + I) = ab + I, \tag{1}$$

pour tout $a, b \in A$. Pour vérifier que cette formule fait sens, il faut, à nouveau, vérifier que si a' (resp. b') est un autre représentant de la classe $a + I$ (resp. $b + I$), 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 $h, h' \in I$, alors

$$a'b' = (a + h)(b + h') = ab + ah' + hb + hh', \tag{2}$$

et chacun des trois produits ah', hb, et hh' appartient à I. Ceci montre que la formule (1) a bien un sens (c.-à-d., le terme de droite est bien défini). On vérifie alors aussitôt, en utilisant cette formule, que la multiplication est associative, commutative et distributive sur l'addition, que la classe $1 + I$ est l'élément unité, et que π est un morphisme d'anneaux. Ceci prouve la première assertion du théorème suivant.

Théorème 9.4.3 (Existence et propriété universelle de A/I)

Soient A un anneau et I un idéal bilatère de A.

1) *Il existe sur A/I une unique structure d'anneau telle que la projection canonique $\pi : A \to A/I$ soit un morphisme d'anneaux.*

2) *L'anneau A/I vérifie la propriété universelle suivante. Tout morphisme d'anneaux $\phi : A \to B$ tel que $\phi(I) = 0$ se factorise de façon unique à travers A/I, c.-à-d., il existe un unique morphisme d'anneaux $\overline{\phi} : (A/I) \to B$ tel que $\overline{\phi} \circ \pi = \phi$.*

Démonstration. On a déjà vu le 1er point, et la preuve du second est analogue à celle du théorème 9.2.4. □

Dans la suite du cours, on s'intéressera à des anneaux commutatifs A mais on aura besoin (à deux occasions) d'appliquer la propriété universelle du théorème précédent pour un anneau B non commutatif (un anneau d'endomorphismes). Ce cas mis à part, on ne rencontrera pas d'anneaux non commutatifs. Pour cette raison, on énonce les résultats qui suivent dans le cas d'anneaux commutatifs, bien qu'ils soient valables en général.

Théorème 9.4.4 (Théorème fondamental d'isomorphisme) (*pour les anneaux commutatifs*)
Soit $f : A \to B$ un morphisme d'anneaux commutatifs, et soit $C = f(A)$ son image. Alors C est un sous-anneau de B et f induit un isomorphisme d'anneaux

$$\bar{f} : A/\operatorname{Ker}(f) \cong C.$$

Démonstration. On a déjà vu que C est un sous-anneau de B, que $\operatorname{Ker}(f)$ est un idéal de A, et que f induit un isomorphisme de groupes abéliens

$$\bar{f} : A/\operatorname{Ker}(f) \xrightarrow{\sim} C.$$

Ceci étant, on voit facilement que $\bar{f}$ est un morphisme d'anneaux : avec des notations évidentes, on a

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

Enfin, comme $\bar{f}$ est bijectif, c'est un isomorphisme d'anneaux de $A/\operatorname{Ker}(f)$ sur C. □

Enfin, on a la proposition suivante, qui décrit les idéaux de A/I et dont la démonstration est laissée au lecteur. (Elle est analogue à celle du théorème 9.1.2.)

Proposition 9.4.5 *Les applications $K \mapsto \pi^{-1}(K)$ et $J \mapsto \pi(J) = J/I$ sont des bijections réciproques entre l'ensemble des idéaux de A/I et l'ensemble des idéaux de A contenant I.*

En d'autres termes, tout idéal K de A/I s'écrit $K = J/I$, pour un unique idéal J de A contenant I, et l'on a $J = \pi^{-1}(K)$.

Remarque 9.4.6 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". L'exemple de base est celui des anneaux $\mathbb{Z}/n\mathbb{Z}$.

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 le paragraphe suivant.

9.5 Algèbres de fonctions polynomiales

Définition 9.5.1 *Soit E un ensemble quelconque. On note $\mathcal{F}(E, \mathbb{C})$ l'algèbre de toutes les applications $E \to \mathbb{C}$.*

Tout polynôme $P \in \mathbb{C}[X_1, \ldots, X_n]$ définit une fonction (polynomiale) $\mathbb{C}^n \to \mathbb{C}$, $(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n)$, que, par abus de notation, on notera encore P. On obtient ainsi un morphisme d'algèbres

$$\mathbb{C}[X_1, \ldots, X_n] \to \mathcal{F}(\mathbb{C}^n, \mathbb{C}), \quad P \mapsto P.$$

Pour tout sous-ensemble E de $\mathbb{C}^n$, on obtient ainsi, par restriction à E, un morphisme d'algèbres

$$\phi_E : \mathbb{C}[X_1, \ldots, X_n] \to \mathcal{F}(E, \mathbb{C}), \quad P \mapsto P|_E,$$

et le noyau de ϕ_E, noté $I(E)$, est l'idéal formé des polynômes s'annulant en tout point de E :

$$I(E) = \{P \in \mathbb{C}[X_1, \ldots, X_n] \mid P(x) = 0, \quad \forall x \in E\}.$$

Par définition, l'algèbre des fonctions polynomiales sur E est l'algèbre quotient

$$\mathbb{C}[X_1, \ldots, X_n]/I(E).$$

Si E est un sous-ensemble de $\mathbb{C}^n$ défini par des équations polynomiales, c.-à-d., s'il existe $P_1, \ldots, P_m \in \mathbb{C}[X_1, \ldots, X_n]$ tels que

$$E = \{x = (x_1, \ldots, x_n) \in \mathbb{C}^n \mid P_j(x) = 0, \quad \forall j = 1, \ldots, m\}$$

alors le théorème des zéros de Hilbert (4.1.3) affirme que $I(E)$ est le **radical** de l'idéal $(P_1, \ldots, P_m)$, c.-à-d.,

$$I(E) = \{P \in \mathbb{C}[X_1, \ldots, X_n] \mid P^r \in (P_1, \ldots, P_m) \text{ pour un certain } r \geq 1\}.$$

Pour se familiariser avec ces algèbres quotients, on pourra essayer de traiter les deux exemples ci-dessous, proposés en exercice.

Exercice 9.5.1 1) Soit $A = \mathbb{C}[X, Y]$ et soit E la courbe algébrique

$$E = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3\}.$$

On veut montrer que $I(E) = I$, où I est l'idéal engendré par $Y^2 - X^3$. On note x et y les images de X et Y dans A/I.

Montrer que tout élément de A/I s'écrit sous la forme $P(x)+yQ(x)$, avec $P, Q \in \mathbb{C}[X]$. (Faire, dans $(\mathbb{C}[X])[Y]$, la division euclidienne par $Y^2 - X^3$).

Soient $P, Q \in \mathbb{C}[X]$. Montrer que $P + YQ \in I(E)$ si, et seulement si, $P = 0 = Q$. (Observer que, pour tout $t \in \mathbb{C}$, le point (t^2, t^3) de $\mathbb{C}^2$ appartient à E.) En déduire que $I(E) = I$.

2) Soient $A = \mathbb{C}[U, V, W]$ et $B = \mathbb{C}[X, Y]$ et soit $f : A \to B$ le morphisme défini par $f(U) = X^2$, $f(V) = Y^2$ et $f(W) = XY$. Soit I l'idéal de A engendré par $UV - W^2$. On note u, v, w et les images de U, V, W dans A/I.

Montrer que tout élément de A/I s'écrit sous la forme $P(u,v)+wQ(u,v)$, avec $P, Q \in \mathbb{C}[U,V]$. (Faire, dans $(\mathbb{C}[U,V])[W]$, la division euclidienne par $W^2 - UV$).

Soient $P, Q \in \mathbb{C}[U,V]$. Montrer que $P + WQ \in \mathrm{Ker}(f)$ si, et seulement si, $P = 0 = Q$. **Indication** Pour tout $(x,y) \in \mathbb{C}^2$, on a

$$f(P + WQ)(x,y) = P(x^2, y^2) + xyQ(x^2, y^2).$$

Montrer que A/I est isomorphe au sous-anneau de B engendré par X^2, Y^2 et XY.

9.6 Anneaux d'endomorphismes et A/I-modules

Définition et proposition 9.6.1 *Soit M un groupe abélien. L'ensemble des* **endomorphismes** *de M, c.-à-d., des morphismes de groupe abélien $f : M \to M$, est noté* $\mathrm{End}(M)$. *Pour $f, g \in \mathrm{End}(M)$, on définit $f + g$ par*

$$(f + g)(m) = f(m) + g(m).$$

Ceci munit $\mathrm{End}(M)$ *d'une structure de groupe abélien. De plus,* $\mathrm{End}(M)$ *est un anneau non commutatif, la multiplication étant la composition des endomorphismes.*

Démonstration. Il faut d'abord vérifier que $f + g$ est bien un élément de $\mathrm{End}(M)$. Mais ceci est clair, car pour $m, n \in M$, on a

$$\begin{aligned}(f + g)(m + n) = f(m + n) + g(m + n) &= f(m) + f(n) + g(m) + g(n)\\ &= (f + g)(m) + (f + g)(n).\end{aligned}$$

Ensuite, on voit facilement que l'addition des endomorphismes est associative, commutative, et admet pour 0 le morphisme nul, et que tout endomorphisme f admet pour opposé le morphisme $-f : m \mapsto -f(m)$.

De plus, la composition des endomorphismes est associative, et admet pour élément neutre l'application identique $\mathrm{id}_M \in \mathrm{End}(M)$. Il reste à vérifier la distributivité. Soient $f, g, h \in \mathrm{End}(M)$. L'égalité $(g+h) \circ f = g \circ f + h \circ f$ résulte de la définition de l'addition. D'autre part, pour tout $m \in M$, on a

$$(f \circ (g + h))(m) = f(g(m) + h(m) \overset{*}{=} f(g(m)) + f(h(m)),$$

où dans l'égalité $(*)$ on a utilisé le fait que f est un morphisme de groupes abéliens. Ceci prouve que $f \circ (g + h) = f \circ g + f \circ h$. La proposition est démontrée. □

Proposition 9.6.2 *Soient A un anneau commutatif et M un groupe abélien. Se donner une structure de A-module*

$$\mu : A \times M \to M$$

équivaut à se donner un morphisme d'anneaux $\phi : A \to \mathrm{End}(M)$.

Démonstration. Supposons donné μ et définissons $\phi : A \to \mathrm{End}(M)$ par

$$\phi(a)(m) = \mu(a, m), \qquad \forall a \in A, m \in M.$$

L'axiome de bi-additivité assure que ϕ est bien à valeurs dans $\mathrm{End}(M)$, et est un morphisme de groupes abéliens. Les deux autres axiomes (associativité et unité) assurent que ϕ est un morphisme d'anneaux.

Réciproquement, supposé donné un morphisme d'anneaux $\phi : A \to \mathrm{End}(M)$, et posons $\mu(a, m) = \phi(a)(m)$, pour tout $a \in A$, $m \in M$. On vérifie facilement que ceci fait de M un A-module. □

Soient A un anneau commutatif et I un idéal de A. Notons π la projection $A \to A/I$. Tout A/I-module N est aussi un A-module via π, c.-à-d., l'action

$$a \cdot n = \pi(a)n \qquad \forall a \in A, n \in N,$$

fait de N un A-module. De plus, pour tout $x \in I$ on a $xN = 0$ (c.-à-d., $xn = 0$ pour tout $n \in N$) et donc, comme A-module, N est annulé par I.

Maintenant, soit M un A-module.

Définition 9.6.3 *On note IM le sous-module de M engendré par les éléments xm, pour $x \in I$ et $m \in M$. C.-à-d., IM est l'ensemble des sommes finies $x_1m_1 + \cdots + x_nm_n$, où $n \in \mathbb{N}^*$, $x_i \in I$, $m_i \in M$.*

On peut donc former le A-module quotient M/IM. Il est annulé par I puisque $Im \subseteq IM$ pour tout $m \in M$.

Théorème 9.6.4 1) *L'action de A sur M/IM se factorise en une action de A/I sur M, telle que*

$$(*) \qquad (a + I)(m + IM) = am + IM, \qquad \forall a \in A, m \in M.$$

2) *Tout morphisme de A-modules $f : M \to M'$ induit un morphisme de A/I-modules*

$$(**) \qquad \overline{f} : M/IM \to M'/IM', \qquad m + IM \mapsto f(m) + IM'.$$

En particulier, si $f = \mathrm{id}_M$ *alors* $\overline{f} = \mathrm{id}_{M/IM}$.

3) *Si* $g : M' \to M''$ *est un second morphisme de* A*-modules, alors* $\overline{g \circ f} = \overline{g} \circ \overline{f}$. *Par conséquent, si* f *est un isomorphisme, il en est de même de* $\overline{f}$.

Démonstration. 1) D'après la proposition 9.6.2, la structure de A-module sur M/IM équivaut à la donnée du morphisme d'anneaux

$$\phi : A \to \mathrm{End}(M)$$

défini par $\phi(a)(m) = am$. Par hypothèse, ce morphisme est nul sur I. Donc d'après la propriété universelle 9.4.3 de A/I (appliquée à l'anneau non-commutatif $B = \mathrm{End}(M)$), ϕ se factorise en un morphisme d'anneaux

$$\overline{\phi} : A/I \to \mathrm{End}(M),$$

et l'action $\overline{\mu} : (A/I) \times (M/IM)$ associée vérifie $(*)$.

2) Soient $\pi : M \to M/IM$ et $\pi' : M' \to M'/IM'$ les projections. Le morphisme de A-modules $\pi' \circ f$ est nul sur IM donc induit un morphisme de A-modules

$$\overline{f} : M/IM \to M'/IM', \qquad m + IM \mapsto f(m) + IM'.$$

En considérant M/IM et M'/IM' munis de leur structure de A/I-module définie par $(*)$, on voit facilement que $\overline{f}$ est un morphisme de A/I-module.

Enfin, en utilisant $(**)$ on voit facilement que $\overline{f} = \mathrm{id}_{M/IM}$ et que $\overline{g \circ f} = \overline{g} \circ \overline{f}$. Par conséquent, si f et g sont des isomorphismes réciproques l'un de l'autre, alors il en est de même de $\overline{f}$ et $\overline{g}$. Le théorème est démontré. □

Corollaire 9.6.5 *Un* A*-module annulé par* I *est la même chose qu'un* A/I*-module.*

Démonstration. On a déjà vu qu'un A/I-module peut être vu comme un A-module annulé par I. Réciproquement, si M est un A-module annulé par I, alors $IM = (0)$ et donc $M = M/IM$ est un A/I-module. □

10 Algèbres de type fini et noethérianité

10.1 Algèbres de type fini

Soit $\rho : A \to B$ une A-algèbre (où A, B sont des anneaux commutatifs). On rappelle que B est alors un A-module, via $a \cdot b = \rho(a)b$.

Définition et proposition 10.1.1 *Soit S un sous-ensemble non vide de B. On note $A[S]$ le sous-A-module de B engendré par tous les monômes*

$$(*) \qquad x_1^{\nu_1} \cdots x_n^{\nu_n}, \quad \text{où} \quad n \in \mathbb{N}^*, x_i \in S, \nu_i \in \mathbb{N}.$$

C'est une sous-A-algèbre de B, et c'est la plus petite sous-A-algèbre contenant S. On l'appelle la **sous-algèbre** *de B* **engendrée par** *S.*

Démonstration. Comme le produit de deux monômes du type $(*)$ est encore un monôme de même type, on voit facilement que $A[S]$ est une sous-algèbre contenant S. Réciproquement, soit C une sous-A-algèbre de B contenant S. Alors C contient tous les monômes de type $(*)$ et contient donc $A[S]$. Ceci démontre la proposition. □

Remarque 10.1.2 Si S est un ensemble fini $\{x_1, \ldots, x_n\}$, ce qui sera le cas dans la pratique, alors $A[S]$ est le sous-A-module de B engendré par les monômes

$$x^\nu := x_1^{\nu_1} \cdots x_n^{\nu_n}, \quad \text{où} \quad \nu \in \mathbb{N}^n.$$

Définition 10.1.3 *On dit que B est une* **A-algèbre de type fini** *si elle est engendrée comme A-algèbre par un nombre fini d'éléments $x_1, \ldots, x_n$. D'après ce qui précède, ceci signifie que tout élément de B peut s'écrire (de façon non unique en général) comme une combinaison A-linéaire finie de monômes $x_1^{\nu_1} \cdots x_n^{\nu_n}$.*

Proposition 10.1.4 *B est une A-algèbre de type fini $\Leftrightarrow$ B est isomorphe à un quotient d'une algèbre de polynômes $A[X_1, \ldots, X_n]$.*

Démonstration. Supposons B engendrée comme A-algèbre par $x_1, \ldots, x_n$. D'après la propriété universelle de l'algèbre $A[X_1, \ldots, X_n]$ (8.6.1), ρ se prolonge en un morphisme de A-algèbres $\phi : A[X_1, \ldots, X_n] \to B$ tel que $\phi(X_i) = x_i$ pour $i = 1, \ldots, n$. Ce morphisme est surjectif (car les x_i engendrent B comme algèbre), donc induit un isomorphisme de A-algèbres

$$(*) \qquad A[X_1, \ldots, X_n]/I \xrightarrow{\sim} B,$$

où $I = \mathrm{Ker}(\phi)$. Réciproquement, si l'on a un isomorphisme $(*)$, notons x_i l'image dans B de X_i. Alors les x_i engendrent B comme A-algèbre. Ceci prouve la proposition. □

10.2 Résultats de noethérianité

On rappelle que tous les anneaux considérés sont commutatifs.

Théorème 10.2.1 *Si A est noethérien, toute A-algèbre B de type fini est noethérienne.*

Démonstration. D'abord, grâce à l'isomorphisme

$$A[X_1, \ldots, X_n] \cong (A[X_1, \ldots, X_{n-1}])[X_n],$$

le théorème de transfert de Hilbert 8.2.1 entraîne, par récurrence sur n, que l'anneau $A[X_1, \ldots, X_n]$ est noethérien, pour tout $n \geq 1$.

Ensuite, soit B une A-algèbre de type fini. D'après la proposition 10.1.4, on a un isomorphisme

$$B \cong \mathcal{A}/I,$$

où $\mathcal{A} = A[X_1, \ldots, X_n]$, pour un certain $n \geq 1$, et où I est un idéal de $\mathcal{A}$. Alors, B est noethérien comme $\mathcal{A}$-module, d'après la proposition 9.3.2, et aussi comme B-module (puisque tout idéal de B est un sous-$\mathcal{A}$-module de B). Donc, B est un anneau noethérien. □

On déduit du théorème précédent la proposition suivante, dûe à Artin et Tate. Elle sera utilisée plus loin dans la preuve du Théorème des zéros de Hilbert.

Proposition 10.2.2 (Lemme d'Artin-Tate) *Soient $A \subseteq B \subseteq C$ des anneaux commutatifs. On suppose que A est noethérien, que C est une A-algèbre de type fini, et que C est de type fini comme $\underline{B\text{-module}}$. Alors, B est une A-algèbre de type fini. En particulier, B est noethérien.*

Démonstration. Soient $x_1, \ldots, x_m$ des générateurs de C comme A-algèbre, et soient $y_1, \ldots, y_n$ des générateurs de C comme $\underline{B\text{-module}}$. Alors, on a des expressions de la forme

$$x_r = \sum_{j=1}^{n} b_{rj} y_j \qquad (b_{rj} \in B); \tag{1}$$

$$y_i y_j = \sum_{k=1}^{n} b_{ijk} y_k \qquad (b_{ijk} \in B). \tag{2}$$

Soit B_0 la sous-A-algèbre de B engendrée par les éléments b_{ri} et b_{ijk}. C'est un anneau noethérien, d'après le théorème précédent.

D'autre part, en procédant par récurrence sur $|\nu|$, on déduit de (1) et (2) que tout monôme

$$x_1^{\nu_1} \cdots x_n^{\nu_n}$$

s'écrit comme combinaison linéaire $\beta_1 y_1 + \cdots + \beta_n y_n$, avec β_k dans B_0.

Comme tout $c \in C$ est une combinaison A-linéaire finie des monômes x^ν, on en déduit que C est engendré comme B_0-module par $y_1, \ldots, y_n$. Puisque B_0 est noethérien, il en résulte que C est un B_0-module noethérien.

Comme B est un sous-B_0-module de C, alors B est engendré comme B_0-module par un nombre fini d'éléments $z_1, \ldots, z_p$. Donc, tout élément de B s'écrit comme une combinaison A-linéaire finie de termes

$$\beta_t z_t,$$

pour $t = 1, \ldots, p$, où chaque β_t est un monôme en les b_{ri} et les b_{ijk}. Ceci montre, en particulier, que B est engendrée comme A-algèbre par les b_{ri}, les b_{ijk}, et les z_t. La proposition en découle. □

Références citées dans ce chapitre

[Pe1]

Bibliographie

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

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

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[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, 1979, et 2ème édition, 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.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

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

[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.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.