Université Pierre et Marie Curie
Master de Sciences et Technologie
Mention Mathématiques et Applications
1ère année
Algèbre et Théorie de Galois
2007-2008

Patrick Polo

I. LES ANNEAUX DE LA GÉOMÉTRIE ALGÉBRIQUE OU DE LA THÉORIE DES NOMBRES

1. Courbes algébriques et fonctions polynomiales

1.1. Courbes algébriques. — On note $\mathbb{C}$ le corps des nombres complexes. Soit $\mathrm{F} \in \mathbb{C}[\mathrm{X}, \mathrm{Y}]$ un polynôme à deux variables ; pour fixer les idées, considérons les exemples suivants :

$$\begin{aligned}
\mathrm{F}_1 &= \mathrm{Y}^2 - \mathrm{X}^3 \\
\mathrm{F}_2 &= \mathrm{Y}^2 - \mathrm{X}^2 - \mathrm{X}^3 \\
\mathrm{F}_3 &= \mathrm{Y}^2 - \mathrm{X}^2 \\
\mathrm{F}_4 &= \mathrm{Y}^3 - 2\mathrm{X}\mathrm{Y}^2 + \mathrm{X}^2\mathrm{Y} - \mathrm{X}^2(\mathrm{Y}^2 - 2\mathrm{X}\mathrm{Y} + \mathrm{X}^2) \\
\mathrm{F}_5 &= \mathrm{Y}^2 + \mathrm{X}^2(\mathrm{X} - 1)^2.
\end{aligned}$$

On note $\mathscr{C}(\mathrm{F})$, ou simplement $\mathscr{C}$ s'il n'y a pas d'ambiguïté, le sous-ensemble du plan complexe $\mathbb{C}^2$ suivant :

$$\mathscr{C}(\mathrm{F}) = \{(x, y) \in \mathbb{C}^2 \mid \mathrm{F}(x, y) = 0\}.$$

On obtient ainsi les exemples suivants :

$$\begin{aligned}
\mathscr{C}_1 &= \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3\} \\
\mathscr{C}_2 &= \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^2 + x^3\} \\
\mathscr{C}_3 &= \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^2\} \\
\mathscr{C}_4 &= \{(x, y) \in \mathbb{C}^2 \mid y^3 - 2xy^2 + x^2y = x^2(y^2 - 2xy + x^2)\} \\
\mathscr{C}_5 &= \{(x, y) \in \mathbb{C}^2 \mid y^2 + (x(x - 1))^2 = 0\}.
\end{aligned}$$

Un tel ensemble s'appelle une **courbe algébrique plane** : « plane » car c'est un sous-ensemble du plan complexe $\mathbb{C}^2$, et « algébrique » car définie par une équation polynomiale $\mathrm{F}(x, y) = 0$.

Exercice 1.1. — Tracer dans le plan réel $\mathbb{R}^2$ les analogues réels des "courbes" $\mathscr{C}_1$ à $\mathscr{C}_5$.

1.2. Fonctions polynomiales. — Dans la suite, on va noter $\mathbb{A}^2$ le plan affine $\mathbb{C}^2$ (c'est juste une notation). L'anneau des polynômes $\mathbb{C}[X, Y]$ peut être considéré comme l'anneau des **fonctions polynomiales** sur $\mathbb{C}^2 = \mathbb{A}^2$; on le notera donc

$$\mathbb{C}[\mathbb{A}^2].$$

Si V est un sous-ensemble de $\mathbb{C}^2$, notons

$$\mathscr{F}(V)$$

l'anneau de toutes les fonctions $V \to \mathbb{C}$. Alors, on a une application de restriction

$$\theta : \mathbb{C}[\mathbb{A}^2] \longrightarrow \mathscr{F}(\mathscr{C}(F)), \qquad P \mapsto P|_{\mathscr{C}(F)},$$

où $P|_{\mathscr{C}(F)}$ désigne la *restriction* de P à $\mathscr{C}(F)$. On note

$$\mathbb{C}[\mathscr{C}(F)]$$

l'image de θ, et on l'appelle l'anneau des fonctions polynomiales sur $\mathscr{C}(F)$. Donc, par définition, une *fonction polynomiale sur* $\mathscr{C}(F)$ est la restriction à $\mathscr{C}(F)$ d'une fonction polynomiale $P = P(X, Y) \in \mathbb{C}[X, Y]$.

Ainsi, par définition, l'application de restriction

$$\pi : \mathbb{C}[X, Y] \twoheadrightarrow \mathbb{C}[\mathscr{C}(F)]$$

est surjective (c'est la signification de la flèche $\twoheadrightarrow$). Remarquons que si $Q - P = RF$, avec $R \in \mathbb{C}[X, Y]$, alors P et Q ont même image dans $\mathbb{C}[\mathscr{C}(F)]$, puisque le polynôme RF est identiquement nul sur $\mathscr{C}(F)$. Introduisons

$$I := \{P \in \mathbb{C}[X, Y] \mid P(x, y) = 0, \quad \forall\, (x, y) \in \mathscr{C}(F)\}.$$

Alors

$$I = \{P \in \mathbb{C}[X, Y] \mid \pi(P) = 0\};$$

on dit que I est le **noyau** de π et on le note $\operatorname{Ker} \pi$ ou $\operatorname{Ker}(\pi)$. On voit facilement que pour tous $P_1, P_2 \in I$ et $R \in \mathbb{C}[X, Y]$ on a :

$$P_1 + RP_2 \in I;$$

ceci signifie que I est un **idéal** de $\mathbb{C}[X, Y]$ (sous-groupe stable par la multiplication par $R \in \mathbb{C}[X, Y]$ arbitraire).

Il résulte de ce qui précède que l'on peut identifier les éléments de $\mathbb{C}[\mathscr{C}(F)]$ aux **classes** $P + I$ d'éléments de $\mathbb{C}[X, Y]$ modulo I : tout élément de $\mathbb{C}[\mathscr{C}(F)]$

est par définition l'image par l'application de restriction π d'un polynôme P, et deux polynômes P et Q ont même image si et seulement si $P - Q \in I$.

On dit que $\mathbb{C}[\mathscr{C}(F)]$ est l'**anneau quotient**

$$\mathbb{C}[X, Y]/I.$$

Étudions l'exemple où $F = Y^2 - S(X)$, avec $S(X) = X^3$ ou $X^3 + X^2$, et montrons que **dans ce cas**, on a

$$I = (F) := \{RF \mid R \in \mathbb{C}[X, Y]\}.$$

On a déjà vu que $(F) \subseteq I$, et il s'agit ici de montrer l'inclusion réciproque. Soit $P \in I$ arbitraire, non nul. Considérons P comme élément de $\mathbb{C}[X][Y]$, c.-à-d., un polynôme en Y à coefficients dans $\mathbb{C}[X]$, et écrivons :

$$P = a_d(X)Y^d + \cdots + a_1(X)Y + a_0(X).$$

Comme $F = Y^2 - S(X)$ est un polynôme **unitaire** en Y (c.-à-d., coefficient dominant $= 1$), on peut faire la *division euclidienne* de P par F, c.-à-d.,

$$P_1 := P - a_d(X)Y^{d-2}F$$

est de degré $< d$ en Y, et le coefficient de Y^{d-1} est

$$a_{d-1}(X)$$

(inchangé car F n'a pas de terme de degré 1 en Y). Alors

$$P_2 := P_1 - a_{d-1}(X)Y^{d-3}F$$

est de degré $< d - 1$ en Y, et le coefficient de Y^{d-2} est

$$a_{d-2}(X) + a_d(X)S(X).$$

Alors,

$$P_3 := P_2 - \big(a_{d-2}(X) + a_d(X)S(X)\big)Y^{d-4}F$$

est de degré $< d - 2$ en Y. On peut continuer ainsi tant que le polynôme P_k est de degré $\geqslant 2$ en Y ; on obtient au bout du compte une égalité

$$(*) \qquad P = QF + b_1(X)Y + b_0(X),$$

pour un certain $Q \in \mathbb{C}[X, Y]$. On peut montrer que Q et b_1, b_0 sont uniquement déterminés ; on dit que Q est le *quotient de la division euclidienne* de P par $F = Y^2 + S(X)$, et que

$$R := b_1(X)Y + b_0(X)$$

en est le *reste*. L'égalité $(*)$ signifie que P et R sont **congrus** modulo (F), c.-à-d., que $P - R$ appartient à l'idéal (F).

Puisque $(F) \subseteq I$ et que l'on a supposé $P \in I$, on obtient donc $R \in I$. Il reste donc à montrer que

$$b_1(X)Y + b_0(X) \in I$$

implique $b_1 = 0 = b_0$. Soit $x \in \mathbb{C}$. Comme $\mathbb{C}$ est algébriquement clos, l'équation

$$y^2 = S(x)$$

a au moins une solution y_0, et donc le point (x, y_0) appartient à $\mathscr{C}(F)$. Comme $R \in I$, on a donc

$$0 = R(x, y_0) = b_1(x)y_0 + b_0(x).$$

Multipliant cette égalité par $b_1(x)y_0 - b_0(x)$, on obtient

$$b_0(x)^2 = b_1(x)^2 y_0^2 = b_1(x)^2 S(x).$$

Comme $x \in \mathbb{C}$ était arbitraire, ceci montre que le polynôme

$$b_0(X)^2 - b_1(X)^2 S(X)$$

est identiquement nul. Supposons b_1 non nul, disons de degré n. Comme $S(X) = X^3 + X^2$, alors $b_1^2 S$ est non nul, de degré $2n + 3$; or ceci est impossible, car b_0^2 est nul ou bien de degré pair. Donc nécessairement $b_1 = 0 = b_0$, d'où $P = QF$. Ceci montre que, dans ce cas, on a $I = (F)$, et tout élément de $\mathbb{C}[\mathscr{C}(F)]$ est l'image d'un unique élément

$$b_1(X)Y + b_0(X).$$

En d'autres termes, si l'on note x et y les images de X et Y dans $\mathbb{C}[\mathscr{C}(F)]$, on obtient que tout élément de $\mathbb{C}[\mathscr{C}(F)]$ s'écrit de façon unique

$$b_1(x)y + b_0(x).$$

Exercice 1.2. — Déterminer l'idéal I pour $F = F_3$, puis pour $F = F_4$. Quelle différence de nature y-a-t-il entre les polynômes F_1 et F_3, et entre F_3 et F_4 ?

1.3. Espaces tangents. — Par définition, l'**espace tangent** à la courbe $\mathscr{C}(F) \subseteq \mathbb{C}^2$ en un point (x_0, y_0) est :

$$T_{(x_0,y_0)}\mathscr{C}(F) := \operatorname{Ker} d_{(x_0,y_0)}F,$$

où $d_{(x_0,y_0)}F$ désigne la différentielle au point (x_0, y_0) de l'application polynomiale (et donc C^∞) $F : \mathbb{C}^2 \to \mathbb{C}$.

Par exemple, si $F = F_1 = Y^2 - X^3$, alors

$$d_{(x_0,y_0)}F_1 = 2y_0 dy - 3x_0^2 dx$$

est non nulle sauf si $x_0 = y_0 = 0$. Donc, en tout point de $\mathscr{C}_1 := \mathscr{C}(F_1)$ autre que le point $0 := (0, 0)$, l'espace tangent est une droite, comme on s'y attend

pour une "courbe". Par contre, au point $0 = (0, 0)$ la différentielle de F_1 est nulle, et donc l'espace tangent est $\mathbb{C}^2$ tout entier ! On dit que 0 est un point *singulier* de la courbe $\mathscr{C}_1$.

1.4. Sous-variétés algébriques de $\mathbb{C}^n$. — Plus généralement, une *sous-variété algébrique* de $\mathbb{C}^n$ est un sous-ensemble de $\mathbb{C}^n$ défini par l'annulation d'un nombre fini de polynômes à n variables $\mathrm{F}_1, \ldots, \mathrm{F}_p \in \mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. On note

$$\mathscr{V}(\mathrm{F}_1, \ldots, \mathrm{F}_p) := \{x = (x_1, \ldots, x_n) \in \mathbb{C}^n \mid \mathrm{F}_1(x) = 0 = \cdots = \mathrm{F}_p(x)\}.$$

Par définition, l'**espace tangent** à $\mathscr{V} := \mathscr{V}(\mathrm{F}_1, \ldots, \mathrm{F}_p) \subseteq \mathbb{C}^n$ en un point $x^0 = (x_1^0, \ldots, x_n^0)$, est le sous-espace vectoriel intersection des noyaux des différentielles $d_{x^0}\mathrm{F}_1, \ldots, d_{x^0}\mathrm{F}_p$:

$$\mathrm{T}_{x^0}\mathscr{V} := \bigcap_{i=1}^{p} \operatorname{Ker} d_{x^0}\mathrm{F}_i,$$

où, à nouveau, $d_{x^0}\mathrm{F}_i$ désigne la différentielle au point x^0 de l'application polynomiale (et donc C^∞) $\mathrm{F}_i : \mathbb{C}^n \to \mathbb{C}$.

Attention : l'exemple de la courbe plane $\mathscr{C}_1$ montre qu'une variété algébrique n'est pas une "variété" au sens de la géométrie différentielle : en géométrie algébrique, il peut y avoir des points singuliers.

Une sous-variété algébrique de $\mathbb{C}^n$ définie par une seule équation $\mathrm{F} = 0$ s'appelle une *hypersurface* ; c'est une sous-variété de dimension $n - 1$. Par exemple, une courbe plane est une hypersurface de $\mathbb{C}^2$; par contre une courbe dans $\mathbb{C}^3$ n'est pas une hypersurface, et doit être définie par au moins deux équations. Par exemple, les coordonnées étant (x, y, z), l'axe des x a pour équations $y = 0 = z$, et la courbe

$$\mathscr{C} := \{(t, t^2, t^3) \in \mathbb{C}^3 \mid t \in \mathbb{C}\}$$

a pour équations $y = x^2, z = x^3$.

Remarquons que la sous-variété algébrique de $\mathbb{C}^3$ définie par les deux équations $zx = 0$ et $z^3 = zx^2$ est le plan $\{z = 0\}$, qui est une hypersurface. Ceci indique deux choses. D'une part, le système d'équations donné au départ n'est pas forcément un "bon" système d'équations ; en tout cas, il y en a (beaucoup) d'autres. En effet, revenant au cas général, soit I l'**idéal** de $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ **engendré par** $\mathrm{F}_1, \ldots, \mathrm{F}_p$, c.-à-d., I est l'ensemble des combinaisons linéaires

$$\mathrm{R}_1\mathrm{F}_1 + \cdots + \mathrm{R}_p\mathrm{F}_p, \qquad \mathrm{R}_i \in \mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n].$$

(**Exercice** de compréhension de la notion d'idéal : vérifier que I est un idéal !)

Alors, on voit que $\mathscr{V}(\mathrm{F}_1, \ldots, \mathrm{F}_p)$ égale la sous-variété

$$\mathscr{V}(\mathrm{I}) := \{x \in \mathbb{C}^n \mid \mathrm{P}(x) = 0, \quad \forall\, \mathrm{P} \in \mathrm{I}\},$$

et, de même, on a

$$\mathscr{V}(\mathrm{I}) = \mathscr{V}(\mathrm{G}_1, \ldots, \mathrm{G}_q)$$

pour **tout** système de générateurs de I. Ceci montre qu'il peut être intéressant de remplacer $\mathrm{F}_1, \ldots, \mathrm{F}_p$ par l'idéal engendré. Réciproquement, tout idéal J de $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est-il obtenu de cette manière, c.-à-d., est-ce que tout idéal J de $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est engendré par un nombre fini de polynômes ? La réponse est oui, c'est le théorème d'engendrement de Hilbert (Hilbert's basis theorem).

La deuxième chose, plus subtile, est la suivante. Partant d'un idéal I de $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, on forme la variété

$$\mathscr{V} := \mathscr{V}(\mathrm{I}) \subseteq \mathbb{C}^n.$$

On peut alors considérer l'idéal $\mathscr{I}(\mathscr{V})$ des polynômes nuls sur $\mathscr{V}$:

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

Il est clair que $\mathrm{I} \subseteq \mathscr{I}(\mathscr{V})$; mais l'on n'a pas nécessairement l'égalité. Par exemple, lorsque I est l'idéal de $\mathbb{C}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$ engendré par ZX et $\mathrm{Z}(\mathrm{Z}^2 - \mathrm{X}^2)$, $\mathscr{V}(\mathrm{I})$ est le plan $\mathrm{Z} = 0$, et $\mathscr{I}(\mathscr{V}(\mathrm{I}))$ est l'idéal (Z) ; or $\mathrm{Z} \notin \mathrm{I}$. Comment décrire, en général, $\mathscr{I}(\mathscr{V}(\mathrm{I}))$ en fonction de I ? La réponse est donnée par un autre célèbre théorème de Hilbert : le théorème des zéros de Hilbert, ou Nullstellensatz (en allemand).

1.5. Morphismes. — Revenons à la courbe plane

$$\mathscr{C}_1 = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3\},$$

qui est singulière au point $p_0 = (0, 0)$. Considérons l'application

$$\phi : \mathbb{C} \longrightarrow \mathscr{C}_1, \qquad t \mapsto (t^2, t^3).$$

C'est une application **polynomiale** $\mathbb{C} \to \mathbb{C}^2$ (en ce sens que ses deux coordonnées $t \mapsto t^2$ et $t \mapsto t^3$ sont polynomiales), dont l'image est exactement la courbe $\mathscr{C}_1$ (le vérifier !). Elle induit un morphisme d'anneaux ϕ^* de

$$\mathbb{C}[\mathscr{C}_1] = \mathbb{C}[\mathrm{X}, \mathrm{Y}]/\mathrm{I}, \qquad \text{où} \quad \mathrm{I} = (\mathrm{Y}^2 - \mathrm{X}^3)$$

vers $\mathbb{C}[\mathrm{X}]$, défini par : si $\mathrm{P} + \mathrm{I}$ est un élément de $\mathbb{C}[\mathscr{C}_1]$, où $\mathrm{P} \in \mathbb{C}[\mathrm{X}, \mathrm{Y}]$, alors

$$\phi^*(\mathrm{P}) = \mathrm{P} \circ \phi = \mathrm{P}(\mathrm{T}^2, \mathrm{T}^3) \in \mathbb{C}[\mathrm{T}].$$

Ceci est **bien défini** : si $Q \in \mathbb{C}[X, Y]$ est un autre représentant de la classe $P + I$, c.-à-d., si $Q - P \in I$, c.-à-d., si

$$Q - P = (Y^2 - X^3)R, \qquad \text{avec} \quad R \in \mathbb{C}[X, Y],$$

alors $Q(T^2, T^3) - P(T^2, T^3) = 0$.

Cet exemple, fondamental, illustre à la fois la notion de **passage au quotient d'un morphisme** d'anneaux, et le lien qui existe entre *applications polynomiales* d'une part, et morphismes d'anneaux, d'autre part.

1.6. Fonctions rationnelles. — L'anneau des polynômes $\mathbb{C}[X]$ se plonge dans son corps des fractions, le *corps des fractions rationnelles* :

$$\mathbb{C}(X) := \{\frac{P}{Q} \mid P, Q \in \mathbb{C}[X], \quad Q \neq 0\}.$$

Soit $x_0 \in \mathbb{C}$. On dit qu'une fraction rationnelle F est **définie** en x_0 si elle peut s'écrire

$$F = \frac{P}{Q} \qquad \text{avec} \quad Q(x_0) \neq 0.$$

Dans ce cas, par continuité, on a $Q(x) \neq 0$ pour x voisin de x_0, donc F est définie au voisinage de x_0.

Considérons maintenant la courbe plane $\mathscr{C}$ définie par l'équation $XY = 0$, c.-à-d., $\mathscr{C}$ est la réunion des droites $\{x = 0\}$ et $\{y = 0\}$. L'anneau des fonctions polynomiales sur $\mathscr{C}$ est

$$A := \mathbb{C}[\mathscr{C}] = \mathbb{C}[X, Y]/(XY).$$

Si on note x et y les images de X et Y dans A, alors

$$A = \mathbb{C}1 \bigoplus x\mathbb{C}[x] \bigoplus y\mathbb{C}[y]$$

comme espace vectoriel. Soit $x_0 \in \mathbb{C} \setminus \{0\}$. Au voisinage du point $p_0 := (x_0, 0)$, la courbe $\mathscr{C}$ ressemble (est isomorphe !) à l'axe des x. Plus précisément, considérons l'ouvert de $\mathscr{C}$ suivant :

$$U := \{(x, y) \in \mathscr{C} \mid x \neq 0\} = \{(x, 0) \in \mathbb{C}^2 \mid x \neq 0\}.$$

Il contient p_0, et la fraction rationnelle $1/x$ est définie en tout point de U. Si on adjoint à $\mathbb{C}[\mathscr{C}]$ cette fraction rationnelle $1/x$, inverse de x, la relation $xy = 0$ donne $y = 0$. Donc l'anneau obtenu, appelé le **localisé de** A (par rapport au complémentaire du lieu où $x = 0$), est

$$A[1/x] = \mathbb{C}[x, x^{-1}].$$

D'une part, c'est le même anneau que celui obtenu à partir de $\mathbb{C}[X]$ en inversant X : c'est en ce sens précis que $\mathscr{C}$ est isomorphe, sur le voisinage U de p_0, à l'axe

des x. D'autre part, on voit qu'en inversant x, on a "tué" y ; en particulier, le morphisme "de localisation"

$$\mathrm{A} \longrightarrow \mathrm{A}[1/x]$$

n'est **pas injectif** (son noyau est l'idéal engendré par y), à la différence de ce qui se passe pour $\mathbb{C}[\mathrm{X}] \hookrightarrow \mathbb{C}(\mathrm{X})$ (la flèche $\hookrightarrow$ désigne une application injective). C'est une des subtilités du procédé de localisation en général, qui nécessite une définition un peu plus compliquée que la construction du corps des fractions d'un anneau intègre (cf. la construction de $\mathbb{Q}$, resp. $\mathbb{C}(\mathrm{X})$, à partir de $\mathbb{Z}$, resp. $\mathbb{C}[\mathrm{X}]$).

1.7. Sujet du cours. — L'objet du cours est de fournir des concepts et outils pour étudier les anneaux commutatifs, en particulier les anneaux de la géométrie algébrique, comme les anneaux $\mathbb{C}[\mathscr{C}(\mathrm{F})] = \mathbb{C}[\mathrm{X},\mathrm{Y}]/\mathrm{I}$ ou, plus généralement, $\mathbb{C}[\mathrm{X}_1,\ldots,\mathrm{X}_n]/\mathrm{I}$. Une autre grande classe d'exemples est donnée par les anneaux de nombres, étudiés en théorie des nombres, comme par exemple $\mathbb{Z}[\sqrt{2}\,]$, $\mathbb{Z}[i]$ ou $\mathbb{Z}[(1+i\sqrt{3}\,)/2]$, voir la section suivante.

On étudiera les concepts esquissés dans cette section d'introduction, en particulier la notion d'idéal et sa généralisation, celle de **module**, les notions d'anneau ou module quotient, de factorisation d'un morphisme, de localisation, le théorème d'engendrement de Hilbert, la théorie des corps, le théorème des zéros, etc.

2. Anneaux de nombres

2.1. Notations et définitions. — On rappelle que $\mathbb{Z}$ désigne l'ensemble des nombres entiers, positifs ou négatifs, c.-à-d., $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$, et $\mathbb{Q}$ désigne l'ensemble des nombres rationnels, c.-à-d.,

$$\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}.$$

On note $\mathbb{N} = \{0, 1, 2, \ldots\}$ l'ensemble des entiers $\geqslant 0$. On suppose également connus l'ensemble $\mathbb{R}$ des nombres réels, et l'ensemble $\mathbb{C}$ des nombres complexes,

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\},$$

où $i^2 = -1$.

On note $\mathbb{Z}^*$, resp. $\mathbb{Q}^*$, l'ensemble des entiers, resp. rationnels, non nuls, et l'on note $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Pour tout $r \in \mathbb{Q}$, on note $|r|$ sa valeur absolue, c.-à-d.,

$$|r| = \sqrt{r^2} = \begin{cases} r & \text{si } r \geqslant 0; \\ -r & \text{si } r \leqslant 0. \end{cases}$$

On rappelle qu'un entier n est dit inversible s'il existe un entier n' tel que $nn' = 1$. Les seuls entiers inversibles sont ± 1.

Définition 2.1. — On dit qu'un entier p est **premier** s'il est non-inversible (c.-à-d., $\neq \pm 1$), et n'est divisible que par ± 1 et $\pm p$.

Ainsi, $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$ sont des nombres premiers.

Pour tout $n \geqslant 1$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des entiers modulo n, c.-à-d., des classes d'équivalence pour la relation $a \equiv b$ si $a - b \in n\mathbb{Z}$. On note $\dot{a}$ ou $a + n\mathbb{Z}$ la classe de a. On rappelle que l'on peut additionner, soustraire et multiplier les entiers modulo n, par les formules :

$$\dot{a} \pm \dot{b} = \dot{\overbrace{a \pm b}}, \qquad \dot{a}\dot{b} = \dot{\overbrace{ab}}.$$

Il faut bien entendu vérifier que ces opérations sont bien définies ; ceci est supposé connu. C'est un cas particulier de construction d'un anneau quotient, construction qu'on introduira plus loin.

2.2. Division euclidienne et conséquences. —

Proposition 2.2 **(Division euclidienne)**. — *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple d'entiers (q, r) tels que $a = bq + r$ et $0 \leqslant r < b$.*

On appelle q et r le quotient et le reste de la division euclidienne de a par b.

Démonstration. — Soit q le plus grand entier tel que $bq \leqslant a$ et soit $r = a - bq$. Alors $0 \leqslant r < b$ et $a = bq + r$. Ceci prouve l'existence. Si (q', r') est un second couple vérifiant les mêmes propriétés, alors $b(q' - q)$ égale $r - r'$ donc est de valeur absolue $< b$, et ceci entraîne $q' = q$ et $r' = r$. Ceci prouve l'unicité. □

Proposition 2.3. — *Tout sous-groupe $\neq \{0\}$ de $\mathbb{Z}$ est de la forme $b\mathbb{Z}$, pour un $b > 0$ uniquement déterminé.*

Démonstration. — Soit G un sous-groupe non-nul de $\mathbb{Z}$ et soit b le plus petit élément > 0 de G. Soit $a \in$ G arbitraire. Alors a est multiple de b. En effet, faisons la division euclidienne $a = bq + r$; alors le reste $r = a - bq$ appartient à G, et est $< b$, donc nécessairement nul. Ceci prouve que G $= b\mathbb{Z}$. De plus, b est uniquement déterminé par cette propriété. En effet, si G $= b'\mathbb{Z}$, alors il existe

$n, n' \in \mathbb{Z}$ tels que $b' = nb$ et $b = n'b'$, d'où $b = n'nb$ et $1 = nn'$ (car $b \neq 0$), d'où $n = \pm 1 = n'$ et donc $b' = \pm b$. Donc, si on impose $b' > 0$ alors $b' = b$. □

Définition 2.4. — Soient $n_1, \ldots, n_r \in \mathbb{Z}$. L'ensemble des entiers de la forme $a_1 n_1 + \cdots + a_r n_r$, avec $a_i \in \mathbb{Z}$, est un sous-groupe de $\mathbb{Z}$. C'est le plus petit sous-groupe contenant les n_i. On l'appelle le sous-groupe engendré par $n_1, \ldots, n_r$ et on le note $\mathbb{Z}n_1 + \cdots + \mathbb{Z}n_r$.

Définition et proposition 2.5 **(PGCD)**. —

Soient $n_1, \ldots, n_r \in \mathbb{Z}$, non tous nuls. Le sous-groupe G *qu'ils engendrent est de la forme $d\mathbb{Z}$, pour un unique $d > 0$. Alors d divise chaque n_i et, réciproquement, tout diviseur commun aux n_i divise d. On dit que d est le PGCD (plus grand commun diviseur) des n_i.*

Démonstration. — D'après la proposition 2.3, G est engendré par son plus petit élément $d > 0$, qui est de la forme

$$d = a_1 n_1 + \cdots + a_r n_r. \qquad (*)$$

Comme $n_i \in d\mathbb{Z}$, alors d divise n_i. Réciproquement, soit f un diviseur commun aux n_i. Alors $n_i = f q_i$ et l'on déduit de $(*)$ que $d = f(a_1 q_1 + \cdots + a_r q_r)$, donc f divise d. La proposition est démontrée. □

Théorème 2.6 **(Lemme d'Euclide)**. — *Soit p un nombre premier. Si p divise un produit ab, il divise a ou b.*

Démonstration. — Supposons a non divisible par p. Alors, comme p est premier, le PGCD de p et a est nécessairement 1, donc il existe $u, v \in \mathbb{Z}$ tels que $1 = up + va$. Multipliant cette égalité par b, on obtient

$$b = upb + vab,$$

d'où on déduit que p divise b si (et seulement si) p divise ab. Le théorème est démontré. □

Par récurrence sur s, on en déduit le corollaire suivant.

Corollaire 2.7. — *Si un nombre premier p divise un produit $a_1 \cdots a_s$, il divise l'un des a_i.*

Le Lemme d'Euclide (avec son corollaire) a des conséquences très importantes.

***Théorème 2.8* (Euclide).** — *Tout entier $n \neq 0$, non inversible, (c.-à-d., $n \neq 0, \pm 1$) s'écrit de façon unique*

$$n = \varepsilon(n) p_1 \cdots p_r,$$

où $\varepsilon(n)$ est le signe de n et où les p_i sont des nombres premiers > 0 uniquement déterminés.

Démonstration. — Il suffit de traiter le cas $n > 0$. Montrons par récurrence que tout entier $n \geqslant 2$ est produit de nombres premiers > 0. C'est bien le cas si n est premier. Sinon, l'ensemble des diviseurs d de n tels que $1 < d < n$ est non vide, donc admet un plus petit élément p, qui est nécessairement premier. Alors $n = pm$ et $1 < m < n$, donc par hypothèse de récurrence m est produit de nombres premiers > 0. Ceci prouve l'existence.

Pour montrer l'unicité, il est commode de prendre la convention qu'un produit de 0 termes (c.-à-d., un produit sur l'ensemble vide), est égal à 1. Supposons alors qu'on ait deux décompositions de l'entier $n \geqslant 1$ en produit de nombres premiers :

$$n = p_1 \cdots p_r = q_1 \cdots q_s. \qquad (*)$$

Montrons par récurrence sur $n \geqslant 1$ que $s = r$ et que, quitte à renuméroter les q_j, l'on a $q_i = p_i$ pour $i = 1, \ldots, r$.

Si $n = 1$, alors $r = 0$ et $s = 0$, car sinon p_1 ou q_1 serait inversible, une contradiction. On peut donc supposer $n > 1$ et l'unicité établie pour tout $m < n$. Comme n est non inversible (puisque $n > 1$), alors r et s sont $\geqslant 1$. D'après le (corollaire du) Lemme d'Euclide, p_1 divise l'un des q_i, donc, quitte à permuter les q_j, on peut supposer que p_1 divise q_1. Comme q_1 est premier, ceci entraîne $q_1 = p_1$. Alors, en simplifiant par p_1 l'égalité $(*)$, on obtient $p_2 \cdots p_r = q_2 \cdots q_s$. Par hypothèse de récurrence, appliquée à l'entier $m = n/p_1$, on conclut que $s = r$ et que l'on peut renuméroter les q_j de sorte que $q_i = p_i$ pour $i = 1, \ldots, r$. Le théorème est démontré. □

Soit $n > 0$, non inversible. D'après le théorème d'Euclide, n s'écrit de façon unique

$$n = p_1^{a_1} \cdots p_r^{a_r},$$

où les p_i sont des nombres premiers deux à deux distincts, et les a_i des entiers $\geqslant 1$. Il est commode de numéroter les p_i de sorte que $p_1 < \cdots < p_r$. On peut "lire" sur cette écriture certaines propriétés de n. Par exemple, on a le lemme suivant.

Lemme 2.9. — *n est un carré si et seulement si chaque a_i est pair.*

Démonstration. — Si $a_i = 2b_i$ pour tout i, alors n est le carré de $p_1^{b_1} \cdots p_r^{b_r}$. Réciproquement, si $n = m^2$, on peut supposer $m > 0$, et donc $m \geqslant 2$ (car $n \geqslant 2$). Alors $m = q_1^{b_1} \cdots q_s^{b_s}$, avec $q_1 < \cdots < q_s$, et donc

$$p_1^{a_1} \cdots p_r^{a_r} = n = m^2 = q_1^{2b_1} \cdots q_s^{2b_s}.$$

L'unicité de l'écriture entraîne $s = r$ et $p_i = q_i$, $a_i = 2b_i$ pour tout i. □

***Corollaire 2.10* (Euclide).** — $\sqrt{2} \notin \mathbb{Q}$.

Démonstration. — Supposons $\sqrt{2} = a/b$, avec $a, b \in \mathbb{N}^*$. Alors

$$2b^2 = a^2.$$

D'après le lemme précédent, le nombre premier 2 apparaît un nombre pair, resp. impair, de fois dans le terme de droite, resp. de gauche. Ceci contredit l'unicité de la décomposition du nombre $n = a^2 = 2b^2$ en produit de facteurs premiers. Cette contradiction montre que $\sqrt{2} \notin \mathbb{Q}$. □

Remarque 2.11. — La même démonstration montre que $\sqrt{n}$ est irrationnel si n est un entier $\geqslant 2$ qui n'est pas un carré (en particulier si n est premier).

***Définition et proposition 2.12* (PPCM (et PGCD))**. —

Soient $a_1, \ldots, a_n \in \mathbb{Z}^*$ et soient $p_1, \ldots, p_r$ l'ensemble des nombres premiers > 0 qui divisent l'un des a_i. On peut donc écrire :

$$\begin{cases} a_1 = \varepsilon(a_1) p_1^{c_{11}} \cdots p_r^{c_{1r}}, \\ \vdots \qquad\qquad \vdots \\ a_n = \varepsilon(a_n) p_1^{c_{n1}} \cdots p_r^{c_{nr}}, \end{cases}$$

où les c_{ij} sont des entiers $\geqslant 0$. Pour $j = 1, \ldots, r$, soient

$$\mathrm{M}_j = \max\{c_{1j}, \ldots, c_{nj}\}, \quad m_j = \min\{c_{1j}, \ldots, c_{nj}\}.$$

Posons $\mathrm{M} = p_1^{\mathrm{M}_1} \cdots p_r^{\mathrm{M}_r}$. Alors M est multiple de chaque a_i, et tout multiple commun à tous les a_i est un multiple de M. On dit que M est le PPCM (plus petit commun multiple) des a_i.

D'autre part, $d = p_1^{m_1} \cdots p_r^{m_r}$ est le PGCD des a_i.

Démonstration. — Tout ceci résulte de l'unicité de la décomposition en facteurs premiers. □

***Définition 2.13* (Valuations p-adiques)**. — On peut éviter, dans ce qui précède, d'avoir à "nommer" les nombres premiers qui divisent l'un des a_i, en introduisant, pour tout nombre premier p, l'application $v_p : \mathbb{Z}^* \to \mathbb{N}$ définie comme suit. Pour tout $n \in \mathbb{Z}^*$, $v_p(n)$ est l'exposant de p dans la décomposition de

n en facteurs premiers ; cet exposant étant nul si p n'apparaît pas dans la décomposition (c.-à-d., $p^0 = 1$). On peut alors écrire :

$$n = \varepsilon(n) \prod_p p^{v_p(n)},$$

le produit étant pris sur tous les nombres premiers > 0. C'est en fait un produit fini, puisqu'il n'y a qu'un nombre fini de facteurs $\neq 1$. Alors, si $a_1, \ldots, a_n \in \mathbb{Z}^*$, leur PPCM est

$$\mathrm{PPCM}(a_1, \ldots, a_n) = \prod_p p^{\max\{v_p(a_i)\}}.$$

L'application v_p s'appelle la valuation p-adique ; il est parfois commode de l'étendre en une application $\mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ en posant $v_p(0) = \infty$.

Définition 2.14. — On dit que des entiers $a_1, \ldots, a_n$ sont premiers entre eux s'ils n'ont pas de diviseur commun (autre que ± 1). Ceci équivaut à dire que leur PGCD est 1, et donc qu'il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que $u_1 a_1 + \cdots + u_n a_n = 1$.

Lemme 2.15. — *Soient $a, b \in \mathbb{Z}^*$.*

1) *a divise b si et seulement si $v_p(a) \leqslant v_p(b)$, pour tout p.*

2) *a et b sont premiers entre eux si et seulement si $v_p(b) = 0$ pour tout p tel que $v_p(a) > 0$.*

Démonstration. — Laissée au lecteur. □

Proposition 2.16 **(Lemme de Gauss)**. — *Soient $a, b, c \in \mathbb{Z}$, avec a, b premiers entre eux. Si a divise bc, il divise c.*

Démonstration. — Comme a, b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $1 = ua + vb$. On a donc $c = uac + vbc$. Par conséquent, si a divise bc, il divise c. □

Remarque 2.17. — On peut aussi démontrer le Lemme de Gauss en considérant les décompositions en facteurs premiers de a, b, c et en utilisant l'unicité. On peut aussi utiliser le lemme 2.15.

Corollaire 2.18. — *Tout nombre rationnel $r \neq 0$ s'écrit de façon unique*

$$r = \varepsilon(r) \frac{a}{b},$$

où $\varepsilon(r)$ est le signe de r et où $a, b \in \mathbb{N}^*$ sont premiers entre eux.

Démonstration. — Sans perte de généralité, on peut supposer $r > 0$. Alors r s'écrit c/d, pour des entiers $c, d \in \mathbb{N}^*$. En simplifiant les éventuels facteurs communs à c et d, on obtient une écriture $r = a/b$, où a et b sont premiers entre eux. Ceci prouve l'existence. Montrons l'unicité.

Supposons $a/b = a'/b'$, avec $a', b' > 0$. Alors $ab' = a'b$ et donc, d'après le Lemme de Gauss, a divise a' et b divise b'. On en déduit qu'il existe $c > 0$ tel que $a' = ac$ et $b' = bc$. Donc, si l'on suppose de plus a' et b' premiers entre eux, on obtient $c = 1$, d'où $a' = a$ et $b' = b$. Ceci prouve l'unicité voulue. □

Une conséquence immédiate du Lemme d'Euclide est que, dans $\mathbb{Z}/p\mathbb{Z}$, le produit de deux éléments non nuls est non nul. En fait, la démonstration montre qu'on a le résultat plus fort suivant.

Proposition 2.19. — *Soit p un nombre premier. Dans $\mathbb{Z}/p\mathbb{Z}$, tout élément non nul est inversible.*

Démonstration. — Soit $a \in \mathbb{Z}$ non divisible par p. Alors, le PGCD de p et a est 1, donc il existe $u, v \in \mathbb{Z}$ tels que

$$1 = up + va.$$

Par conséquent, dans $\mathbb{Z}/p\mathbb{Z}$ on a $\dot{a}\dot{v} = \dot{1}$. □

2.3. Solutions entières de $x^2 + y^2 = z^2$. — Une autre conséquence du théorème d'Euclide 2.8 est la détermination de toutes les solutions entières de l'équation de Pythagore $x^2 + y^2 = z^2$.

Si un triplet d'entiers (a, b, c) est solution de $a^2 + b^2 = c^2$, alors les triplets $(\pm a, \pm b, \pm c)$ sont également solutions. D'autre part, on s'intéresse aux solutions non triviales, c.-à-d., telles que $ab \neq 0$. On peut donc se limiter à chercher les solutions où a, b, c sont > 0.

On dit qu'une solution (a, b, c) est primitive si a, b, c sont premiers entre eux. Si (a, b, c) est une solution arbitraire dont le pgcd est d, on peut écrire $(a, b, c) = (da', db', dc')$ et alors (a', b', c') est une solution primitive. Donc toute solution est multiple d'une solution primitive, et il suffit de déterminer ces dernières.

Proposition 2.20 **(Euclide)**. — *Les solutions entières de $a^2 + b^2 = c^2$, avec $a, b, c > 0$, sont de la forme suivante (à permutation près de a et b) :*

$$a = 2uvw, \quad b = (u^2 - v^2)w, \quad c = (u^2 + v^2)w,$$

où $u, v, w \in \mathbb{N}^*$.

Démonstration. — On peut supposer a, b, c premiers entre eux. Alors a, b ne sont pas tous deux pairs. Comme le carré d'un nombre impair (resp. pair) est congru à 1 (resp. 0) modulo 4, ils ne sont pas non plus tous deux impairs, car sinon $a^2 + b^2$ serait congru à 2 modulo 4 et ne pourrait être un carré. Donc, quitte à échanger a et b, on peut supposer a pair et b, c impairs. Posons $a = 2\alpha$. Alors

$$\alpha^2 = \frac{c+b}{2}\frac{c-b}{2}.$$

Or, les entiers $(c+b)/2$ et $(c-b)/2$ sont premiers entre eux (car un diviseur premier commun diviserait b et c, d'où aussi a^2 et donc a). On en déduit que chacun est un carré, d'où $c + b = 2u^2$ et $c - b = 2v^2$, avec $u, v \in \mathbb{N}^*$. Donc

$$b = u^2 - v^2, \quad c = u^2 + v^2, \quad a^2 = c^2 - b^2 = 4u^2v^2,$$

et $a = 2uv$ puisque $a > 0$. □

2.4. Somme de deux carrés et entiers de Gauss. — Quels sont les entiers qui s'écrivent comme somme de deux carrés d'entiers ? Cette question remonte au moins à Diophante d'Alexandrie, qui vécut dans une période comprise entre l'an 150 et l'an 350. Il écrivit :

"65 s'écrit de deux façons différentes comme somme de deux carrés : $65 = 7^2 + 4^2 = 8^2 + 1^2$. Ceci est dû au fait que 65 est le produit de 13 et 5, dont chacun est somme de deux carrés."

Ceci semble indiquer que Diophante connaissait l'égalité :

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2, \qquad (\dagger)$$

que l'on peut vérifier par un calcul direct. On verra plus bas un moyen de l'obtenir. Cette égalité montre que, pour qu'un entier $n > 0$ soit somme de deux carrés, il suffit que chacun de ses facteurs premiers le soit. (On verra plus loin une condition nécessaire et suffisante). On a bien sûr $2 = 1^2 + 1^2$. D'autre part, comme un carré est congru à 0 ou 1 modulo 4, un nombre premier impair de la forme $4n+3$ ne peut être somme de deux carrés. Fermat a affirmé en 1640 que tout nombre premier de la forme $4n + 1$ s'écrivait de façon unique comme somme de deux carrés, mais n'a pas publié sa démonstration. La première preuve connue remonte à Euler, en 1756. Lagrange donna vers 1770 une autre preuve, simplifiée vers 1801 par Gauss. Gauss introduisit et étudia les nombres de la forme $a + ib$, où $a, b \in \mathbb{Z}$ et $i^2 = -1$, qu'on appelle entiers de Gauss.

Pour tout entier de Gauss $z = a + ib$, on définit son conjugué $\overline{z} = a - ib$, et sa norme

$$\mathrm{N}(z) := z\overline{z} = a^2 + b^2.$$

Soit $v = c + id$ un autre entier de Gauss. On a

$$zv = (a + ib)(c + id) = (ac - bd) + i(bc + ad). \tag{1}$$

On en déduit, premièrement, que $\overline{zv} = \overline{z}\,\overline{v}$. Ceci entraîne que la norme est multiplicative, c.-à-d.,

$$\mathrm{N}(zv) = zv\overline{zv} = \mathrm{N}(z)\mathrm{N}(v) = (a^2 + b^2)(c^2 + d^2). \tag{2}$$

D'autre part, (1) entraîne $\mathrm{N}(zv) = (ac - bd)^2 + (bc + ad)^2$. Comparant avec (2), on obtient l'égalité

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (bc + ad)^2. \tag{†}$$

Si $z = a + ib$ est inversible, alors $\mathrm{N}(z) = 1$. On en déduit que les entiers de Gauss inversibles sont ± 1 et $\pm i$.

Définition 2.21. — On dit qu'un entier de Gauss z est **irréductible** s'il est non inversible et si les seuls entiers de Gauss non inversibles qui le divisent sont $\pm z$ et $\pm iz$.

Proposition 2.22. — *Tout élément non nul et non inversible de $\mathbb{Z}[i]$ est produit d'éléments irréductibles.*

Démonstration. — Montrons par récurrence sur $\mathrm{N}(z)$ que tout élément non nul $z \in \mathbb{Z}[i]$ est inversible ou bien produit d'irréductibles. Si $\mathrm{N}(z) = 1$, alors z égale ± 1 ou $\pm i$ et est inversible. Supposons $\mathrm{N}(z) \geqslant 2$ et soit ξ un diviseur de z de norme minimale. Alors ξ est nécessairement irréductible, car si $\xi = uv$ alors l'égalité $\mathrm{N}(\xi) = \mathrm{N}(u)\mathrm{N}(v)$ entraîne, disons, que $\mathrm{N}(u) = \mathrm{N}(\xi)$ et v est inversible. Posant $z = \xi\xi'$, on a $\mathrm{N}(\xi') < \mathrm{N}(z)$ et donc ξ' est inversible ou bien produit d'irréductibles. Ceci prouve la proposition. □

Gauss a démontré que les éléments irréductibles de $\mathbb{Z}[i]$ vérifient le Lemme d'Euclide, de sorte que la théorie de la divisibilité dans $\mathbb{Z}[i]$ est analogue à celle dans $\mathbb{Z}$. Plus précisément, Gauss a établi l'existence d'une division euclidienne dans $\mathbb{Z}[i]$.

Proposition 2.23 **(Division euclidienne dans $\mathbb{Z}[i]$)**. —
Soient $z, u \in \mathbb{Z}[i]$, avec $u \neq 0$. Il existe $\eta, \xi \in \mathbb{Z}[i]$ tels que $z = \eta u + \xi$, et $\sqrt{\mathrm{N}(\xi)} < \sqrt{\mathrm{N}(u)}$.

Démonstration. — On considère les éléments de $\mathbb{Z}[i]$ dans le plan complexe $\mathbb{C} \cong \mathbb{R}^2$. Alors, pour $\alpha, \beta \in \mathbb{Z}[i]$, $\sqrt{\mathrm{N}(\beta - \alpha)}$ est la distance euclidienne usuelle entre α et β.

Les multiples ηu, avec $\eta \in \mathbb{Z}[i]$, forment les sommets d'un quadrillage du plan, formé de carrés de côté de longueur $\sqrt{\mathrm{N}(u)}$. Un carré arbitraire a pour quatre sommets les points :

$$\eta u, \quad (\eta+1)u, \quad (\eta+i)u, \quad (\eta+1+i)u.$$

Notre élément $z \in \mathbb{Z}[i]$ appartient à (au moins) un tel carré, et la distance de z au sommet le plus proche est $\leqslant \sqrt{\mathrm{N}(u)/2}$ (longueur d'une demi-diagonale). Par conséquent, il existe un multiple ηu tel que $\xi := z - \eta u$ vérifie $\sqrt{\mathrm{N}(\xi)} < \sqrt{\mathrm{N}(u)}$. La proposition est démontrée. □

Soient $z, z' \in \mathbb{Z}[i]$. Notons

$$\mathbb{Z}[i]z + \mathbb{Z}[i]z' := \{\eta z + \eta' z' \mid \eta, \eta' \in \mathbb{Z}[i]\};$$

cet ensemble est stable par addition, soustraction, et multiplication par un élément arbitraire de $\mathbb{Z}[i]$: c'est un **idéal** de $\mathbb{Z}[i]$, selon la terminologie introduite vers 1870 par Dedekind. Soit d un élément de $\mathbb{Z}[i]z + \mathbb{Z}[i]z'$ de norme minimale. En utilisant la division euclidienne, on montre, comme dans le cas des entiers rationnels, que tout élément de $\mathbb{Z}[i]z + \mathbb{Z}[i]z'$ est multiple de d. (En particulier, d est uniquement déterminé, à multiplication par un inversible près).

Corollaire 2.24. — *Soient $\xi, z \in \mathbb{Z}[i]$. On suppose ξ irréductible et z non divisible par ξ. Alors il existe $u, v \in \mathbb{Z}[i]$ tels que $u\xi + vz = 1$.*

Démonstration. — D'après ce qui précède, il existe $d \in \mathbb{Z}[i]$ tel que

$$d\mathbb{Z}[i] = \xi\mathbb{Z}[i] + z\mathbb{Z}[i].$$

Donc d divise ξ et z. Comme ξ est irréductible, d est inversible, ou bien produit de ξ par un inversible. Comme, par hypothèse, ξ ne divise pas z, le second cas est exclu. Donc d est inversible, d'où $d\mathbb{Z}[i] = \mathbb{Z}[i]$. Le corollaire en découle. □

***Théorème 2.25* (Gauss)**. — *Le Lemme d'Euclide est valable dans $\mathbb{Z}[i]$, c.-à-d., si un élément irréductible ξ divise un produit zz', il divise z ou z'.*

Démonstration. — Tenant compte du corollaire précédent, la démonstration est identique à celle du Lemme d'Euclide dans $\mathbb{Z}$. □

Nous admettrons pour le moment la proposition suivante. Nous la signalons avec une $(*)$ pour indiquer qu'elle fait partie des résultats énoncés, mais non démontrés dans ce chapitre.

Proposition 2.26. — $(*)$ *Soit $p \in \mathbb{Z}$ un nombre premier > 2. Alors, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \mod 4$.*

En admettant cette proposition, voyons comment Dedekind a démontré, vers 1870, le théorème des deux carrés.

Théorème 2.27. — *Soit $p \in \mathbb{Z}$ un nombre premier > 2. Alors $p = a^2 + b^2$, avec $a, b \in \mathbb{Z}^*$, si et seulement si $p \equiv 1 \mod 4$.*

Démonstration. — On a déjà vu que, pour une raison de congruence modulo 4, un entier congru à 3 modulo 4 ne pouvait être somme de deux carrés. On peut donc supposer $p \equiv 1 \mod 4$. Alors, d'après la proposition, il existe un entier $m \in \{1, \ldots, p-1\}$ tel que p divise $m^2 + 1$. Or, dans $\mathbb{Z}[i]$ on a l'égalité

$$m^2 + 1 = \mathrm{N}(m + i) = (m + i)(m - i),$$

et p ne divise aucun des facteurs de droite, car

$$\frac{m \pm i}{p} = \frac{m}{p} \pm i\frac{1}{p}$$

n'appartient pas à $\mathbb{Z}[i]$. Comme le Lemme d'Euclide est valable dans $\mathbb{Z}[i]$, on en déduit que p n'est pas irréductible. Donc, il existe $\xi, \eta \in \mathbb{Z}[i]$ non inversibles tels que $p = \xi\eta$, d'où

$$p^2 = \mathrm{N}(p) = \mathrm{N}(\xi)\mathrm{N}(\eta).$$

Comme $\mathrm{N}(\xi)$ et $\mathrm{N}(\eta)$ sont > 1, on en déduit que $\mathrm{N}(\xi) = p = \mathrm{N}(\eta)$. Écrivant $\xi = a + ib$, on obtient ainsi

$$p = a^2 + b^2 = \xi\overline{\xi}.$$

De plus cette écriture est unique. En effet, l'égalité $\mathrm{N}(\xi) = p$ entraîne que ξ est irréductible. Si $p = c^2 + d^2 = z\overline{z}$, où $z = c + id$, alors z est aussi irréductible et, quitte à changer z en $\overline{z}$, on déduit du Lemme d'Euclide que $z = \xi u$, où u est un élément inversible, c.-à-d., ± 1 ou $\pm i$. Il en résulte que $\{a^2, b^2\} = \{c^2, d^2\}$. □

Corollaire 2.28. — *Pour qu'un entier $n \geqslant 2$ soit somme de deux carrés, il faut et il suffit que $v_p(n)$ soit pair, pour tout nombre premier $p > 0$ de la forme $4k + 3$.*

Démonstration. — La suffisance résulte du théorème précédent, combiné avec le fait que $2 = 1^2 + 1^2$, l'égalité (†), et le fait que si $m = a^2 + b^2$ alors $mr^2 = (ar)^2 + (br)^2$.

Pour montrer la nécessité, supposons que n soit un contre-exemple minimal, c.-à-d., que $n = x^2 + y^2$ vérifie $v_p(n) = 2k + 1$ pour un nombre premier $p > 0$

congru à 3 modulo 4, et que n soit minimal pour cette propriété. Si p ne divise ni x ni y, alors dans $\mathbb{Z}/p\mathbb{Z}$ on a

$$0 = \dot{x}^2 + \dot{y}^2 = 1 + \left(\frac{\dot{y}}{\dot{x}}\right)^2,$$

donc -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, ce qui contredit la proposition 2.26. Par conséquent, on peut supposer que p divise x. Alors p divise y^2 et donc y (d'après le Lemme d'Euclide), et donc p^2 divise n. Mais alors $v_p(n) = 2k+1 \geqslant 3$ et n/p^2 est encore un contre-exemple, puisque $n/p^2 = (x/p)^2 + (y/p)^2$ et $v_p(n/p^2) = 2k-1 \geqslant 1$. Ceci contredit la minimalité de n. Le corollaire est démontré. □

Remarque 2.29. — Une démonstration plus conceptuelle du corollaire, basée sur la détermination des éléments irréductibles de $\mathbb{Z}[i]$ et de leur norme, se trouve dans [**Elk**], Ch.X, Ex.2.

2.5. Les anneaux de nombres $\mathbb{Z}[\sqrt{n}\,]$. —

Définition 2.30. — On dira qu'un sous-ensemble A de $\mathbb{C}$ est un *anneau de nombres*, s'il contient 1 et est stable par addition, soustraction et multiplication.

Définition 2.31. — Soit A un anneau de nombres. On dit qu'un élément $p \in \mathrm{A}$ est **irréductible** s'il est non inversible et si les seuls éléments de A qui divisent p sont inversibles ou de la forme pu, avec u inversible.

Ceci équivaut à dire que p est non inversible et vérifie la propriété suivante : si $p = ab$, avec $a, b \in \mathrm{A}$, alors a ou b est inversible.

Ainsi, par exemple, l'ensemble $\mathbb{Z}[i]$ des entiers de Gauss est un anneau de nombres. De façon plus générale, soit $n \in \mathbb{Z}$, distinct de 1 et sans facteur carré (c.-à-d., $n = -1$ ou bien $\pm n$ est un produit de nombres premiers > 0 deux à deux distincts). On peut considérer l'anneau de nombres

$$\mathbb{Z}[\sqrt{n}] = \{a + \sqrt{n}\,b \mid a, b \in \mathbb{Z}\},$$

où $\sqrt{n}$ désigne l'une quelconque des racines carrées de n dans $\mathbb{C}$. Cet ensemble contient 1 et est clairement stable par addition et soustraction. Il est aussi stable par multiplication, puisque

$$(*) \qquad (a + \sqrt{n}\,b)(a' + \sqrt{n}\,b') = (aa' + nbb') + \sqrt{n}\,(ab' + ba').$$

C'est donc bien un anneau de nombres. Pour $u = a + \sqrt{n}\, b$, on définit, comme pour les entiers de Gauss,

$$\overline{u} = a - \sqrt{n}\, b, \qquad \mathrm{N}(u) = u\overline{u} = a^2 - nb^2.$$

On déduit de $(*)$ que $\overline{uv} = \overline{u}\,\overline{v}$ et $\mathrm{N}(uv) = \mathrm{N}(u)\mathrm{N}(v)$. Il en résulte que u est inversible si et seulement si $\mathrm{N}(u) = \pm 1$. En utilisant la (valeur absolue de la) norme, on établit, exactement comme pour $\mathbb{Z}[i]$, la proposition suivante.

Proposition 2.32. — *Tout élément non nul et non inversible de $\mathbb{Z}[\sqrt{n}\,]$ est produit d'éléments irréductibles.*

Par contre, le Lemme d'Euclide, et l'unicité des facteurs irréductibles, peuvent être en défaut. C'est le cas, par exemple, pour $n = -3, -5$, ou 5. Avant de détailler ces exemples, il est utile d'introduire la définition suivante.

Définition 2.33. — Soit A un anneau de nombres. On dit que A est **factoriel** si les deux conditions ci-dessous sont satisfaites :

1) Tout élément de A, distinct de 0 et non inversible, est un produit fini d'éléments irréductibles.

2) Tout élément irréductible p vérifie le Lemme d'Euclide, c.-à-d., si p divise un produit ab, il divise a ou b.

Exemples 2.34. — 1) Dans $\mathbb{Z}[\sqrt{-3}\,]$, on a $\mathrm{N}(a + \sqrt{-3}\, b) = a^2 + 3b^2$ donc les inversibles sont ± 1 et il n'y a pas d'élément de norme 2. D'autre part, on a l'égalité suivante :

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Tous les facteurs sont de norme 4, donc irréductibles (car il n'y a pas d'élément de norme 2). Si $1 + \sqrt{-3}$ vérifiait le Lemme d'Euclide, il diviserait 2, et comme ce dernier est irréductible, on aurait $2 = u(1 + \sqrt{-3}\,)$, avec u inversible, donc $u = \pm 1$, une contradiction. Ceci montre que $\mathbb{Z}[\sqrt{-3}\,]$ n'est pas factoriel.

2) De même, dans $\mathbb{Z}[\sqrt{-5}\,]$, $\mathrm{N}(a + \sqrt{-5}\, b) = a^2 + 5b^2$ donc les inversibles sont ± 1 et il n'y a pas d'élément de norme 2 ou 3. D'autre part, on a l'égalité

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Les facteurs sont de norme, respectivement, $4, 9, 6, 6$, donc sont irréductibles. Le même argument que précédemment montre que si $1 + \sqrt{-5}$ vérifiait le Lemme d'Euclide, il serait égal à ± 2 ou ± 3, ce qui n'est pas le cas. Ceci montre que $\mathbb{Z}[\sqrt{-5}\,]$ n'est pas factoriel.

3) Dans $\mathbb{Z}[\sqrt{5}\,]$, on a $\mathrm{N}(a+\sqrt{-5}\,b) = a^2-5b^2$. Il n'y a pas d'élément de norme ± 2. En effet, une égalité $a^2 = \pm 2 + 5b^2$ est impossible, puisque le carré d'un nombre pair (resp. impair) est congru à 0 (resp. 1) modulo 4.

D'autre part, on a l'égalité

$$(1+\sqrt{5}\,)(-1+\sqrt{5}\,) = 2\cdot 2.$$

Les facteurs le gauche sont de norme -4, ceux de droite de norme 4, donc chaque facteur est irréductible, puisqu'il n'y a pas d'élément de norme ± 2. L'élément irréductible 2 ne vérifie pas le Lemme d'Euclide, car sinon on aurait, disons, $1+\sqrt{5} = 2u$, et

$$u = \frac{1}{2} + \frac{1}{2}\sqrt{5}$$

appartiendrait à $\mathbb{Z}[\sqrt{5}\,]$, ce qui n'est pas le cas, puisque 1 et $\sqrt{5}$ sont linéairement indépendants sur $\mathbb{Q}$. Ceci montre que $\mathbb{Z}[\sqrt{5}\,]$ n'est pas factoriel.

4) Il faut se garder de croire que l'argument précédent s'applique à $\mathbb{Z}[\sqrt{7}\,]$. Dans cet anneau, on a bien l'égalité

$$2\cdot 3 = 6 = (1+\sqrt{7}\,)(-1+\sqrt{7}\,),$$

mais aucun des facteurs ci-dessus n'est irréductible. En effet, on a

$$\begin{array}{ll} 2 = (3+\sqrt{7}\,)(3-\sqrt{7}\,), & 1+\sqrt{7} = (3+\sqrt{7}\,)(-2+\sqrt{7}\,), \\ 3 = (2+\sqrt{7}\,)(-2+\sqrt{7}\,), & -1+\sqrt{7} = (3-\sqrt{7}\,)(2+\sqrt{7}\,). \end{array}$$

En fait, on peut montrer que $\mathbb{Z}[\sqrt{7}\,]$ est un anneau factoriel, mais la démonstration nécessite des techniques plus sophistiquées, voir par exemple [**Sa**, Ex.V.7].

2.6. Les anneaux $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. — Soit $j = (-1+i\sqrt{3})/2 = \exp(2i\pi/3)$; c'est une racine cubique de 1, et une racine du polynôme $\mathrm{X}^2+\mathrm{X}+1$. D'autre part, posons $\theta = (1+\sqrt{5}\,)/2$. C'est une racine du polynôme $\mathrm{X}^2-\mathrm{X}-1$.

Le défaut d'unicité de la factorisation dans $\mathbb{Z}[\sqrt{-3}\,]$ (resp., dans $\mathbb{Z}[\sqrt{5}\,]$) peut être pallié en élargissant cet anneau en l'anneau de nombres

$$\mathbb{Z}[j] = \{a+jb \mid a,b\in\mathbb{Z}\},$$

resp.

$$\mathbb{Z}[\theta] = \{a+\theta b \mid a,b\in\mathbb{Z}\}.$$

Chacun de ces ensembles contient 1, et est stable par addition et soustraction, et aussi par multiplication car $j^2 = -j-1$ (resp. $\theta^2 = \theta+1$). Ce sont donc des anneaux de nombres. Le premier contient $\mathbb{Z}[\sqrt{-3}\,]$ car $i\sqrt{-3} = 2j+1$, et le second contient $\sqrt{5} = 2\theta - 1$.

On peut montrer que $\mathbb{Z}[j]$ et $\mathbb{Z}[\theta]$ sont tous deux factoriels. Pour $\mathbb{Z}[\theta]$, on renvoie le lecteur intéressé à [**Sa**, Ex. V.7.a)]. Pour $\mathbb{Z}[j]$, un argument géométrique élémentaire montre l'existence d'une division euclidienne. Plus précisément, désignant par $\rho(z) = \sqrt{z\overline{z}}$ la norme d'un nombre complexe z, on a la proposition suivante.

***Proposition 2.35* (Division euclidienne dans $\mathbb{Z}[j]$).** —
Soient $z, u \in \mathbb{Z}[j]$ avec $u \neq 0$. Il existe $\eta, \xi \in \mathbb{Z}[j]$ tels que $z = \eta u + \xi$, et $\rho(\xi) < \rho(u)$.

Démonstration. — Les multiples $(a + jb)u$ de u forment les sommets d'une triangulation du plan formée de triangles équilatéraux de côté $\rho(u)$. Chaque point d'un triangle est à une distance $\leqslant \rho(u)/\sqrt{3} < \rho(u)$ du sommet le plus proche. □

Comme pour les entiers de Gauss, on en déduit, exactement comme dans la preuve du corollaire 2.24 et du théorème 2.25, le corollaire suivant.

Corollaire 2.36. — *$\mathbb{Z}[j]$ est factoriel.*

Donc, en quelque sorte, on peut dire que le défaut de factorialité observé dans $\mathbb{Z}[\sqrt{n}\,]$, pour $n = -3$ et $n = 5$, provient du fait que l'on n'a pas considéré le "bon anneau", qui se trouve être, dans ce cas, l'anneau

$$\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{n}}{2}.$$

Par contre, on peut montrer que $\mathbb{Z}[\sqrt{-5}\,]$ ne peut pas être élargi en un sous-anneau A de $\mathbb{Q}[\sqrt{-5}\,] = \{a + \sqrt{-5}\,b \mid a, b \in \mathbb{Q}\}$, qui soit engendré comme $\mathbb{Z}$-module par un nombre fini d'éléments. C.-à-d., on peut démontrer la

Proposition 2.37. — (∗) *Soit* A *un sous-anneau de $\mathbb{Q}[\sqrt{-5}\,]$, contenant $\sqrt{-5}$. On suppose qu'il existe $a_1, \ldots, a_r \in$ A tels que tout élément de* A *s'écrive $n_1a_1 + \cdots + n_ra_r$, avec $n_i \in \mathbb{Z}$. Alors* $\mathrm{A} = \mathbb{Z}[\sqrt{-5}\,]$.

Ceci suggère les questions suivantes : que sont les anneaux $\mathbb{Z}[(1 + \sqrt{n}\,)/2]$, pour $n = -3$ et $n = 5$? Pourquoi apparaissent-ils, et pourquoi le cas de $\mathbb{Z}[\sqrt{-5}\,]$ est-il différent ? La réponse à ces questions se trouve dans la notion de nombre algébrique **entier**, introduite par Dedekind en 1871 (voir [**De**]).

2.7. Entiers algébriques. —

Définition 2.38. — Soit $z \in \mathbb{C}$.

1) On dit que z est un **nombre algébrique** s'il existe un polynôme unitaire $\mathrm{P} = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_1\mathrm{X} + a_0$ dans $\mathbb{Q}[\mathrm{X}]$ tel que $\mathrm{P}(z) = 0$, c.-à-d., si z est racine d'une équation

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0,$$

avec les a_i dans $\mathbb{Q}$.

2) On dit de plus que z est un **nombre algébrique entier**, ou simplement un **entier algébrique**, s'il existe un polynôme unitaire $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ tel que $\mathrm{P}(z) = 0$, c.-à-d., si z est racine d'une équation

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0,$$

avec les a_i dans $\mathbb{Z}$.

Exemples 2.39. — 1) Tout entier rationnel $n \in \mathbb{Z}$ est un entier algébrique : il est racine du polynôme $\mathrm{X} - n$.

2) Le rationnel $\frac{1}{2}$ n'est pas un entier algébrique. Plus généralement, si r est un élément de $\mathbb{Q}$ n'appartenant pas à $\mathbb{Z}$, alors r n'est pas un entier algébrique.

Exercice : démontrer cette assertion. *Indication* : écrire $r = a/b$, avec a et b premiers entre eux, et supposer qu'il existe P unitaire dans $\mathbb{Z}[\mathrm{X}]$ tel que $\mathrm{P}(a/b) = 0$; en déduire une contradiction.

3) Pour tout $n \in \mathbb{Z}^*$, les deux racines $\pm\sqrt{n}$ du polynôme $\mathrm{X}^2 - n$ sont des entiers algébriques. Si $n = 4k + 1$, il en est de même de $(1 + \sqrt{n}\,)/2$, qui est racine du polynôme $\mathrm{X}^2 - \mathrm{X} - k$.

Théorème 2.40 **(Dedekind (1871))**. — *L'ensemble $\mathscr{A}$ de tous les entiers algébriques est un anneau.*

Démonstration. — $\mathscr{A}$ contient 1. Soient $\alpha, \beta \in \mathscr{A}$. Par hypothèse, il existe des entiers $a_1, \ldots, a_r$ et $b_1, \ldots, b_s$ tels que

$$(*) \qquad \begin{cases} \alpha^r = a_1\alpha^{r-1} + \cdots + a_r; \\ \beta^s = b_1\beta^{s-1} + \cdots + b_s. \end{cases}$$

Posons $n = rs$ et désignons par $\omega_1, \omega_2, \ldots, \omega_n$ l'ensemble des monômes

$$\alpha^i\beta^j, \qquad 0 \leqslant i \leqslant r-1,\ 0 \leqslant j \leqslant s-1,$$

en choisissant la numérotation de sorte que ω_1 soit le monôme $\alpha^0\beta^0 = 1$.

Soit η l'un des trois nombres $\alpha+\beta$, $\alpha-\beta$, ou $\alpha\beta$. On déduit des égalités $(*)$ que chacun des n produits $\eta\omega_i$ peut s'exprimer comme une combinaison linéaire

$$(\mathrm{E}_i) \qquad \eta\omega_i = k_{i1}\omega_1 + \cdots + k_{in}\omega_n,$$

à coefficients $k_{ij} \in \mathbb{Z}$. Soustrayant $\eta\omega_i$ aux deux membres de l'égalité (E_i), on obtient que le système linéaire suivant, à coefficients dans $\mathbb{C}$,

$$\begin{cases} (k_{11}-\eta)x_1 + & k_{12}x_2 + \cdots + & k_{1n}x_n = 0 \\ k_{21}x_1 + (k_{22}-\eta)x_2 + \cdots + & & k_{2n}x_n = 0 \\ \cdots & \cdots \quad \cdots & \cdots \quad \cdots \\ k_{n1}x_1 + & k_{n2}x_2 + \cdots + & (k_{nn}-\eta)x_n = 0 \end{cases}$$

admet la solution non nulle $x_i = \omega_i$, pour $i = 1, \ldots, n$. On en déduit que le déterminant de ce système, c.-à-d., le déterminant suivant, est nul :

$$\begin{vmatrix} k_{11}-\eta & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22}-\eta & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn}-\eta \end{vmatrix} = 0.$$

En développant ce déterminant, on obtient une équation

$$\eta^n + e_1\eta^{n-1} + \cdots + e_{n-1}\eta + e_n = 0,$$

avec les e_i dans $\mathbb{Z}$. Donc η est un entier algébrique, pour $\eta = \alpha+\beta$, $\alpha-\beta$, ou $\alpha\beta$. Ceci montre que l'ensemble $\mathscr{A}$ des entiers algébriques est un anneau. Le théorème est démontré. □

Corollaire 2.41. — *L'ensemble $\mathscr{K} = \overline{\mathbb{Q}}$ des nombres algébriques est un* **corps** (c.-à-d., un anneau dans lequel tout élément non nul admet un inverse).

Démonstration. — D'abord, la même démonstration que précédemment, où cette fois les k_{ij} et les e_i sont dans $\mathbb{Q}$, montre que $\mathscr{K}$ est un anneau. Il reste à montrer que tout élément $\alpha \neq 0$ de $\mathscr{K}$ est inversible.

Soit $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ un polynôme unitaire tel que $\mathrm{P}(\alpha) = 0$, et de degré minimal pour cette propriété. Écrivons

$$\mathrm{P} = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_1\mathrm{X} + a_0,$$

et désignons par Q le polynôme unitaire $(\mathrm{P}-a_0)/\mathrm{X} = \mathrm{X}^{n-1} + \cdots + a_1$.

Alors $a_0 \neq 0$ car sinon on aurait $\alpha\mathrm{Q}(\alpha) = 0$ et donc $\mathrm{Q}(\alpha) = 0$, contredisant la minimalité de $n = \deg(\mathrm{P})$. Donc a_0 est un rationnel non nul, et l'égalité

$\mathrm{P}(\alpha) = 0$ se récrit $\alpha\mathrm{Q}(\alpha) = -a_0$. Ceci montre que l'élément

$$-\frac{\mathrm{Q}(\alpha)}{a_0} = \frac{-1}{a_0}\alpha^{n-1} - \cdots - \frac{a_1}{a_0},$$

qui appartient à l'anneau $\mathscr{K}$ (car $\mathscr{K}$ contient $\mathbb{Q}$ et α), est l'inverse de α. Le corollaire est démontré. □

De plus, $\mathscr{A}$ est **intégralement clos** dans $\mathbb{C}$, et $\mathscr{K} = \overline{\mathbb{Q}}$ est **algébriquement clos** dans $\mathbb{C}$, c.-à-d., on a la proposition suivante.

Proposition 2.42. — *Soient $\alpha_1, \ldots, \alpha_n$ des éléments de $\mathscr{A}$ (resp., de $\mathscr{K}$), et soit $\eta \in \mathbb{C}$ une racine de l'équation*

$$\mathrm{X}^n + \alpha_1\mathrm{X}^{n-1} + \cdots + \alpha_{n-1}\mathrm{X} + \alpha_n = 0. \tag{1}$$

Alors, $\eta \in \mathscr{A}$ (resp., $\eta \in \mathscr{K}$).

Démonstration. — On va prouver la première assertion, la seconde se traitant de la même manière. Par hypothèse, il existe des entiers

$$a_{11}, \ldots, a_{1r_1}, \quad a_{21}, \ldots, a_{2r_2}, \quad \ldots \quad a_{n1}, \ldots, a_{nr_n}$$

dans $\mathbb{Z}$ tels que

$$\begin{cases} \alpha_1^{r_1} = a_{11}\alpha_1^{r_1-1} + \cdots + a_{1r_1}, \\ \cdots \qquad\qquad\qquad \cdots \\ \alpha_n^{r_n} = a_{n1}\alpha_n^{r_n-1} + \cdots + a_{nr_n}. \end{cases} \tag{2}$$

Posons $\mathrm{N} = n\, r_1 \cdots r_n$ et désignons, comme précédemment, par $\omega_1, \ldots, \omega_\mathrm{N}$ les monômes

$$\eta^i \alpha_1^{i_1} \cdots \alpha_n^{i_n},$$

pour $0 \leqslant i \leqslant n-1$ et $0 \leqslant i_j \leqslant r_j - 1$, pour $j = 1, \ldots, n$; la numérotation étant choisie de sorte que $\omega_1 = 1$.

En utilisant les égalités (1) et (2), on obtient que chacun des N produits $\eta\omega_i$ peut s'exprimer comme une combinaison linéaire

$$\eta\omega_i = k_{i1}\omega_1 + \cdots + k_{i\mathrm{N}}\omega_\mathrm{N},$$

à coefficients $k_{ij} \in \mathbb{Z}$. On en déduit, comme dans la preuve du théorème 2.40, que le déterminant suivant est nul :

$$\begin{vmatrix} k_{11} - \eta & k_{12} & \cdots & k_{1\mathrm{N}} \\ k_{21} & k_{22} - \eta & \cdots & k_{2\mathrm{N}} \\ \cdots & \cdots & \cdots & \cdots \\ k_{\mathrm{N}1} & k_{\mathrm{N}2} & \cdots & k_{\mathrm{NN}} - \eta \end{vmatrix} = 0.$$

En développant ce déterminant, on obtient une équation

$$\eta^{\mathrm{N}} + e_1\eta^{\mathrm{N}-1} + \cdots + e_{\mathrm{N}-1}\eta + e_{\mathrm{N}} = 0,$$

avec les e_i dans $\mathbb{Z}$. Donc η est un entier algébrique, c.-à-d., $\eta \in \mathscr{A}$. Ceci montre que l'anneau $\mathscr{A}$ est intégralement clos dans $\mathbb{C}$, et la seconde assertion de la proposition s'obtient de façon exactement analogue. □

Remarque 2.43. — Une conséquence de la proposition précédente est que l'anneau $\mathscr{A}$ ne contient aucun élément irréductible. En effet, soit $\alpha \in \mathscr{A}$ un élément non inversible (par exemple, $\alpha = 2$), et soit β l'une des racines de l'équation $x^2 = \alpha$. Alors β appartient à $\mathscr{A}$ (d'après la proposition précédente), et β est non inversible (car sinon α le serait). Par conséquent, l'écriture $\alpha = \beta^2$ montre que α n'est pas irréductible.

La remarque précédente montre que, en un certain sens, $\mathscr{A}$ est "trop gros" pour posséder des éléments irréductibles. De façon plus précise, dans un anneau commutatif A (ou, si l'on veut, dans un sous-anneau A de $\mathbb{C}$), l'existence d'éléments irréductibles et d'une décomposition de tout élément comme produit fini d'irréductibles est, comme on le verra plus loin, une conséquence d'une propriété de "petitesse" de A, la **noethérianité**, c.-à-d., le fait que tout idéal de A soit engendré par un nombre fini d'éléments.

II. ANNEAUX ET MODULES

3. Anneaux et modules

3.0. Complément d'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. Un des premiers aspects de ce cours est donc une généralisation de **l'algèbre linéaire**. Par ailleurs, 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 diophantiennes) ; d'autre part, comme indiqué dans la section 1, une autre motivation du cours (et prolongement possible) est la **géométrie algébrique**, c.-à-d., l'étude des "variétés" définies par des équations polynomiales.

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 principal $\mathbb{C}[X]$.

3.1. Anneaux. —

Définition 3.1. — 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 $a,b,c\in \mathrm{A}$.
(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 3.2. — 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 3.3. — 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 3.4. — 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 3.5. — Un **corps** est un anneau commutatif $k \neq \{0\}$ dans lequel tout élément non nul est inversible.

Définition 3.6. — 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 3.7. — 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 : $\mathbb{Z}/6\mathbb{Z}$.

3.2. Morphismes. — Voici quelques généralités sur les morphismes.

Remarque 3.8. — 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 3.9. — 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 3.10. — 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 $f : \mathrm{A} \hookrightarrow \mathrm{B}$ 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 3.11. — 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 3.12. — *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.

3.3. A-modules. — Soit A un anneau.

Définition 3.13. — 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 3.14. — 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 3.15. — 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 3.16. — *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 $n \geqslant 1$

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

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

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

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 3.17. — *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 3.18 **(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 3.19. — 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 3.17. 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 3.20. — 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 3.21. — Si k est un corps, ses seuls idéaux sont $\{0\}$ et k.

Définition 3.22. — Pour tout $a \in \mathrm{A}$, on note

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

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 3.23. — 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 3.24. — 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 3.25. — *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.

4. Modules et anneaux quotients, théorèmes de Noether

4.1. 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 4.1. — (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 4.2* (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 $\mathrm{R} = \mathrm{PU}$ pour un certain $\mathrm{U} \in k[\mathrm{X}]$; comme

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

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

Remarque 4.3. — On montrera plus loin que tout $\mathbb{C}[\mathrm{X}]$-module qui est de dimension finie sur $\mathbb{C}$ est une somme directe de modules

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

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

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

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

Exercice 4.4. — 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 $r \in \mathbb{N}$, $x_i \in \mathrm{I}$, $m_i \in \mathrm{M}$. 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

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

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

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

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

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

On a donc démontré que les applications $\mathrm{L} \mapsto \pi^{-1}(\mathrm{L})$ et $\mathrm{M}' \mapsto \pi(\mathrm{M}') = \mathrm{M}'/\mathrm{N}$ 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 4.5. — *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 4.6. — Les deux théorèmes précédents s'appliquent en particulier au cas des groupes abéliens (c.-à-d., le cas $\mathrm{A} = \mathbb{Z}$).

Remarque 4.7. — 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 $\mathbb{R}[\mathrm{X}]/(\mathrm{X}^n)$.

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 la section 1. Le lecteur intéressé pourra consulter aussi, par exemple [**Pe2**], [**Re**] ou [**Die**].

4.2. Noyaux et théorèmes de Noether. —

Définition 4.8. — 1) Soit $f : M \to M'$ un morphisme de A-modules. Son noyau et son image :

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

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

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

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

est un sous-anneau commutatif de B.

Remarque 4.9. — 1) Une application d'ensembles $f : X \to Y$ est bijective si, et seulement si, elle est injective et surjective.

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

Théorème 4.10 **(Factorisation des morphismes)**. — 1) *Soit* $f : M \to M'$ *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*

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

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*

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

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 $\overline{f} : \mathrm{M/N} \to \mathrm{Im}(f) \subseteq \mathrm{M}'$ 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 $\overline{x}, \overline{y} \in \overline{\mathrm{M}} := \mathrm{M/N}$ 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 4.11. — 1) Comme $12\mathbb{Z} \subseteq 4\mathbb{Z}$, le 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 4.12 **(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 4.13 **(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* $\phi : \mathrm{M}/\mathrm{P} \to \mathrm{M}/\mathrm{N}$, $m + \mathrm{P} \mapsto m + \mathrm{N}$, *et son noyau est le sous-module* N/P.

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

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

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

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

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

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

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. □

5. Construction de modules ou d'idéaux

5.1. Sous-module ou idéal engendré. — Soit M un A-module.

Proposition 5.1. — *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 M = 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 5.2. — 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

$$\mathrm{A}x_1 + \cdots + \mathrm{A}x_r \quad \text{ou} \quad \sum_{i=1}^{r} \mathrm{A}x_i.$$

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

$$(\mathrm{S}) = \sum_{i \in \mathrm{I}} \mathrm{A}x_i,$$

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

Exercice 5.3. — Soit $\lambda \in \mathbb{C}$. Montrer que l'idéal $\mathrm{I}_\lambda = \{\mathrm{P} \in \mathbb{C}[\mathrm{X}] \mid \mathrm{P}(\lambda) = 0\}$ est l'idéal engendré par le polynôme $\mathrm{X} - \lambda$. (Utiliser la division euclidienne par $\mathrm{X} - \lambda$).

5.2. Sommes de sous-modules et sommes directes. — Soient $\mathrm{M}_1, \ldots, \mathrm{M}_n$ des sous-modules d'un A-module M.

***Définition 5.4* (Somme de sous-modules)**. — On note $\mathrm{M}_1 + \cdots + \mathrm{M}_n$ ou $\sum_{i=1}^n \mathrm{M}_i$ le sous-module de M engendré par $\mathrm{M}_1 \cup \cdots \cup \mathrm{M}_n$. Il résulte de la proposition 5.1 que $\mathrm{M}_1 + \cdots + \mathrm{M}_n$ est l'ensemble des éléments de la forme

$$x_1 + \cdots + x_n,$$

avec $x_i \in \mathrm{M}_i$ pour $i = 1, \ldots, n$.

Définition et proposition 5.5. — *On dit que les sous-modules* $\mathrm{M}_1, \ldots, \mathrm{M}_n$ *de* M *sont en* **somme directe** *si tout élément* $x \in \sum_{i=1}^n \mathrm{M}_i$ *s'écrit de façon* **unique** *sous la forme*

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

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

$$(*) \qquad \forall\, i = 1, \ldots, n, \qquad \mathrm{M}_i \cap \sum_{j \neq i} \mathrm{M}_j = \{0\}.$$

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

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

avec $x_j, x'_j \in \mathrm{M}_j$. 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 5.6. — 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 5.7. — 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 $\mathrm{M}^{\oplus n}$.

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

Définition 5.8. — 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 5.1, 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 5.1 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 5.9. — 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 5.10. — Si M est un A-module, on note M^n la somme directe $M \oplus \cdots \oplus M$. Ainsi, lorsque M est un idéal I, la notation I^n peut *a priori* faire référence ou bien au A-module $I \oplus \cdots \oplus I$ (somme directe externe de n copies de I), ou bien à l'idéal produit $I \cdots I$ (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 $I \cdots I$.

Lemme 5.11. — *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*

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

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

Démonstration. — Laissée au lecteur. □

5.4. Racine d'un idéal, et idéaux premiers. —

Définition 5.12. — Un élément $f \in A$ est dit **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que $f^n = 0$.

Définition 5.13. — Soient A un anneau commutatif et I un idéal de A. On pose

$$\sqrt{I} := \{a \in A \mid \exists\, n \geqslant 1 \text{ tel que } a^n \in I\}.$$

On voit sans difficultés, en utilisant la formule du binôme, que I est un idéal de A ; on l'appelle la **racine** (ou le **radical**) de I. En particulier, l'idéal $\sqrt{0}$ est l'ensemble des éléments nilpotents de A.

On dit que A est **réduit** si $\sqrt{(0)} = (0)$, c.-à-d., si A ne possède pas d'élément nilpotent non nul. On dira que I est **réduit** si $I = \sqrt{I}$, c.-à-d., si l'anneau quotient A/I est réduit.

L'intérêt de cette notion provient, en partie, du théorème suivant, qu'on démontrera plus loin dans le cours.

Théorème 5.14 **(Théorème des zéros de Hilbert)**. — *Soient* I *un idéal de* $\mathbb{C}[X_1, \ldots, X_n]$, $\mathscr{V}(I)$ *sa variété des zéros, et*

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

Alors, $\mathscr{I}(\mathscr{V}(I)) = \sqrt{I}$.

Ce théorème est utile pour avancer dans la résolution de l'exercice 1.2.

Lemme 5.15. — *Soient* I, J *deux idéaux de* A. *Alors*

$$\sqrt{\mathrm{IJ}} = \sqrt{\mathrm{I} \cap \mathrm{J}} = \sqrt{\mathrm{I}} \cap \sqrt{\mathrm{J}}.$$

Plus généralement, pour des idéaux $\mathrm{I}_1, \ldots, \mathrm{I}_n$, *on a*

$$\sqrt{\mathrm{I}_1 \cdots \mathrm{I}_n} = \sqrt{\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n} = \sqrt{\mathrm{I}_1} \cap \cdots \cap \sqrt{\mathrm{I}_n}.$$

Démonstration. — Comme $\mathrm{IJ} \subseteq \mathrm{I} \cap \mathrm{J} \subseteq \mathrm{I}, \mathrm{J}$, on a

$$\sqrt{\mathrm{IJ}} \subseteq \sqrt{\mathrm{I} \cap \mathrm{J}} \subseteq \sqrt{\mathrm{I}} \cap \sqrt{\mathrm{J}}.$$

Réciproquement, soit $x \in \sqrt{\mathrm{I}} \cap \sqrt{\mathrm{J}}$. Alors, il existe $m, n \in \mathbb{N}^*$ tels que $x^m \in \mathrm{I}$ et $x^n \in \mathrm{J}$, d'où $x^{m+n} \in \mathrm{IJ}$ et donc $x \in \sqrt{\mathrm{IJ}}$. Ceci prouve l'inclusion réciproque. La généralisation au cas de n idéaux est facile et laissée au lecteur. □

Définition 5.16 **(Idéaux premiers)**. — 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 $\mathrm{IJ} \not\subseteq \mathrm{P}$.

On laisse au lecteur le soin de vérifier l'équivalence des conditions ci-dessus.

Définition 5.17 **(Idéaux maximaux)**. — Soit I un idéal de A. On dit que I est un idéal **maximal** si $\mathrm{I} \neq \mathrm{A}$ et s'il n'existe pas d'idéal $\mathrm{J} \neq \mathrm{A}$ contenant strictement I.

On notera que, par définition, l'idéal A n'est ni maximal ni premier.

Lemme 5.18. — *Soit* I *un idéal de* A. *Alors :* I *est maximal* $\Leftrightarrow$ A/I *est un corps.*

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

Démonstration. — Supposons que A/I soit un corps et soit $x \in \mathrm{A} \setminus \mathrm{I}$. Alors, l'image $\overline{x}$ de x dans A/I est $\neq 0$, donc inversible, donc il existe $a \in \mathrm{A}$ tel que $\overline{a}\,\overline{x} = 1$. Ceci signifie que $ax - 1 \in \mathrm{I}$. Alors

$$1 = ax + (1 - ax) \in \mathrm{A}x + \mathrm{I}$$

et donc $\mathrm{I} + \mathrm{A}x = \mathrm{A}$, pour tout $x \notin \mathrm{I}$. Ceci prouve que I est maximal.

Réciproquement, supposons que I soit maximal et soit $x \notin \mathrm{I}$. Alors l'idéal $\mathrm{A}x + \mathrm{I}$ égale A, donc il existe $a \in \mathrm{A}$ et $y \in \mathrm{I}$ tels que $ax + y = 1$. Alors, dans A/I on a $\overline{a}\,\overline{x} = 1$ et ceci prouve que $\overline{x}$ est inversible. Comme x est arbitraire dans $\mathrm{A} \setminus \mathrm{I}$ ceci prouve que A/I est un corps. □

Notation 5.19. — On note Spec(A), resp. Max(A), l'ensemble des idéaux premiers, resp. maximaux, de A.

Le lemme suivant est très utile dans la pratique.

Lemme 5.20. — *Soit* $\mathrm{P} \in \mathrm{Spec(A)}$. *Soient* $x_1, \ldots, x_n \in \mathrm{A}$ *et* $\mathrm{I}_1, \ldots, \mathrm{I}_n$ *des idéaux de* A.

1) *Si* $x_1 \cdots x_n \in \mathrm{P}$, *alors* P *contient l'un des* x_k.

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

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

Démonstration. — Les points 1) et 2) se démontrent par récurrence sur n. Le point 3) découle de 2), car $\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n$ contient le produit $\mathrm{I}_1 \cdots \mathrm{I}_n$. □

Lemme 5.21. — 1) *Si* P *est un idéal premier contenant* I, *il contient aussi* $\sqrt{\mathrm{I}}$. *En particulier,* $\mathrm{P} = \sqrt{\mathrm{P}}$.

2) *Si* $\mathrm{P}_1, \ldots, \mathrm{P}_n \in \mathrm{Spec(A)}$, *l'idéal* $\mathrm{P}_1 \cap \cdots \cap \mathrm{P}_n$ *est réduit.*

Démonstration. — Soit $x \in \sqrt{\mathrm{I}}$; il existe $n \in \mathbb{N}^*$ tel que $x^n \in \mathrm{I} \subseteq \mathrm{P}$. Comme P est premier, ceci entraîne $x \in \mathrm{P}$. Ceci prouve la première assertion de 1), et la seconde en découle en prenant $\mathrm{P} = \mathrm{I}$.

Le point 2) découle du point 1) et du lemme 5.15. □

6. Modules libres

6.1. Définitions et exemples. —

Définition 6.1. — Soit M un A-module et soit $(x_i)_{i \in \mathrm{I}}$ une famille d'éléments de M.

1) On dit que $(x_i)_{i \in \mathrm{I}}$ est une **famille libre** si les x_i sont **linéairement indépendants** sur A, c.-à-d., si la propriété suivante est vérifiée :

Pour tout sous-ensemble fini $\mathrm{J} = \{i_1, \ldots, i_n\}$ de I, si $a_1, \ldots, a_n \in \mathrm{A}$ et $a_1 x_{i_1} + \cdots + a_n x_{i_n} = 0$, alors $a_i = 0$ pour tout $i = 1, \ldots, n$.

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

2) On dit que $(x_i)_{i\in \mathrm{I}}$ est une **base** de M si les x_i sont linéairement indépendants sur A et engendrent M ; ceci équivaut à dire que tout $m \in \mathrm{M}$ s'écrit de façon **unique** comme une somme finie

$$m = \sum_{i\in \mathrm{I}} a_i x_i,$$

où les a_i sont dans A et sont nuls sauf pour un nombre fini d'entre eux.

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

Remarque 6.2. — Si l'anneau A n'est pas un corps, il existe des A-modules qui ne sont pas libres. En effet, soit I un idéal propre non nul de A. Alors le A-module non nul A/I n'est pas libre. En effet, soit $\alpha \in \mathrm{I}$ non nul. Pour tout $x \in \mathrm{A/I}$, on a $\alpha x = 0$; par conséquent aucune famille non vide d'éléments de A/I n'est libre.

Une autre obstruction au fait d'être libre est donnée par la remarque suivante.

Remarque 6.3. — Toute partie libre de A est nécessairement réduite à un seul élément. En effet, entre deux éléments distincts $a, b \in \mathrm{A}$ on a toujours la relation de dépendance linéaire non triviale :

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

Comme conséquence de cette remarque, on a l'exemple suivant.

Exemple 6.4. — Soient $\mathrm{A} = \mathbb{C}[\mathrm{X}, \mathrm{Y}]$ et soit $\mathfrak{m} = (\mathrm{X}, \mathrm{Y})$, l'idéal engendré par X et Y. Alors, $\mathfrak{m}$ n'est pas un A-module libre.

En effet, s'il l'était, il aurait, d'après la remarque précédente, une base formée d'un seul polynôme $\mathrm{P} \neq 0$. Mais alors P, divisant X et Y, devrait être une constante $\lambda \in \mathbb{C}^*$, absurde puisque $\mathfrak{m} \neq \mathrm{A}$.

Par contre, voici des exemples de A-modules libres.

Exemples 6.5. — 1) Le A-module A possède la base $\{1\}$. Donc A est un A-module libre.

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

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

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

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

3) Soit A[X] l'anneau des polynômes sur A. Alors, comme A-module, A[X] possède la base $\{X^n\}_{n\geqslant 0}$. Donc A[X] est un A-module libre.

Plus généralement, on va voir dans le paragraphe suivant que pour tout ensemble I, il existe un A-module libre $A^{(I)}$ ayant une base paramétrée par I.

Remarque 6.6. — 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 6.3. Pourtant $\{2\}$ n'engendre pas $\mathbb{Z}$: le sous-module engendré est $2\mathbb{Z}$, l'idéal 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 6.3 : on a $3 \cdot 2 - 2 \cdot 3 = 0$.

6.2. Les modules libres $A^{(I)}$. — Soit A un anneau et soit I un ensemble arbitraire. On va construire « le » A-module libre $A^{(I)}$ de base I, et montrer qu'il possède une certaine propriété universelle, qui le caractérise à isomorphisme près. Pouvoir disposer de modules libres de bases arbitraires n'est pas une généralité gratuite : par exemple, le cas $I = \mathbb{N}^n$ permet de construire formellement l'anneau de polynômes à n variables

$$A[X_1, \ldots, X_n];$$

d'autre part, cette généralité est nécessaire pour la définition du produit tensoriel de deux modules (voir plus loin).

Pour obtenir le module libre $A^{(I)}$, on a d'abord besoin du module produit A^I ci-dessous.

Définition 6.7. — Le A-module produit

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

est l'ensemble des familles paramétrées par I d'éléments de A. L'addition est définie composante par composante, et l'action de A par :

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

Pour tout $i \in \mathrm{I}$, notons e_i la famille $(\delta_{ij})_{j\in\mathrm{I}}$, 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 6.8. — *Les e_i, pour $i \in \mathrm{I}$, sont linéairement indépendants sur* A.

Démonstration. — C'est clair. □

Définition 6.9. — On note $\mathrm{A}^{(\mathrm{I})}$ le sous-A-module de A^{I} engendré par les éléments e_i, pour $i \in \mathrm{I}$. Alors, d'après le lemme précédent, $(e_i)_{i\in\mathrm{I}}$ est une base de $\mathrm{A}^{(\mathrm{I})}$ et, d'après la définition du sous-A-module engendré, $\mathrm{A}^{(\mathrm{I})}$ est l'ensemble de toutes les sommes finies

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

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

Exemple 6.10. — Soit $\mathrm{I} = \mathbb{N}$. Alors $\mathrm{A}^{\mathbb{N}}$ est l'ensembles des **suites** $(a_0, a_1, \dots)$ d'éléments de A, et $\mathrm{A}^{(\mathbb{N})}$ est l'ensemble des suites **nulles à partir d'un certain rang**. Pour tout $i \in \mathbb{N}$, l'élément e_i est la suite

$$e_i = (0, \dots, 0, 1, 0, \dots), \quad \text{où 1 est à la } i\text{-ème place,}$$

et si $\underline{\mathbf{a}} = (a_0, a_1, \dots)$ est une suite nulle à partir d'un certain rang, c.-à-d., telle que $a_n = 0$ pour tout $n \geqslant n_0$, on a bien

$$\underline{\mathbf{a}} = \sum_{i\in\mathbb{N}} a_i e_i = \sum_{i=0}^{n_0} a_i e_i.$$

Remarque 6.11. — 1) Si $\mathrm{I} = \{1, \dots, n\}$ alors $\mathrm{A}^{(\mathrm{I})}$ égale A^{I} et s'identifie au A-module A^n déjà considéré, de base $(e_1, \dots, e_n)$.

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

Remarque 6.12. — On peut montrer (ce n'est pas facile) que le $\mathbb{Z}$-module produit $\mathbb{Z}^{\mathbb{N}}$ n'est pas un $\mathbb{Z}$-module libre, cf. [**BAlg**], Chap. VII, § 3, Exercice 8.

Afin d'énoncer la propriété universelle du A-module libre $\mathrm{A}^{(\mathrm{I})}$, introduisons la notation suivante. Pour tout ensemble Y, notons $\mathrm{Applic}(\mathrm{I}, \mathrm{Y})$ l'ensemble des applications $\mathrm{I} \to \mathrm{Y}$.

***Théorème 6.13* (Propriété universelle du A-module $\mathrm{A}^{(\mathrm{I})}$)**

Soit P *un* A*-module arbitraire. Pour avoir un morphisme de* A*-modules* $\phi : \mathrm{A}^{(\mathrm{I})} \to \mathrm{P}$*, il suffit d'avoir une application d'ensembles* $\psi : \mathrm{I} \to \mathrm{P}$*. De façon plus précise, l'application*

$$\mathrm{Hom}_{\mathrm{A}}(\mathrm{A}^{(\mathrm{I})}, \mathrm{P}) \longrightarrow \mathrm{Applic}(\mathrm{I}, \mathrm{P}) \cong \mathrm{P}^{\mathrm{I}}, \qquad \phi \mapsto \phi|_{\mathrm{I}},$$

où $\phi|_{\mathrm{I}}$ *désigne l'application* $i \mapsto \phi(e_i)$*, est une bijection. Son inverse est l'application* $\psi \mapsto \widetilde{\psi}$*, où* $\widetilde{\psi}$ *est définie, pour tout* $\underline{a} = \sum_{i\in\mathrm{I}} a_i e_i$*, par*

$$(*) \qquad \widetilde{\psi}\left(\sum_{i\in\mathrm{I}} a_i e_i\right) = \sum_{i\in\mathrm{I}} a_i \psi(e_i).$$

(*Le slogan à retenir est : « un morphisme de source un module libre est uniquement déterminé par l'image d'une base ».*)

Démonstration. — Observons d'abord que la formule $(*)$ qui définit $\widetilde{\psi}$ fait sens. En effet, pour chaque $\underline{a} = \sum_{i\in\mathrm{I}} a_i e_i$, il n'y a qu'un nombre fini de coefficients a_i qui sont $\neq 0$ et donc la somme de droite dans $(*)$ est une honnête somme finie d'éléments de P. Ceci étant vu, il est clair que $\widetilde{\phi|_{\mathrm{I}}} = \phi$ et $\widetilde{\psi}\Big|_{\mathrm{I}} = \psi$, c.-à-d., les applications $\phi \mapsto \phi|_{\mathrm{I}}$ et $\psi \mapsto \widetilde{\psi}$ sont inverses l'une de l'autre. Le théorème est démontré. □

III. ANNEAUX DE POLYNÔMES, CONDITIONS DE FINITUDE

7. Anneaux de polynômes

7.1. Polynômes en une variable. — Soit A un anneau commutatif. De la même façon qu'on a défini $\mathbb{R}[X]$, on peut définir l'anneau de polynômes $A[X]$.

Définition 7.1. — 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 :

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

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.

On renvoie à 3.6 pour la notion d'anneau intègre.

Proposition 7.2. — *Supposons* A *intègre. Alors, pour tout* $P, Q \in A[X] \setminus \{0\}$,

$$\deg(PQ) = \deg P + \deg Q.$$

En particulier, $A[X]$ *est intègre et ses éléments inversibles sont les éléments inversibles de* A.

Démonstration. — Soient $P, Q \in A[X] \setminus \{0\}$, de termes dominants aX^d et bX^f, respectivement, où $d = \deg P$ et $f = \deg Q$. Comme A est intègre, $ab \neq 0$ et donc PQ est de degré $d + f$. En particulier, $PQ \neq 0$.

De plus, si P est inversible, d'inverse Q, l'égalité $PQ = 1$ entraîne $\deg P = \deg Q = 0$, et donc P et Q sont des éléments inversibles de A. La proposition est démontrée. □

***Théorème 7.3* (Division euclidienne 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 $n + \deg U \geqslant \deg U$. 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 $n \geqslant d$ 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. □

Corollaire 7.4. — *Soient* A *un anneau intègre,* $U \in A[X]$ *un polynôme unitaire de degré* n. *Alors* $A[X]/(U)$ *est un* A*-module libre, de base les images des monômes* $1, X, \ldots, X^{n-1}$.

Démonstration. — Posons $\mathrm{B} = \mathrm{A}[\mathrm{X}]/(\mathrm{U})$ et notons x l'image de X dans B. Il résulte de la division euclidienne que les éléments $1, x, \ldots, x^{n-1}$ engendrent B comme A-module. De plus, ils sont linéairement indépendants sur A : si on a une égalité

$$\sum_{i=0}^{n-1} a_i x^i = 0,$$

alors le polynôme $\mathrm{P} = \sum_{i=0}^{n-1} a_i \mathrm{X}^i$ appartient à l'idéal (U) ; comme P est nul ou bien de degré $< n = \deg \mathrm{U}$, ceci n'est possible que si $\mathrm{P} = 0$, c.-à-d., si tous les a_i sont nuls. Ceci montre que $\{1, \ldots, x^{n-1}\}$ est une base du A-module B. □

7.2. Polynômes à n variables. — On va généraliser la construction de l'anneau de polynômes A[X] au cas de n indéterminées $\mathrm{X}_1, \ldots, \mathrm{X}_n$. Commençons par le cas $n = 2$, c.-à-d., le cas de deux indéterminées X et Y.

Définition 7.5. — Soit A[X, Y] le A-module libre de base les monômes $\mathrm{X}^r\mathrm{Y}^s$, pour $(r, s) \in \mathbb{N}^2$. On définit le degré d'un tel monôme comme étant $r + s$.

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

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

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

$$\left(\sum_{\substack{(r,s)\in\mathbb{N}^2 \\ r+s\leqslant m}} a_{r,s}\mathrm{X}^r\mathrm{Y}^s\right)\left(\sum_{\substack{(t,u)\in\mathbb{N}^2 \\ t+u\leqslant n}} b_{t,u}\mathrm{X}^t\mathrm{Y}^u\right)$$

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

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 :

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

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

$$\mathrm{X}_1^{\nu_1} \cdots \mathrm{X}_n^{\nu_n};$$

il est de degré $|\nu|$. On peut alors définir l'anneau de polynômes $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ comme suit.

Proposition 7.6. — *Soit* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *le* A*-module libre de base les monômes*

$$\mathrm{X}^\nu := \mathrm{X}_1^{\nu_1} \cdots \mathrm{X}_n^{\nu_n},$$

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

Tout élément $\mathrm{P} \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *est une somme finie de termes* $a_\nu \mathrm{X}^\nu$*, avec* $a_\nu \in \mathrm{A}$*, et le plus grand des degrés* $|\nu|$ *tels que* $a_\nu \neq 0$ *s'appelle le degré de* P *et se note* $\deg \mathrm{P}$ *; ainsi* P *peut s'écrire comme somme finie*

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

où $n = \deg \mathrm{P}$*. On munit* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *de la multiplication définie par*

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

Définition 7.7. — Soient A, B deux **anneaux commutatifs**. On dit que B est une **A-algèbre** si l'on s'est donné un morphisme d'anneaux $\phi : \mathrm{A} \to \mathrm{B}$. Dans ce cas, B est aussi un A-module, via

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

Définition 7.8. — Soient $\phi : \mathrm{A} \to \mathrm{B}$ et $\psi : \mathrm{A} \to \mathrm{C}$ deux A-algèbres. Un **morphisme de A-algèbres** $f : \mathrm{B} \to \mathrm{C}$ 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 $a \in \mathrm{A}$, $b \in \mathrm{B}$.

Remarque 7.9. — Si A est un sous-anneau de B et de C, un morphisme de A-algèbres $f : \mathrm{B} \to \mathrm{C}$ est simplement un morphisme d'anneaux $f : \mathrm{B} \to \mathrm{C}$ tel que $f(a) = a$, pour tout $a \in \mathrm{A}$.

***Théorème 7.10* (Propriété universelle de $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$).** — *Soit $\rho : \mathrm{A} \to \mathrm{B}$ une* A*-algèbre. Pour tout n-uplet $(b_1, \ldots, b_n)$ d'éléments de* B*, il existe un unique morphisme de* A*-algèbres*

$$\phi : \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \longrightarrow \mathrm{B}$$

prolongeant ρ et tel que $\phi(\mathrm{X}_i) = b_i$, pour $i = 1, \ldots, n$.

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

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

Réciproquement, l'application $\phi : \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{B}$ définie par la formule $(*)$ est A-linéaire et vérifie $\phi(1) = 1$. Il reste à vérifier que $\phi(\mathrm{PQ}) = \phi(\mathrm{P})\phi(\mathrm{Q})$, pour tout $\mathrm{P}, \mathrm{Q} \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Par bilinéarité, il suffit de le vérifier lorsque $\mathrm{P} = \mathrm{X}^\nu$ et $\mathrm{Q} = \mathrm{X}^\eta$ sont des monômes. Mais alors c'est clair, car

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

Ceci prouve le théorème. □

***Corollaire 7.11*.** — *Pour tout $n \geqslant 1$, on a un isomorphisme de* A*-algèbres*

$$\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \cong (\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}])[\mathrm{X}_n].$$

Démonstration. — Posons $\mathscr{A} = \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et $\mathscr{B} = \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}]$. D'après la propriété universelle de $\mathscr{A}$, il existe un (unique) morphisme de A-algèbres

$$\phi : \mathscr{A} \longrightarrow \mathscr{B}[\mathrm{X}_n] \quad \text{tel que} \quad \phi(\mathrm{X}_i) = \mathrm{X}_i, \qquad \forall\, i = 1, \ldots, n.$$

D'autre part, $\mathscr{B}$ est un sous-anneau de $\mathscr{A}$, donc $\mathscr{A}$ est une $\mathscr{B}$-algèbre et, d'après la propriété universelle de $\mathscr{B}[\mathrm{X}_n]$, il existe un unique morphisme de $\mathscr{B}$-algèbres

$$\psi : \mathscr{B}[\mathrm{X}_n] \longrightarrow \mathscr{A} \quad \text{tel que} \quad \phi(\mathrm{X}_i) = \mathrm{X}_i, \qquad \forall\, i = 1, \ldots, n.$$

Alors ϕ et ψ sont des isomorphismes réciproques. □

8. Conditions de finitude

8.1. Union filtrante de sous-modules. — Soit M un A-module.

Définition 8.1. — Une famille de sous-modules $(\mathrm{M}_i)_{i\in\mathrm{I}}$ de M est dite **filtrante** si elle vérifie la propriété suivante :

(filt) $$\forall\, i,j,\quad \exists\,\ell \ \text{ tel que } \ \mathrm{M}_i+\mathrm{M}_j\subseteq\mathrm{M}_\ell.$$

Remarque 8.2. — En particulier, toute suite croissante de sous-modules $\mathrm{M}_0\subseteq\mathrm{M}_1\subseteq\cdots$ est une famille filtrante : il suffit de prendre $\ell=\max\{i,j\}$. Mais on peut rencontrer des familles filtrantes de sous-modules plus générales.

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

Lemme 8.3. — *Soit* $(\mathrm{M}_i)_{i\in\mathrm{I}}$ *une famille filtrante de sous-*A*-modules de* M*. Alors, la réunion*

$$\mathrm{U}:=\bigcup_{i\in\mathrm{I}}\mathrm{M}_i$$

*est un sous-*A*-module de* M*.*

Démonstration. — Soient $a\in\mathrm{A}$ et $x,y\in\mathrm{U}$. Alors, il existe $i,j\in\mathrm{I}$ tels que $x\in\mathrm{M}_i$ et $y\in\mathrm{M}_j$ et donc, comme la famille est filtrante, il existe $\ell\in\mathrm{I}$ tel que $x,y\in\mathrm{M}_\ell$. Comme M_ℓ est un sous-module, on a $x+ay\in\mathrm{M}_\ell$, et donc $x+ay\in\mathrm{U}$. Ceci prouve le lemme. □

8.2. Modules de type fini. — Soient A un anneau, M un A-module.

Définition 8.4. — Soit $(x_i)_{i\in\mathrm{I}}$ (où I est un ensemble fini ou infini) une famille d'éléments de M. On rappelle (cf. proposition 5.1) que le sous-module engendré par les x_i est l'ensemble des sommes **finies**

$$\sum_{\substack{\mathrm{J}\subset\mathrm{I}\\ \mathrm{J\ fini}}} a_jx_j,\qquad a_j\in\mathrm{A}.$$

On le note $\sum_{i\in\mathrm{I}}\mathrm{A}x_i$, étant entendu que ceci désigne l'ensemble des sommes finies de termes a_ix_i.

En particulier, lorsque I est un ensemble fini, $\mathrm{I}=\{1,\dots,n\}$, le sous-module engendré par $x_1,\dots,x_n\in\mathrm{M}$ est

$$\mathrm{A}x_1+\cdots+\mathrm{A}x_n=\{a_1x_1+\cdots+a_nx_n\mid a_i\in\mathrm{A}\};$$

on le note aussi $(x_1,\dots,x_n)$.

Définition 8.5. — On dit qu'un A-module M est **de type fini** s'il peut être engendré par un nombre fini d'éléments, c.-à-d., s'il existe $x_1,\dots,x_n\in\mathrm{M}$ tels que

$$\mathrm{M}=\mathrm{A}x_1+\cdots+\mathrm{A}x_n,$$

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

Exemples 8.6. — 1) Le A-module A est de type fini : il est engendré par l'élément 1 puisque $a = a1$ pour tout $a \in \mathrm{A}$.

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

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

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 $\mathrm{A} = k$ 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 $\overline{1}$. Par contre, ici, l'écriture n'est pas unique puisque $a\overline{1} = b\overline{1}$ si $a - b \in n\mathbb{Z}$.

Exercice 8.7. — Soit V un $\mathbb{R}$-espace vectoriel. Montrer que V est de type fini comme $\mathbb{R}$-module si et seulement si $\dim_{\mathbb{R}} \mathrm{V} < \infty$. Donc, pour un espace vectoriel, type fini = dimension finie.

Proposition 8.8. — *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. — 1) Soit $\pi : \mathrm{M} \to \mathrm{M/N}$. Supposons M engendré par des éléments $x_1, \ldots, x_n$. Alors tout $m \in \mathrm{M}$ 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 $y_1, \ldots, y_s \in \mathrm{N}$ des générateurs de N et soient $x_1, \ldots, x_r \in \mathrm{M}$ dont les images engendrent M/N. Soit $m \in \mathrm{M}$ arbitraire. Alors, il existe $a_1, \ldots, a_r \in \mathrm{A}$ tels que

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

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

Donc, il existe $b_1, \ldots, b_s \in \mathrm{A}$ 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 $x_1, \dots, x_r$, $y_1, \dots, y_s$. La proposition est démontrée. □

Remarque 8.9. — **Attention**, un sous-module d'un module de type fini n'est pas nécessairement de type fini. Voici deux exemples.

1) Soit A l'anneau des polynômes sur $\mathbb{C}$ en une infinité de variables :

$$\mathbb{C}[\mathrm{X}_1, \mathrm{X}_2, \dots] = \bigcup_{n \geqslant 1} \mathbb{C}[\mathrm{X}_1, \dots, \mathrm{X}_n],$$

et soit $\mathfrak{m}$ l'idéal de A engendré par les X_i. Bien sûr, A est un A-module de type fini, engendré par 1, mais on va montrer que le sous-module (l'idéal) $\mathfrak{m}$ n'est pas de type fini. On a la suite croissante d'idéaux

$$(\mathrm{X}_1) \subseteq (\mathrm{X}_1, \mathrm{X}_2) \subseteq (\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3) \subseteq \cdots$$

et $\mathfrak{m}$ en est la réunion. Supposons que $\mathfrak{m}$ soit engendré par un nombre fini d'éléments $\mathrm{Q}_1, \dots, \mathrm{Q}_r$; alors, ils sont tous dans un certain $(\mathrm{X}_1, \dots, \mathrm{X}_n)$ et donc

$$\mathfrak{m} = (\mathrm{X}_1, \dots, \mathrm{X}_n).$$

Par conséquent, il existe $\mathrm{P}_1, \dots, \mathrm{P}_n \in \mathrm{A}$ tels que

$$(*) \qquad \mathrm{X}_{n+1} = \sum_{i=1}^{n} \mathrm{P}_i \mathrm{X}_i.$$

Tous les P_i appartiennent à $\mathbb{C}[\mathrm{X}_1, \dots, \mathrm{X}_\mathrm{N}]$, pour un certain $\mathrm{N} \geqslant n+1$, et donc l'égalité $(*)$ ci-dessus a lieu dans l'anneau $\mathbb{C}[\mathrm{X}_1, \dots, \mathrm{X}_\mathrm{N}]$. Alors, on peut évaluer X_{n+1} en 1, et les autres X_i, pour $i \leqslant \mathrm{N}$, $i \neq n+1$, en 0, et $(*)$ donne $1 = 0$, une contradiction ! Ceci montre que l'idéal $\mathfrak{m}$ n'est pas de type fini.

2) Soit $\mathscr{A}$ l'anneau des entiers algébriques de $\mathbb{C}$ (voir 2.40). Soit $\alpha_0 \in \mathscr{A}$ un élément non inversible (par exemple, $\alpha_0 = 2$) et, pour tout $n \geqslant 1$, soit α_n une racine 2^n-ième de α. Alors, 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

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

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

Toutefois, cette « pathologie » ne se produit pas pour les anneaux et modules noethériens, qu'on va étudier plus bas.

8.3. Anneaux et modules noethériens. — Soient A un anneau et M un A-module.

Proposition 8.10. — *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*

$$\mathrm{N}_0 \subseteq \mathrm{N}_1 \subseteq \mathrm{N}_2 \subseteq \cdots$$

il existe un entier k tel que $\mathrm{N}_i = \mathrm{N}_k$ pour tout $i \geqslant k$.

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

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

$$(*) \qquad \mathrm{N}_0 \subseteq \mathrm{N}_1 \subseteq \mathrm{N}_2 \subseteq \cdots$$

une suite croissante de sous-modules. Posons $\mathrm{N} = \bigcup_{i \geqslant 0} \mathrm{N}_i$; 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 $\mathrm{N} = \mathrm{N}_r$ et la suite $(*)$ est stationnaire à partir du cran r.

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

$$\mathrm{N}_0 \subset \mathrm{N}_1 \subset \mathrm{N}_2 \subset \cdots$$

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

3) $\Rightarrow$ 1) Soit N un sous-module de M et soit $\mathscr{F}$ 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 $n \in \mathrm{N}$ arbitraire. Alors $\mathrm{N}' + \mathrm{A}n$ 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 $\mathrm{N}' = \mathrm{N}' + \mathrm{A}n$, d'où $n \in \mathrm{N}'$. Ceci montre que $\mathrm{N}' = \mathrm{N}$, et donc N est de type fini. La proposition est démontrée. □

Définition 8.11. — 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).

Définition 8.12. — On dit que l'anneau A est **noethérien** s'il est noethérien comme A-module, c.-à-d., si tout idéal de A est de type fini.

Exemples 8.13. — Tout corps k est un anneau noethérien (car les seuls idéaux de k sont (0) et (1)).

D'autre part, l'anneau $\mathbb{Z}$ est noethérien car on a vu (2.3) que tout idéal de $\mathbb{Z}$ est *principal*, c.-à-d., engendré par un élément.

Proposition 8.14. — *Soient* M *un* A*-module,* N *un sous-module, et* $\mathrm{Q} = \mathrm{M}/\mathrm{N}$ *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 $\mathrm{Q}' = \mathrm{M}'/\mathrm{N}$, où $\mathrm{M}' = \pi^{-1}(\mathrm{Q}')$ est un sous-module de M. Par hypothèse, M' est de type fini, donc Q' l'est aussi, d'après le point 1) de la proposition 8.8.

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

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

est un sous-module de Q, donc est de type fini. Par conséquent, d'après le point 2) de la proposition 8.8, M' est de type fini. Ceci montre que M est noethérien. □

Corollaire 8.15. — *Soit* $\mathrm{M}_1, \cdots, \mathrm{M}_n$ *un nombre fini de modules noethériens. Alors* $\mathrm{M}_1 \oplus \cdots \oplus \mathrm{M}_n$ *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 4.12), le module quotient $(M_1 \oplus M_2)/M_1$ est isomorphe à M_2. Donc, dans ce cas, le résultat découle du point 2) de la proposition précédente.

Enfin, le cas général s'en déduit par récurrence, puisque pour tout $n \geqslant 3$ 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. □

Corollaire 8.16. — *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 4.10, 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 8.14. □

8.4. Le théorème de transfert de Hilbert. —

Théorème 8.17 **(Théorème de transfert de Hilbert)**. — *Soit* A *un anneau noethérien. Alors* A[X] *est noethérien.*

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 le corollaire 8.16.

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 $\mathrm{P} \neq 0$ de I, de degré n, appartient à J. C'est clair si $n < d$, car dans ce cas $\mathrm{P} \in \mathrm{N}$ donc est combinaison A-linéaire de $\mathrm{Q}_1, \ldots, \mathrm{Q}_s$. Soit donc $n \geqslant d$ et supposons l'assertion établie pour tout $n' < n$. Soit $\mathrm{P} \in \mathrm{I} \setminus \{0\}$, de degré n, et soit α son coefficient dominant. Alors $\alpha \in \mathrm{D}$ donc il existe $a_1, \ldots, a_r \in \mathrm{A}$ tels que

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

Alors,

$$a_1\alpha_1\mathrm{X}^{n-d_1}\mathrm{P}_1 + \cdots + a_r\alpha_r\mathrm{X}^{n-d_r}\mathrm{P}_r$$

a pour terme dominant $\alpha\mathrm{X}^n$, et donc

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

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

Remarque 8.18. — En anglais, le théorème précédent est appelé « Hilbert's Basis Theorem ».

Corollaire 8.19. — *Si* A *est noethérien, alors* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *l'est aussi, pour tout* $n \in \mathbb{N}$.

Démonstration. — Ceci découle, par récurrence sur n, du théorème précédent et du corollaire 7.11. □

Soit $\rho : \mathrm{A} \to \mathrm{B}$ une A-algèbre commutative.

Définition et proposition 8.20. — *Soit* S *un sous-ensemble non vide de* B. *On note* A[S] *le sous-*A*-module de* B *engendré par tous les monômes*

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

*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 8.21. — 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 8.22. — 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 8.23. — B *est une* A*-algèbre de type fini* $\Leftrightarrow$ B *est isomorphe à un quotient d'une algèbre de polynômes* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

Démonstration. — Supposons B engendrée comme A-algèbre par $x_1, \ldots, x_n$. D'après la propriété universelle de l'algèbre $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ (7.10), ρ se prolonge en un morphisme de A-algèbres $\phi : \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{B}$ tel que $\phi(\mathrm{X}_i) = x_i$ pour $i = 1, \ldots, n$. Ce morphisme est surjectif (car les x_i engendrent B comme A-algèbre), donc induit un isomorphisme de A-algèbres

$$(*) \qquad \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathrm{I} \xrightarrow{\sim} \mathrm{B},$$

où $\mathrm{I} = \mathrm{Ker}(\phi)$. 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. □

Théorème 8.24. — *Si* A *est noethérien, toute* A*-algèbre* B *de type fini est noethérienne.*

Démonstration. — Soit B une A-algèbre de type fini. D'après la proposition précédente, on a un isomorphisme

$$\mathrm{B} \cong \mathscr{A}/\mathrm{I}, \qquad \text{où} \quad \mathscr{A} = \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n],$$

pour un certain $n \geqslant 1$, et où I est un idéal de $\mathscr{A}$.

D'après 8.19, $\mathscr{A}$ est noethérien et, d'après 8.14, B est noethérien comme $\mathscr{A}$-module, donc aussi comme B-module (puisque tout idéal de B est un sous-$\mathscr{A}$-module de B). Donc, B est un anneau noethérien. □

Corollaire 8.25. — *Toute algèbre de type fini sur* $\mathbb{Z}$*, ou sur un corps* k*, est un anneau noethérien.*

On obtient donc, en particulier, le résultat annoncé en 1.4 : tout idéal I de $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est engendré par un nombre fini d'éléments.

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.

[Ca] J.-C. Carrega, Théorie des corps – La règle et le compas, Hermann, 1981, 2ème édition 1989.

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

[Co] H. S. M. Coxeter, Introduction to Geometry, 2nd edition, Wiley, 1969.

[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, Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

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

[Fu] W. Fulton, Algebraic Curves, Benjamin, 1969.

[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. Nekovář, 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.

[Re] M. Reid, Undergraduate commutative algebra, Cambridge Univ. Press, 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.