Algèbre Commutative

Jean-François Dat

2024-2025

Résumé

Ce cours introduit les techniques algébriques fondamentales utilisées en théorie des nombres et en géométrie algébrique. On parlera d'anneaux, d'algèbres, de modules, de leurs propriétés et de constructions utiles comme le passage au quotient, la localisation ou le produit tensoriel. On mettra l'accent sur les applications à la géométrie algébrique, celles à la théorie des nombres étant abordées dans un autre cours du second semestre.

Table des matières

1 Pourquoi l'algèbre commutative

L'algèbre commutative est l'étude des anneaux commutatifs et de leurs modules. On rappelle qu'un *anneau (unitaire)* A est un ensemble muni d'une addition $+ : A \times A \longrightarrow A$ qui admet un élément neutre noté 0 et fait de $(A, +)$ un groupe abélien, et d'une multiplication (ou produit) $\cdot : A \times A \longrightarrow A$ qui admet un élément neutre 1 et fait de $(A, \cdot)$ un monoïde associatif, et telles que $\cdot$ soit "distributive" (ou encore "bilinéaire") par rapport à $+$. Cet anneau est dit commutatif si la multiplication $\cdot$ est commutative. Nous noterons $A^\times$ le sous-ensemble des éléments de A qui sont inversibles pour la multiplication, de sorte que $(A^\times, \cdot)$ est un groupe. Lorsque $A^\times = A \setminus \{0\}$, on dit que A est un corps.

Certaines définitions et énoncés de ce cours pourront paraitre bien abscons sortis de leur contexte. C'est pourquoi il est important de garder en tête pourquoi et comment les

mathématiciens y ont été conduits. Ce n'est pas le plaisir de l'abstraction qui les a guidés, mais bien le désir de résoudre des problèmes concrets en les reformulant convenablement.

1.1 L'anneau des entiers

Le premier exemple d'anneau commutatif est l'anneau $A = \mathbb{Z}$ des entiers relatifs. Sa structure additive est claire (comme le sera celle de la plupart des anneaux que nous rencontrerons) : elle est engendrée par 1 qui en est la seule "brique élémentaire". C'est la structure multiplicative et son interaction avec l'addition qui est intéressante. Ses "briques élémentaires" en sont les nombres premiers, sur lesquels de nombreuses conjectures sont encore ouvertes. Rappelons le résultat célèbre d'Euclide :

THÉORÈME. (Unique factorisation) – *Tout nombre entier s'écrit sous la forme* $n = \pm p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r}$*, où les* p_i *sont des nombres* premiers *distincts 2 à 2 et* $v_i \in \mathbb{N}^*$*, et cette écriture est unique à l'ordre près.*

L'existence d'une factorisation comme ci-dessus se voit facilement par récurrence mais l'unicité est plus subtile. Rappelons qu'elle découle de la *division euclidienne* selon les étapes suivantes :

- (lemme de Bézout) *si* $a, b \in \mathbb{Z} \setminus \mathbb{Z}^\times$ *n'ont pas de diviseur commun, alors il existe* $u, v \in \mathbb{Z}$ *tels que* $ua + vb = 1$. En effet, posons $r_0 := |a|$ et $r_1 := |b|$ et notons r_2 le reste de la division euclidienne de a par b. On a donc $r_2 \in r_0 + \mathbb{Z}r_1$ et $0 \leqslant r_2 < r_1$. Notons que $r_2 \neq 0$ puisque r_1 ne divise pas r_0. Si $r_2 = 1$, on a terminé. Sinon, on peut considérer encore le reste $0 < r_3 < r_2$ de la division euclidienne de r_1 par r_2, puis, tant que $r_k \neq 1$, définir r_{k+1} comme le reste de la division de r_{k-1} par r_k. On a alors $r_{k+1} \in r_{k-1} + \mathbb{Z}r_k$ puis, par une récurrence immédiate, $r_{k+1} \in \mathbb{Z}r_0 + \mathbb{Z}r_1$. Mais puisque $r_{k+1} < r_k$, l'algorithme s'arrête à un rang $k < |b|$ pour lequel on a $r_{k+1} = 1$.
- (lemme d'Euclide) *si* p *premier divise* ab*, alors* $p|a$ *ou* $p|b$. En effet, si p ne divise pas a, on peut trouver u, v tels que $up + va = 1$, donc $upb + vab = b$, ce qui montre que p divise b.
- On en déduit en particulier que si p divise un produit $p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r}$ comme dans le théorème, alors p est égal à l'un des p_i. De là l'unicité découle facilement : si $p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r} = {p'_1}^{v'_1} {p'_2}^{v'_2} \cdots {p'_{r'}}^{v'_{r'}}$ alors p_1 est égal à un (et un seul) des p'_i et, quitte à numéroter on peut supposer que c'est p'_1. Procédant de même pour p_2 et les suivants, on voit que $r = r'$ et qu'on peut supposer $p_i = p'_i$ pour tout i. Reste à montrer que $v_i = v'_i$ pour tout $i = 1, \cdots, r$, ce que l'on peut faire par récurrence sur l'entier $v_1 + \cdots + v_r$ par exemple.

L'énoncé d'Euclide peut s'écrire de la manière alternative suivante : soit p premier et soit $\nu_p(n)$ la *valuation p-adique de n*, *i.e.* le plus grand entier tel que $p^{\nu_p(n)}$ divise n.

On a l'égalité $n = \varepsilon(n) \cdot \prod_p p^{\nu_p(n)}$*, où* $\varepsilon(n)$ *désigne le signe de n et le produit est indexé par tous les nombres premiers*[1].

1. Cette expression, pour avoir un sens, sous-entend que $\nu_p(n) \neq 0$ et donc $p^{\nu_p(n)} \neq 1$ seulement pour un nombre fini de nombres premiers

Le résultat d'Euclide a plusieurs conséquences auxquelles nous sommes habitués depuis longtemps, comme l'existence de pgcd et de ppcm. La formulation ci-dessus fournit d'ailleurs les formules agréables suivantes :

$$\mathrm{pgcd}(n,m) = \prod_p p^{\min(\nu_p(n),\nu_p(m))} \text{ et } \mathrm{ppcm}(n,m) = \prod_p p^{\max(\nu_p(n),\nu_p(m))}.$$

Surtout, le résultat d'Euclide permet de résoudre certaines équations "diophantiennes", c'est-à-dire des équations polynômiales dont on cherche les solutions dans $\mathbb{Z}$ ou dans $\mathbb{Q}$. Exemples :

- L'équation $x^2 = 2$ n'a pas de solution dans $\mathbb{Q}$ (exercice).
- L'équation $x^2 - 1 = y^3$ a pour solutions $\{(0,-1),(1,0),(-1,0),(3,2),(-3,2)\}$. En effet, on peut factoriser $x^2 - 1 = (x-1)(x+1)$. Cherchons une solution (x,y) avec x pair. Dans ce cas le p.g.c.d. de $x-1$ et $x+1$ est 1, et la propriété d'unique factorisation implique donc que $x-1$ et $x+1$ doivent être des cubes d'entiers, disons $x-1 = a^3$ et $x+1 = b^3$ avec $ab = y$. Or, cela implique $b^3 - a^3 = 2$, ce qui implique $b = 1$ et $a = -1$ et donc $x = 0$ et $y = -1$. Cherchons ensuite une solution avec x impair, disons $x = 2x' + 1$. Alors y doit être pair, disons $y = 2y'$, et on a $x'(x'+1) = 2y'^3$. Si $x' = 2x''$ est pair, alors x'' et $(x'+1)$ doivent être des cubes, disons a^3 et b^3, vérifiant la relation $b^3 - 2a^3 = 1$. On se convainc à coup de majorations grossières que les seules solutions sont $(b,a) = (1,0)$ ou $(-1,-1)$, auxquels cas $(x,y) = (1,0)$ ou $(-3,2)$. Pour x' impair, on trouve les possibilités $(-1,0)$ et $(3,2)$.

Malheureusement, on est vite confronté à des équations, pourtant très proches, où la méthode de factorisation ne s'applique plus du tout. Par exemple :

$$x^2 + N = y^3, \text{ où } N \in \mathbb{Z} \text{ est fixé.}$$

L'idée, naturelle, qu'ont eu les mathématiciens est d'élargir le domaine des nombres "utilisables" de manière à pouvoir factoriser $x^2 + N$.

1.2 Anneaux d'entiers algébriques

Nous supposerons, pour simplifier, que l'on dispose du corps $\mathbb{C}$ des nombres complexes et qu'on sait qu'il est algébriquement clos. Pour $z \in \mathbb{C}$ nous noterons $\mathbb{Z}[z]$ le sous-anneau de $\mathbb{C}$ *engendré par* z, *i.e.* le plus petit sous-anneau de $\mathbb{C}$ qui contient z. Concrètement, c'est le sous-groupe additif de $\mathbb{C}$ engendré par les puissances $\{z^n, n \in \mathbb{N}\}$ de z (s'en convaincre !).

Définition. – *On dit que z est un* entier algébrique *s'il est annulé par un polynôme unitaire $f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$.*

Dans ce cas, $z^d \in \mathbb{Z} + \mathbb{Z}z + \cdots + \mathbb{Z}z^{d-1}$ et par récurrence immédiate chaque z^n pour $n \geqslant d$ est dans $\mathbb{Z} + \mathbb{Z}z + \cdots + \mathbb{Z}z^{d-1}$. En d'autres termes, $\mathbb{Z}[z]$ est engendré, en tant que groupe abélien par la famille *finie* $\{1, z, \cdots, z^{d-1}\}$.

Exemple. – L'anneau $\mathbb{Z}[i]$ et l'équation $x^2+1=y^3$. Le complexe i est annulé par le polynôme X^2+1, donc est un entier algébrique. L'anneau qu'il engendre $\mathbb{Z}[i]=\mathbb{Z}\oplus\mathbb{Z}i$ est appelé "anneau des entiers de Gauss". Il se trouve que cet anneau est muni d'un analogue de la division euclidienne :

$$\textit{Pour tous } x,y\in\mathbb{Z}[i] \textit{ avec } x\neq 0, \textit{ il existe } (q,r)\in\mathbb{Z}[i]^2 \textit{ tels que } y=qx+r \textit{ avec } |r|^2<|x|^2.$$

En fait, si q désigne le (ou un des) point(s) de $\mathbb{Z}\oplus\mathbb{Z}i$ le plus proche de y/x dans $\mathbb{C}$, alors $y/x-q$ est dans le carré défini par les inégalités $|\Re(z)|\leqslant\frac{1}{2}$ et $|\Im(z)|\leqslant\frac{1}{2}$, qui lui même est contenu dans le disque $\{z,|z|<1\}$, donc on a bien $|y-qx|^2<|x|^2$. On dit que $\mathbb{Z}[i]$ muni de la fonction $z\mapsto|z|^2$ est un *anneau euclidien.* Cette division euclidienne montre, comme dans le théorème précédent, que le *lemme de Bézout* est vrai dans $\mathbb{Z}[i]$. De même, le *lemme d'Euclide* est vrai, une fois qu'on a défini correctement l'analogue de ce qu'est un nombre premier.

Définition. – *Dans un anneau commutatif A général, un élément $a\in A$ est dit* irréductible *s'il est non inversible et si $a=bc\Rightarrow b\in A^\times$ ou $c\in A^\times$. Deux éléments irréductibles a,a' sont dits* équivalents *s'il existe un inversible $u\in A^\times$ tel que $a'=ua$.*

Par exemple dans $\mathbb{Z}$, les irréductibles sont les $a=\pm p$ avec p premier, et les classes d'équivalences d'irréductibles sont les $\{-p,p\}$ avec p premier. Dans un anneau général A, on dit que le *lemme d'Euclide* est satisfait si pour tout élément irréductible a divisant un produit bc, on a $a|b$ ou $a|c$. Par le même raisonnement que dans le théorème précédent, un tel anneau satisfait la propriété d'*unicité des factorisations en produit de puissances d'irréductibles.*

Définition. – *Soit A un anneau et supposons fixé un ensemble $P\subset A$ de représentants des classes d'équivalence d'éléments irréducibles. Alors l'anneau A est dit* factoriel *si tout élément x s'écrit de manière unique (à l'ordre près) sous la forme $x=up_1^{\nu_1}\cdots p_r^{\nu_r}$ avec les p_i dans P et $u\in A^\times$.*

Dans un anneau factoriel, on a donc la notion de pgcd et de ppcm (définis à un inversible près ou relativement à un choix P comme ci-dessus) et la notion d'éléments *premiers entre eux.*

Par ce que l'on vient de dire, $\mathbb{Z}[i]$ est factoriel. Il est donc naturel de chercher à déterminer ses éléments inversibles et ses éléments irréductibles. Pour les premiers, on vérifie facilement que $\mathbb{Z}[i]^\times=\{z\in\mathbb{Z}[i],z\bar{z}=1\}=\{\pm1,\pm i\}$. Pour déterminer les irréductibles, on peut d'abord se demander quels nombres premiers p restent irréductibles dans $\mathbb{Z}[i]$. Remarquons que si $z|p$ alors $z\bar{z}|p^2$ donc $z\bar{z}=1,p$ ou p^2. Mais pour que z soit un diviseur "propre" (au sens où ni z ni p/z n'est inversible) il nous faut $z\bar{z}=p$. En écrivant $z=a+ib$ il vient $p=a^2+b^2$. Réciproquement, si $p=a^2+b^2$, on a une factorisation $p=(a+ib)(a-ib)$ dans laquelle on remarque que $z:=a+ib$ est nécessairement irréductible (car $z\bar{z}$ est premier). On voit ainsi que

i) un premier p reste irréductible dans $\mathbb{Z}[i]$ si et seulement si p n'est pas somme de deux carrés.

ii) un élément irréductible de $\mathbb{Z}[i]$ est de la forme up avec $u \in \mathbb{Z}[i]^\times$ et p premier comme au i), ou de la forme $a+ib$ avec a^2+b^2 premier.

A titre d'exemple, on a la factorisation $2 = i(1-i)^2$ dans laquelle i est un inversible et $1-i$ est un irréductible.

Intéressons-nous maintenant à l'équation $x^2+1 = y^3$ qui se factorise en $(x+i)(x-i) = y^3$ dans $\mathbb{Z}[i]$. Calculons le pgcd de $x+i$ et $x-i$ dans $\mathbb{Z}[i]$ (cela a un sens car $\mathbb{Z}[i]$ est factoriel). Celui-ci divise $2i = (i+1)^2$. Mais si $1+i$ divise $x+i$, alors $1-i$ divise $x-i$, donc 2 divise x^2+1. Or, en regardant modulo 4, on observe que x doit être pair (sinon $x^2+1 \equiv 2[4]$, mais 2 n'est pas un cube modulo 4). Il s'ensuit donc que $x+i$ et $x-i$ sont *premiers entre eux*, et par conséquent de la forme uz^3 avec u inversible et $z \in \mathbb{Z}[i]$. Comme, de plus, les inversibles de $\mathbb{Z}[i]$ sont tous des cubes, on obtient l'existence de $a, b \in \mathbb{Z}$ tels que $x+i = (a+ib)^3$. En regardant le coefficient de i dans cette égalité, on obtient la contrainte $b(3a^2-b^2) = 1$, ce qui ne laisse d'autre possibilité que $(a,b) = (0,-1)$, correspondant à l'unique solution $(x,y) = (0,1)$.

Exemple. – L'anneau $\mathbb{Z}[\sqrt{-2}]$ et l'équation $x^2+2 = y^3$. Le nombre $\sqrt{-2} := i\sqrt{2}$, qui est annulé par X^2+2, est un entier algébrique. L'anneau engendré s'écrit $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z} \oplus i\sqrt{2}\mathbb{Z}$ (vérifier que c'est bien un sous-anneau !). Dans cet anneau, on peut factoriser $x^2+2 = (x+\sqrt{-2})(x-\sqrt{-2})$ pour tout $x \in \mathbb{Z}[\sqrt{-2}]$. Il se trouve que le même raisonnement que pour $\mathbb{Z}[i]$ montre que $\mathbb{Z}[\sqrt{-2}]$ est aussi euclidien. Cela tient au fait que le rectangle défini par les inégalités $|\Re(z)| \leqslant \frac{1}{2}$ et $|\Im(z)| \leqslant \frac{\sqrt{2}}{2}$ est encore contenu dans le disque $\{z, |z| < 1\}$. En conséquence, $\mathbb{Z}[\sqrt{-2}]$ est aussi *factoriel*.

Appliquons ceci à la résolution de l'équation $x^2+2 = y^3$ dans $\mathbb{Z}^2$. Tout d'abord, on peut remarquer en raisonnant modulo 4 que x ne peut pas être pair. Supposons donc x impair ; on remarque alors que les éléments $x+\sqrt{-2}$ et $x-\sqrt{-2}$ de $\mathbb{Z}[\sqrt{-2}]$ doivent être premiers entre eux. En effet, un élément irréductible qui diviserait chacun devrait diviser $2\sqrt{-2} = -\sqrt{-2}^3$ donc être égal à $\pm\sqrt{-2}$ (qui est bien irréductible), mais $\pm\sqrt{-2}$ ne divise pas x qui est impair. Il découle alors de la propriété d'unique factorisation que $x+\sqrt{-2}$ et $x-\sqrt{-2}$ sont respectivement de la forme $u\alpha^3$ et $u^{-1}\bar{\alpha}^3$ (conjugué complexe) pour un inversible $u \in \mathbb{Z}[\sqrt{-2}]^\times$ et un élément $\alpha \in \mathbb{Z}[\sqrt{-2}]$. En fait, on vérifie (exercice) que $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$, donc $x+\sqrt{-2}$ et $x-\sqrt{-2}$ doivent être des cubes parfaits dans $\mathbb{Z}[\sqrt{-5}]$. Or un cube s'écrit $(a+b\sqrt{-2})^3 = (a^3-6ab^2) + (3a^2b-2b^3)\sqrt{-2}$, et on vérifie de manière élémentaire que $3a^2b-2b^3 = 1 \Leftrightarrow (a,b) = (\pm 1, 1)$ tandis que $3a^2b-2b^3 = -1 \Leftrightarrow (a,b) = (\pm 1, -1)$. De là il découle que les seuls x possibles sont $x = \pm 5$, puis que les solutions de l'équation de départ sont $(x,y) = (\pm 5, 3)$.

Exemple. – L'anneau $\mathbb{Z}[\sqrt{-3}]$ et l'équation $x^2+3 = y^3$. Essayons la même stratégie avec 3 à la place de 2. On considère donc l'anneau $\mathbb{Z}[\sqrt{-3}] = \mathbb{Z} \oplus i\sqrt{3}\mathbb{Z}$ dans lequel on peut factoriser $x^2+3 = (x+\sqrt{-3})(x-\sqrt{-3})$ pour tout $x \in \mathbb{Z}[\sqrt{-3}]$. Malheureusement,

cet anneau n'est pas factoriel [2]. En effet, regardons l'égalité

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

L'élément 2 est irréductible car si on écrit $2 = xy$ avec $x, y \in \mathbb{Z}[\sqrt{-3}]$, on a $4 = x\bar{x}y\bar{y}$ donc $x\bar{x}$, qui est entier positif, vaut 1, 2 ou 4, mais il ne peut pas valoir 2 car l'équation $u^2 + 3v^2 = 2$ n'a pas de solution dans $\mathbb{Z}^2$, donc on a soit $x\bar{x} = 1$ auquel cas $x = \pm 1$, soit $y\bar{y} = 1$ auquel cas $y = \pm 1$. Pour la même raison, les éléments $1 + \sqrt{-3}$ et $1 - \sqrt{-3}$ sont irréductibles. Comme $\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}$, ces trois éléments sont non équivalents 2 à 2, et l'égalité ci-dessus montre que la propriété d'unique factorisation n'est pas vérifiée dans $\mathbb{Z}[\sqrt{-3}]$.

En fait, cet anneau est encore "pire" que non factoriel : il n'est pas *intégralement clos* non plus. Cela signifie (on y reviendra) que son corps des fractions, qui n'est autre que le sous-corps $\mathbb{Q}[\sqrt{-3}]$ de $\mathbb{C}$ engendré par $\sqrt{-3}$, contient des entiers algébriques qui ne sont pas dans cet anneau. Un exemple est $j := \frac{-1+\sqrt{-3}}{2}$, qui est bien entier algébrique, puisque racine du polynôme $X^3 - 1$, et plus précisément du polynôme irréductible $X^2 + X + 1$.

Il se trouve que l'anneau $\mathbb{Z}[j]$, qui contient $\mathbb{Z}[\sqrt{-3}]$, est bien meilleur que ce dernier ; en effet une légère adaptation de l'argument déjà utilisé montre qu'il est euclidien [3]. Noter que l'égalité $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ ne contredit pas l'unicité des factorisations dans $\mathbb{Z}[j]$ puisque 2, $1 + \sqrt{-3}$ et $1 - \sqrt{-3}$ sont des éléments irréductibles *équivalents* en vertu des égalités $2 = -j(1+\sqrt{-3}) = -j^{-1}(1-\sqrt{-3})$ et du fait que $j \in \mathbb{Z}[j]^\times$. D'ailleurs, il sera utile de remarquer que $\mathbb{Z}[j]^\times = \mu_6 = \{\pm 1, \pm j, \pm\bar{j}\}$.

Puisque la factorisation $x^2 + 3 = (x + \sqrt{-3})(x - \sqrt{-3})$ vit dans $\mathbb{Z}[j]$, on peut l'utiliser pour étudier l'équation $x^2 + 3 = y^3$. Remarquons que pour une éventuelle solution (x, y) on aura $x \neq 0$. Les éléments $x + \sqrt{-3}$ et $x - \sqrt{-3}$ sont donc premiers entre eux. En effet, un diviseur commun diviserait aussi $2\sqrt{-3}$. Or 2 et $\sqrt{-3}$ sont irréductibles et ne divisent visiblement pas $x \pm \sqrt{-3}$ si $x \neq 0$. Grâce à la propriété d'unique factorisation, on peut donc écrire $x + \sqrt{-3}$ sous la forme

$$x + \sqrt{-3} = u(a + b\sqrt{-3})^3 = u((a^3 - 9ab^2) + (3a^2b - 3b^3)\sqrt{-3})$$

avec $u \in \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$. On voit toute de suite, en comparant les termes en $\sqrt{-3}$, qu'il n'y a pas de possibilité avec $u = \pm 1$. Avec $u = \frac{1+\sqrt{-3}}{2}$, on obtient la contrainte

$$a^3 - 9ab^2 + 3a^2b - 3b^3 = 2.$$

Avec "un peu" d'astuce on remarque la congruence modulo 4

$$a^3 - 9ab^2 + 3a^2b - 3b^3 \equiv a^3 + 3ab^2 + 3a^2b + b^3 \equiv (a + b)^3 (\mathrm{mod} 4).$$

2. On remarquera d'ailleurs que le rectangle défini par les inégalités $|\Re(z)| \leqslant \frac{1}{2}$ et $|\Im(z)| \leqslant \frac{\sqrt{3}}{2}$ n'est plus contenu dans le disque $\{z, |z| < 1\}$.

3. On pourra remarquer que les seuls éléments du rectangle défini par les inégalités $|\Re(z)| \leqslant \frac{1}{2}$ et $|\Im(z)| \leqslant \frac{\sqrt{3}}{2}$ hors du disque $\{z, |z| < 1\}$ sont justement $\pm j, \pm j^2$.

Or 2 n'est pas un cube dans $\mathbb{Z}/4\mathbb{Z}$, donc la contrainte ci-dessus est impossible. Un argument similaire pour les autres u nous mène à la conclusion que l'équation $x^2+3=y^3$ n'a pas de solution (le vérifier).

Exemple. – L'anneau $\mathbb{Z}[\sqrt{-5}]$ et l'équation $x^2+5=y^3$. Remplaçons maintenant 3 par 5 et considérons donc l'anneau $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus i\sqrt{5}\mathbb{Z}$ dans lequel on peut factoriser $x^2+5 = (x+\sqrt{-5})(x-\sqrt{-5})$ pour tout $x \in \mathbb{Z}[\sqrt{-5}]$. À nouveau, cet anneau n'est pas factoriel, comme le montre par exemple l'égalité

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

(Exercice : vérifier que 2, 3, $1+\sqrt{-5}$ et $1-\sqrt{-5}$ sont des élements irréductibles non équivalents de $\mathbb{Z}[\sqrt{-5}]$). Mais cette fois-ci c'est plus grave : $\mathbb{Z}[\sqrt{-5}]$ est tout de même intégralement clos, donc on ne peut pas l'agrandir un peu pour le rendre factoriel, comme on l'a fait pour $\mathbb{Z}[\sqrt{-3}]$.

C'est pour pallier les difficultés liées au défaut d'unicité des factorisations que Dedekind a dégagé la notion d'*idéal* d'un anneau.

1.2.1 *Idéaux.* Rappelons qu'un idéal I de A est un sous-groupe additif de A stable par multiplication par A. Si $a_1, \cdots, a_n$ sont des éléments de A, on note $(a_1, \cdots, a_n)$ l'idéal *engendré* par ces éléments, *i.e.* le plus petit idéal qui les contient. On a donc

$$(a_1, \cdots, a_n) = (a_1) + \cdots + (a_n) = Aa_1 + \cdots + Aa_n$$

où l'on utilise la notation "somme" pour deux sous-ensembles S_1, S_2 de A :

$$S_1 + S_2 = \{x \in A, \exists (s_1, s_2) \in S_1 \times S_2,\ x = s_1 + s_2\}.$$

Un idéal engendré par une famille finie comme ci-dessus est dit *de type fini*. Il est dit *principal* s'il est engendré par un seul élément.

Les idéaux de A peuvent être "additionnés" et "multipliés". L'addition est simplement donnée par la somme ensembliste ci-dessus :

$$I + J = \{x \in A,\ \exists (i,j) \in I \times J,\ x = i + j\}.$$

Le produit d'idéaux est plus subtil : si on multiplie naïvement les ensembles I et J, l'ensemble obtenu est certes stable par multiplication par A, mais pas par addition. Il convient de prendre l'idéal engendré par ce produit naïf. Explicitement, on a

$$I \cdot J := \{x \in A, \exists n \in \mathbb{N}, \exists (i_1, \cdots, i_n, j_1, \cdots, j_n) \in I^n \times J^n,\ x = i_1 j_1 + \cdots i_n j_n\}.$$

La découverte de Dedekind est que, pour un anneau de nombres intégralement clos comme $\mathbb{Z}[\sqrt{-5}]$ par exemple, les idéaux propres non nuls admettent une factorisation "unique", même si l'anneau n'est pas factoriel. Evidemment cela suppose d'avoir un analogue pour les idéaux de la notion d'élément irréductible. C'est la notion d'idéal *premier*.

DÉFINITION. – *On dit que l'idéal $I \neq A$ est premier si pour tout $x, y \in A$, on a $xy \in I \Rightarrow x \in I$ ou $y \in I$.*

Il découle de cette définition que pour $a \in A$ non nul, si l'idéal (a) est premier alors a est irréductible. La réciproque n'est pas toujours vraie. En fait, elle est équivalente au lemme d'Euclide, dont on a vu qu'il n'est pas vrai dans $\mathbb{Z}[\sqrt{-5}]$. Concrètement, si $x = 1 + \sqrt{-5}$ et $y = 1 - \sqrt{-5}$, on a $xy \in (2)$ mais ni x ni y n'appartient à (2) donc l'idéal (2) n'est pas premier bien que 2 soit irréductible.

THÉORÈME. (Dedekind) – *Dans l'anneau $\mathbb{Z}[\sqrt{-5}]$ (ou dans tout autre anneau d'entiers algébriques intégralement clos), tout idéal propre non nul I s'écrit de manière "unique à l'ordre près" $I = \mathfrak{p}_1^{\nu_1} \cdot \mathfrak{p}_2^{\nu_2} \cdots \mathfrak{p}_r^{\nu_r}$ pour des idéaux premiers $\mathfrak{p}_i$ distincts 2 à 2.*

Par exemple on a les égalités d'idéaux suivantes :

$$\begin{aligned}
(2) &= (2, 1+\sqrt{-5}) \cdot (2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5})^2 \\
(3) &= (3, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5}) \\
(1+\sqrt{-5}) &= (2, 1+\sqrt{-5}) \cdot (3, 1+\sqrt{-5}) \\
(1-\sqrt{-5}) &= (2, 1-\sqrt{-5}) \cdot (3, 1-\sqrt{-5}).
\end{aligned}$$

Expliquons par exemple la première ligne. Tout d'abord il est clair que $(2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5})$, puisque $1 - \sqrt{-5} = 2 - (1 + \sqrt{-5})$. En remarquant que $(\alpha, \beta) \cdot (\alpha', \beta') = (\alpha\alpha', \alpha\beta', \beta\alpha', \beta\beta')$, on voit que $(2, 1+\sqrt{-5})^2 = (4, 2+2\sqrt{-5}, -4-2\sqrt{-5})$. En particulier cet idéal est engendré par des multiples de 2, donc est contenu dans (2). De plus il contient l'élément $2 = 4 + (2 + 2\sqrt{-5}) - 4 - 2\sqrt{-5})$, donc contient l'idéal (2), et lui est finalement égal. On raisonne de même pour les autres égalités. On peut démontrer que les idéaux $\mathfrak{p}_1 := (2, 1+\sqrt{-5})$, $\mathfrak{p}_2 := (3, 1+\sqrt{-5})$ et $\mathfrak{p}_3 := (3, 1-\sqrt{-5})$ sont premiers, et on voit que l'égalité $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ qui nous posait problème, devient $\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_1\mathfrak{p}_3$ dans le monde des idéaux, ce qui est conforme à la propriété d'unique factorisation pour les idéaux.

Exercice : vérifier que les idéaux $\mathfrak{p}_i$ ci-dessus sont bien premiers (ce sera plus facile quand on aura avancé dans la théorie) et ne sont pas principaux.

Revenons à l'équation $x^2 + 5 = y^3$ que l'on factorise en $y^3 = (x + \sqrt{-5})(x - \sqrt{-5})$ dans l'anneau $\mathbb{Z}[\sqrt{-5}]$. On aimerait prouver que $x + \sqrt{-5}$ est nécessairement de la forme $u \cdot \alpha^3$, mais l'absence d'unicité des factorisations ne permet pas de conclure comme précédemment. Par exemple, l'égalité $6^3 = 2(1 + \sqrt{-5})^2 \times 3(1 - \sqrt{-5})^2$ montre qu'un cube peut être le produit de deux éléments sans diviseur commun mais qui ne sont pas eux-mêmes des cubes.

Cependant, le théorème de Dedekind nous assure tout de même que *l'idéal engendré par $x + \sqrt{-5}$* est de la forme $(x + \sqrt{-5}) = I^3$ pour un idéal non nul de $\mathbb{Z}[\sqrt{-5}]$, *à condition* de voir que les idéaux $(x + \sqrt{-5})$ et $(x - \sqrt{-5})$ n'ont pas de diviseur premier $\mathfrak{p}$ commun, c'est-à-dire qu'il n'y a pas d'idéal premier $\mathfrak{p}$ qui les contienne tous les deux. En effet un tel $\mathfrak{p}$ devrait contenir $2\sqrt{-5}$, donc contenir 2, auquel cas $\mathfrak{p} = (2, 1+\sqrt{-5})$, ou $\sqrt{-5}$, auquel cas $\mathfrak{p} = (\sqrt{-5})$ (vérifier que ce dernier est bien premier). Or, puisque $x \neq 0$, $\sqrt{-5}$ ne divise pas $x + \sqrt{-5}$ donc $(\sqrt{-5})$ ne contient pas $(x + \sqrt{-5})$. De plus, si $(2, 1+\sqrt{-5})$ contient

$(x + \sqrt{-5})$ alors 2 divise y, donc x est impair, ce qui est impossible car on obtiendrait modulo 4 l'égalité $1 + 5 = 0$.

Maintenant que l'on sait que $(x+\sqrt{-5})$ est de la forme I^3 (égalité d'idéaux), on aimerait en tirer que $x+\sqrt{-5}$ est de la forme $u(a+b\sqrt{-5})^3$ (égalité de nombres). Pour cela, il suffirait de prouver que I est *principal* (engendré par un élément). Mais on a vu que c'est loin d'être automatique.

Remarque culturelle "hors programme" : ici intervient un invariant très important de la théorie des anneaux de nombres, appelé *groupe de classes*, qui mesure le "défaut" de principalité (et donc de "factorialité") d'un anneau d'entiers algébriques. Soit $\mathrm{Id}(A)$ l'ensemble des idéaux non nuls de A. Le produit d'idéaux en fait un monoïde commutatif d'élément neutre l'idéal unité A. Soit $\mathrm{Id.Pr}(A)$ le sous-ensemble des idéaux principaux. Il est stable par produit, donc c'est un sous-monoïde. Considérons le monoïde quotient

$$\mathrm{Cl}(A) := \mathrm{Id}(A)/\mathrm{Id.Pr}(A).$$

Ensemblistement, c'est le quotient de $\mathrm{Id}(A)$ par la relation d'équivalence définie par $I \sim I' \Leftrightarrow (\exists a, a' \in A \setminus \{0\},\ Ia = I'a')$. Le théorème de Dedekind implique que ce monoïde quotient est en fait un *groupe* abélien : en effet, il suffit de vérifier que l'image de tout $\mathfrak{p}$ premier non nul y admet un inverse, or, si $a \in \mathfrak{p} \setminus \{0\}$, et si on écrit $(a) = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$, alors $\mathfrak{p}$ est l'un des $\mathfrak{p}_i$, disons $\mathfrak{p}_1$, et on a donc $\mathfrak{pq} = (a)$ avec $\mathfrak{q} := \mathfrak{p}_1^{v_1-1} \cdots \mathfrak{p}_r^{v_r}$, de sorte que $\mathfrak{q}$ est inverse de $\mathfrak{p}$ dans le quotient $\mathrm{Cl}(A)$. Remarquons que, par définition, un idéal I est principal si et seulement si son image dans $\mathrm{Cl}(A)$ est 0.

Le théorème suivant est un pilier de la théorie algébrique des nombres, qui dépasse le cadre de ce cours, mais sera certainement abordé dans tout cours de "théorie des nombres" de niveau M1.

THÉORÈME. – *Le groupe de classes d'un anneau d'entiers algébriques est fini.*

La preuve classique de ce théorème donne en fait un majorant qu'il est parfois raisonnable d'expliciter. Par exemple dans le cas qui nous intéresse, il n'est pas très dur d'en tirer que $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$.

Montrons comment cela suffit pour résoudre notre équation. L'idéal I^3 est principal, donc sa classe dans $\mathcal{C}\ell(A)$ est nulle. Mais celle-ci est 3 fois celle de I. Or la multiplication par 3 est inversible dans $\mathbb{Z}/2\mathbb{Z}$ (c'est même l'identité), donc la classe de I est nulle aussi, et I est principal. Il s'ensuit que $I = (\alpha)$ pour un $\alpha \in \mathbb{Z}[\sqrt{-5}]$, donc $(x + \sqrt{-5}) = (\alpha^3)$ et on en déduit finalement que $x+\sqrt{-5}$ est bien de la forme $u \cdot \alpha^3$ comme souhaité. À partir de là, le même genre de raisonnement élémentaire que dans le cas de l'équation $x^2 + 3 = y^3$ montre que l'équation $x^2 + 5 = y^3$ n'a pas de solution.

Une autre source de motivation pour la théorie des anneaux est la *géométrie algébrique.*

1.3 Anneaux de la géométrie algébrique classique

La géométrie algébrique "classique", développée notamment par Hilbert puis par l'école italienne au début du XXème siècle, étudie les sous-ensemble de $\mathbb{C}^n$ définis par des équations polynômiales (ainsi que leurs variantes projectives dont nous ne parlerons pas ici). Un tel ensemble est donc défini par une famille de polynômes à n variables $f_1, \cdots, f_r \in$

$\mathbb{C}[X_1, \cdots, X_n]$ comme suit :

$$V(f_1, \cdots, f_r) := \{(z_1, \cdots, z_n) \in \mathbb{C}^n,\ f_1(z, \cdots, z_n) = \cdots = f_r(z_1, \cdots, z_n) = 0\}.$$

Un tel sous-ensemble sera appelé "sous-ensemble algébrique" ou "fermé de Zariski" de $\mathbb{C}^n$. On aimerait étudier ce genre d'ensembles de manière *intrinsèque*, c'est-à-dire de manière indépendante des donnée "auxiliaires" utilisées pour le définir, à savoir n et les polynômes f_i. Par exemple, on aimerait pouvoir identifier la courbe plane d'équation $X^3 - Y^2 = 0$ dans $\mathbb{C}^2$ avec l'ensemble algébrique de $\mathbb{C}^3$ défini par les équations $f_1 = X^3 - Z$ et $f_2 = Y^2 - Z$, comme l'intuition nous le dicte. Pour cela, il faut une notion d'*isomorphisme*, et pour commencer, une notion de *morphisme* entre ensembles algébriques. La notion naturelle est celle d'*application polynômiale*.

DÉFINITION. – *Soient $V \subset \mathbb{C}^n$ et $V' \subset \mathbb{C}^{n'}$ deux sous-ensembles algébriques. Une application $\varphi : V \longrightarrow V'$ est dite* polynômiale *si elle est la restriction d'une application polynômiale $\tilde{\varphi} : \mathbb{C}^n \longrightarrow \mathbb{C}^{n'}$, c'est-à-dire de la forme*

$$(z_1, \cdots, z_n) \in \mathbb{C}^n \mapsto (f_1(z_1, \cdots, z_n), \cdots, f_{n'}(z_1, \cdots, z_n)) \in \mathbb{C}^{n'}$$

pour des polynômes $f_1, \cdots, f_{n'} \in \mathbb{C}[X_1, \cdots, X_n]$..

Cas particulier : une *fonction polynômiale* sur V est une application polynômiale $V \longrightarrow \mathbb{C}$ en le sens précédent. L'ensemble $\mathcal{O}(V)$ des fonctions polynômiales sur V est manifestement une $\mathbb{C}$-algèbre (via l'addition et la multiplication point par point des fonctions). Si $\varphi : V \longrightarrow V'$ est une application polynômiale, il découle de ces définitions que la composition des fonctions $f' \mapsto f' \circ \varphi$ induit un morphisme de $\mathbb{C}$-algèbres

$$\varphi^* :\ \mathcal{O}(V') \longrightarrow \mathcal{O}(V),\ \ f' \mapsto f' \circ \varphi.$$

Nous expliquerons plus tard le résultat remarquable suivant :

THÉORÈME. – *L'application $\varphi \mapsto \varphi^*$ induit une bijection entre l'ensemble des applications polynômiales $V \longrightarrow V'$ et l'ensemble des morphismes de $\mathbb{C}$-algèbres $\mathcal{O}(V') \longrightarrow \mathcal{O}(V)$.*

Ceci signifie qu'étudier les ensembles algébriques et les applications polynômiales entre eux revient à étudier *certaines* $\mathbb{C}$-algèbres et les homomorphismes d'algèbres entre elles. C'est pourquoi l'algèbre commutative joue un rôle prépondérant en géométrie algébrique.

On peut se demander quelles algèbres sont des algèbres de fonctions polynômiales sur un ensemble algébrique. Par définition on a $\mathcal{O}(\mathbb{C}^n) = \mathbb{C}[X_1, \cdots, X_n]$. Toujours par définition, pour $V \subset \mathbb{C}^n$, l'application de restriction des fonctions

$$\mathcal{O}(\mathbb{C}^n) = \mathbb{C}[X_1, \cdots, X_n] \longrightarrow \mathcal{O}(V), f \mapsto f_{|V}$$

est surjective. Ceci montre que $\mathcal{O}(V)$ est une $\mathbb{C}$-algèbre *de type fini*, c'est-à-dire engendrée par un nombre fini d'éléments. De plus, elle possède la propriété d'être *réduite*, au sens où pour $f \in \mathcal{O}(V)$ et $k \in \mathbb{N}^*$, $f^k = 0 \Rightarrow f = 0$.

Réciproquement, soit A une $\mathbb{C}$-algèbre de type fini réduite. Si on choisit des générateurs $x_1, \cdots, x_n$ de A, on obtient un morphisme surjectif de $\mathbb{C}$-algèbres

$$\mathbb{C}[X_1, \cdots, X_n] \longrightarrow A,\ X_i \mapsto x_i.$$

Soit I le noyau de ce morphisme. C'est un idéal de $\mathbb{C}[X_1, \cdots, X_n]$. Nous démontrerons le théorème suivant, dû à Hilbert.

THÉORÈME. – *L'idéal I est engendré par un nombre fini de fonctions, disons $f_1, \cdots, f_r$. Ces fonctions définissent un sous-ensemble algébrique $V = V(f_1, \cdots, f_r)$. Le noyau de l'application de restriction $\mathcal{O}(\mathbb{C}^n) \longrightarrow \mathcal{O}(V)$ est justement I, de sorte que $\mathcal{O}(V) = A$.*

Ainsi l'objet intrinsèque sous-jacent d'un ensemble algébrique V est son algèbre de fonctions polynômiales $\mathcal{O}(V)$. Et se donner V comme sous-ensemble algébrique d'un $\mathbb{C}^n$ revient à se donner une surjection $\mathbb{C}[X_1, \cdots, X_n] \longrightarrow \mathcal{O}(V)$.

Pour illustrer les liens entre V et $\mathcal{O}(V)$, voici comment retrouver les points de V à partir de $\mathcal{O}(V)$. On remarque d'abord que pour tout sous-ensemble $E \subset V$, l'ensemble I_E des fonctions polynômiales $f \in \mathcal{O}(V)$ qui s'annulent en tout point $x \in E$ est un *idéal* de $\mathcal{O}(V)$ (le vérifier). Inversement, on peut associer à tout idéal I de $\mathcal{O}(V)$ le lieu E_I des points $x \in V$ qui annulent toutes les fonctions dans I. Remarquer qu'il n'est pas clair que ce lieu soit non vide. Nous démontrerons néanmoins le célèbre Nullstellensatz de Hilbert :

THÉORÈME. – *Les application $E \mapsto I_E$ et $I \mapsto E_I$ induisent des bijections réciproques entre l'ensemble des singletons de V (qu'on identifie évidemment à V) et l'ensemble des idéaux maximaux de $\mathcal{O}(V)$.*

Signalons enfin que les propriétés géométriques de V peuvent se lire sur son algèbre de fonctions : ses espaces tangents, sa dimension, ses composantes connexes, est-ce une variété lisse (au sens de la géométrie différentielle) ou non, etc. À titre d'exemple, la courbe plane d'équation $Y^2 = X^3$ n'est pas une variété lisse car elle a une singularité en 0 (dessiner les points réels). La contrepartie est que l'anneau $\mathcal{O}(V)$ n'est pas intégralement clos. Par contre toute courbe dont l'anneau de fonctions polynômiales est intégralement clos est une variété lisse.

1.3.1 *La géométrie algébrique moderne.* La dualité entre sous-ensembles algébriques de $\mathbb{C}^n$ et $\mathbb{C}$-algèbres réduites de type fini est un prémice d'une vaste refondation de la géométrie algébrique opérée par Grothendieck et ses élèves à partir des années 1960. Dans leur langage, *tout anneau* est l'anneau des fonctions d'un objet géométrique appelé *schéma*. Le schéma associé à un anneau A est un espace topologique appelé *spectre de A*. C'est l'ensemble des idéaux premiers de A muni de la *topologie de Zariski*. En particulier chaque anneau de la théorie des nombres, comme $\mathbb{Z}[\sqrt{-5}]$ par exemple, définit un schéma, et le langage de Grothendieck fournit un cadre commun à la théorie des nombres algébrique et à la géométrie algébrique. La théorie des schémas va au-delà du contenu de ce cours, mais ce cours fournit les fondements d'algèbre commutative nécessaires pour cette théorie.

2 Définitions de base, rappels et compléments

2.1 Généralités sur les anneaux commutatifs

Ici tous les anneaux seront supposés commutatifs, sauf mention du contraire.

2.1.1 *L'anneau nul.* Pour un anneau (unitaire) $(A, +, \cdot)$, l'axiome de distributivité implique que pour tout a on a $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$, donc $a \cdot 0 = 0$. Il s'ensuit que si on a $0 = 1$ (ce que nous n'avons pas exclu), alors $A = \{0\}$. On peut bien-sûr exclure ce cas pathologique, mais il sera pratique de ne pas l'exclure lorsqu'on parlera de quotients.

2.1.2 *Sous-anneau.* Un sous-ensemble B d'un anneau A est appelé *sous-anneau* s'il est non vide, stable par soustraction, par multiplication, *et contient* 1.

2.1.3 *Diviseurs de zéro, éléments réguliers, anneaux intègres.* Un élément *a non nul* d'un anneau est appelé *diviseur de* 0 s'il existe a' *non nul* tel que $aa' = 0$. Un élément *a non nul* et non diviseur de zéro est dit *régulier*. Un anneau *intègre* est un anneau sans diviseur de zéro, c'est-à-dire tel que $ab = 0 \Rightarrow a = 0$ ou $b = 0$. Dans un anneau intègre, on peut simplifier les égalités :

$$a \neq 0 \text{ et } ab = ac \Rightarrow b = c,$$

même si a n'admet pas d'inverse.

Exemple. – Il est clair qu'un sous-anneau d'un anneau intègre est intègre. Par ailleurs, tout corps est évidemment un anneau intègre. Il s'ensuit que les anneaux d'entiers algébriques sont toujours intègres.

Exemple. – Considérons le sous-ensemble algébrique V d'équation $X_1X_2 = 0$ dans $\mathbb{C}^2$. C'est la réunion des deux axes $X_1 = 0$ et $X_2 = 0$. La fonction polynômiale $X_1 : \mathbb{C}^2 \longrightarrow \mathbb{C}, (z_1, z_2) \mapsto z_1$ induit une fonction polynômiale x_1 sur V visiblement non nulle. De même, X_2 induit une fonction non nulle x_2 sur V. Mais par définition de V, la fonction x_1x_2 y est partout nulle. Ainsi, x_1 et x_2 sont des diviseurs de zéro dans l'anneau $\mathcal{O}(V)$, qui n'est donc pas intègre.

Exercice. – Pour quels $N > 0$ l'anneau $\mathbb{Z}/N\mathbb{Z}$ est-il intègre ?

Exercice. – Soit K un corps. Montrer qu'une K-algèbre A (commutative) de dimension finie intègre est un corps. Considérer la multiplication par $a \neq 0$ dans A comme un endomorphisme K-linéaire de A.

2.1.4 *Éléments nilpotents, anneaux réduits.* Un élément $x \in A$ est dit nilpotent s'il existe un entier $k \in \mathbb{N}$ tel que $x^k = 0$. En particulier, si x est nilpotent et non nul, il est diviseur de zéro. On appelle *ordre de nilpotence* de x le plus petit entier k tel que $x^k = 0$. Un anneau est dit *réduit* s'il ne possède pas d'élément nilpotent non nul. Ainsi, pour un anneau, on a *intègre* $\Rightarrow$ *réduit.*

Exemple. – Regardons le cas $\mathbb{Z}/N\mathbb{Z}$. Si N est de la forme $N = p^\nu$ pour un nombre

premier p et un entier $\nu > 0$, on a par définition que p est nilpotent d'ordre ν dans $\mathbb{Z}/N\mathbb{Z}$. On constate alors que

— si $\nu = 1$, $\mathbb{Z}/p^\nu\mathbb{Z}$ est un corps (donc intègre et réduit).

— si $\nu > 1$, $\mathbb{Z}/p^\nu\mathbb{Z}$ n'est pas réduit et l'ensemble de ses éléments nilpotents est $p\mathbb{Z}/p^\nu\mathbb{Z}$.

Plus généralement, en factorisant $N = \prod_p p^{\nu_p(N)}$ et en utilisant le théorème des restes chinois rappelé ci-dessous, on voit que $\mathbb{Z}/N\mathbb{Z}$ est réduit si et seulement si N ne possède aucun facteur carré, c'est-à-dire si $\nu_p(N) = 1$ pour tout p.

2.1.5 *Produits d'anneaux.* Soient A et A' deux anneaux. On munit le produit cartésien $A \times A'$ d'une structure d'anneau appelée *anneau produit* en posant :

$$(a, a') + (b, b') := (a + b, a' + b') \text{ et } (a, a') \cdot (b, b') = (ab, a'b').$$

L'élément neutre de l'addition est $(0, 0)$ et celui de la mutiplication est $(1, 1)$. Si les deux anneaux sont non nuls, le produit $A \times A'$ n'est pas intègre, puisque $(1, 0) \cdot (0, 1) = (0, 0)$.

Exemple. – Le théorème des restes chinois nous dit que pour $pgcd(n, m) = 1$, l'application produit

$$\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \;\; a(\mathrm{mod}\, nm) \mapsto (a(\mathrm{mod}\, n), a(\mathrm{mod}\, m))$$

identifie $\mathbb{Z}/nm\mathbb{Z}$ au produit de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.

2.1.6 *Idempotents.* Dans un anneau A, un élément e est dit *idempotent* si on a $e^2 = e$. Dans ce cas, le sous-ensemble eAe hérite d'une structure d'anneau dont l'addition et la multiplication sont induites par celles de A, et l'élément neutre pour la multiplication est e.

Remarque. – *eAe n'est pas* un sous-anneau de A, car il n'a pas le même élément neutre pour la multiplication (sauf si $e = 1$).

Lorsque A est commutatif (ou plus généralement lorsque e est *central*, i.e. commute à tous les éléments de A) on a simplement $eAe = Ae$.

L'élément $1 - e$ est aussi un idempotent de A et on a une décomposition en somme directe d'idéaux $A = Ae \oplus A(1 - e)$ (noter que la multiplication par e est un *projecteur* comme on en rencontre en algèbre linéaire). Cette décomposition identifie A au *produit* des anneaux Ae et $A(1 - e)$. Plus précisément, l'application

$$A \longrightarrow Ae \times A(1 - e),\ a \mapsto (ae, a(1 - e))$$

est un isomorphisme d'anneaux, au sens rappelé ci-dessous. Son inverse est $(x, y) \mapsto x + y$.

Exemple. – Soient n et m entiers et premiers entre eux. Choisissons $u, v \in \mathbb{Z}$ tels que $un + vm = 1$. En multipliant cette égalité par un, on voit que $(un)^2 \equiv un(\mathrm{mod}\, nm)$. Donc l'image e de un dans $\mathbb{Z}/nm\mathbb{Z}$ est un idempotent. De plus on a $(\mathbb{Z}/nm\mathbb{Z})e = n\mathbb{Z}/nm\mathbb{Z}$ qui est isomorphe (au sens ci-dessous) à $\mathbb{Z}/m\mathbb{Z}$, et de même $(\mathbb{Z}/nm\mathbb{Z})(1 - e) = m\mathbb{Z}/nm\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. On retrouve ainsi le théorème des restes chinois $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Remarque. (interprétation géométrique) – Nous verrons plus tard qu'un sous-ensemble algébrique V est *connexe* si et seulement si les seuls idempotents de son algèbre de fonctions $\mathcal{O}(V)$ sont 0 et 1. Plus généralement, les *composantes connexes* d'un sous-ensemble algébrique sont en bijection avec les *idempotents primitifs* de son algèbre $\mathcal{O}(V)$. Un idempotent est dit *primitif* si on ne peut pas le raffiner en somme de deux idempotents non nuls.

2.1.7 *(Homo)morphismes.* Un morphisme d'anneaux est une application $\varphi : A \longrightarrow A'$ qui respecte la structure d'anneaux au sens où :
— $\forall a, a' \in A$, $\varphi(a + a') = \varphi(a) + \varphi(a')$ et $\varphi(aa') = \varphi(a)\varphi(a')$.
— $\varphi(1) = 1$.
Attention, la condition $\varphi(1) = 1$ n'est pas anodine. Par exemple, l'application $\varphi : A \longrightarrow A \times A$, $a \mapsto (a, 0)$ vérifie la première propriété mais envoie 1 sur $(1, 0)$: ce n'est pas un morphisme d'anneaux. En termes d'idempotents, avec les notations du paragraphe précédent, l'inclusion de Ae dans A n'est pas un morphisme d'anneaux.

Remarque. – L'image d'un morphisme d'anneau $A \longrightarrow A'$ est un sous-anneau de A'.

Remarque. – Pour tout anneau A, il existe un unique morphisme d'anneaux $\mathbb{Z} \longrightarrow A$. Il envoie $n \in \mathbb{Z}$ sur $n \times 1$ (où $n \times -$ est la multiplication par n dans le groupe abélien A).

Comme d'habitude, un *isomorphisme* d'anneaux $\varphi : A \longrightarrow A'$ est, par définition, un morphisme qui admet un inverse à gauche et à droite, c'est-à-dire un morphisme $\psi : A' \longrightarrow A$ tel que $\varphi \circ \psi = \mathrm{id}_{A'}$ et $\psi \circ \varphi = \mathrm{id}_A$.

Lemme. – *Un morphisme est un isomorphisme si et seulement si il est bijectif en tant qu'application.*

Démonstration. Un isomorphisme est clairement bijectif. Réciproquement, supposons que φ soit bijectif ; il nous suffit de voir que la bijection réciproque φ^{-1} est un morphisme d'anneaux. C'est une vérification immédiate. □

Exercice. – Vérifier que chacune des deux projections d'un produit $A \times A'$ sur un de ses facteurs A ou A' est un morphisme d'anneaux. Si $\psi : B \longrightarrow A$ et $\psi' : B \longrightarrow A'$ sont deux morphismes d'anneaux, vérifier que

$$(\psi, \psi') : B \longrightarrow A \times A',\ b \mapsto (\psi(b), \psi'(b))$$

est un morphisme d'anneaux. Montrer que tout morphisme $\Psi : B \longrightarrow A \times A'$ est de cette forme.

Définition. – *Soit A un anneau (commutatif). Une* A-algèbre *est une paire (B, ψ) formée d'un anneau B et d'un morphisme d'anneaux $\psi : A \longrightarrow B$. Un* morphisme de A-algèbres *entre (B, ψ) et (B', ψ') est un morphisme d'anneaux $\varphi : B \longrightarrow B'$ tel que $\varphi \circ \psi = \psi'$.*

Remarque. – Cette définition généralise la notion d'algèbre sur un corps. On a parfois tendance, par abus, à oublier le ψ de la notation. Par exemple on dira simplement "soit B une $\mathbb{C}$-algèbre" plutôt que "Soit (B, ψ) une $\mathbb{C}$-algèbre".

Exemple. – Tout anneau est, de manière unique, une $\mathbb{Z}$-algèbre.

2.1.8 *Idéaux.* On a déjà rappelé ce qu'est un idéal d'un anneau A. En particulier, A est un idéal de lui-même. On dira qu'un idéal est *propre* s'il est distinct de A. Aussi, $\{0\}$ est un idéal, appelé idéal nul. La source principale d'idéaux vient du lemme suivant :

LEMME. – *Le noyau* $\mathrm{Ker}(\varphi) := \varphi^{-1}(\{0\})$ *d'un homomorphisme d'anneaux* $\varphi : A \longrightarrow A'$ *est un idéal de* A.

Démonstration. La théorie des groupes nous dit que $\mathrm{Ker}(\varphi)$ est un sous-groupe additif de A. Il reste donc à vérifier qu'il est stable par multiplication. Or, si $a \in \mathrm{Ker}(\varphi)$ et $a' \in A$, on a $\varphi(a' \cdot a) = \varphi(a') \cdot 0 = 0$, donc $a' \cdot a \in \mathrm{Ker}(\varphi)$. □

Inversement, nous verrons plus loin que tout idéal de A est le noyau d'un morphisme d'anneaux de source A, et même d'un morphisme surjectif.

Exercice. – Montrer plus généralement que l'image inverse $\varphi^{-1}(I')$, d'un idéal de A' est un idéal de A. Montrer avec un contre-exemple que l'image $\varphi(I)$ d'un idéal de A n'est pas nécessairement un idéal de A'. Montrer tout de même que *si* φ *est surjectif* alors l'image $\varphi(I)$ d'un idéal est un idéal.

Exemple. (Nilradical) – L'ensemble $\mathcal{N}(A)$ des éléments nilpotents de A est un idéal, appelé *nilradical* de A. La stabilité de $\mathcal{N}(A)$ par multiplication par A est claire puisque A est commutatif, et la stabilité de $\mathcal{N}(A)$ par addition se voit en utilisant la formule du binôme $(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}$ qui montre que si n est supérieur à la somme des ordres de nilpotence de x et y, alors $(x+y)^n = 0$.

Exercice. (radical d'un idéal) – Soit I un idéal d'un anneau de A. Posons

$$\sqrt{I} := \left\{ x \in A, \exists k \in \mathbb{N}^*, x^k \in I \right\}.$$

Montrer que $\sqrt{I}$ est un idéal contenant I (on pourra remarquer que $\sqrt{\{0\}} = \mathcal{N}(A)$ et essayer d'adapter l'argument précédent). Calculer $\sqrt{I}$ lorsque $A = \mathbb{Z}$ et $I = N\mathbb{Z}$.

Comme l'intersection de deux idéaux est encore un idéal, on peut parler du plus petit (pour l'inclusion) idéal contenant un sous ensemble E de A : c'est l'intersection de tous les idéaux contenant E. On l'appelle *idéal engendré par* E. Explicitement, c'est l'ensemble des $x \in A$ de la forme $x = a_1 e_1 + \cdots + a_r e_r$ où $r \in \mathbb{N}^*$, les e_i sont dans E, et les a_i sont dans A. Lorsque $E = \{x_1, \cdots, x_n\}$, on note aussi cet idéal

$$(x_1, \cdots, x_n) \text{ ou encore } Ax_1 + \cdots + Ax_n.$$

DÉFINITION. – *On dit d'un idéal* I *dans un anneau commutatif* A *qu'il est :*

— de type fini *s'il est engendré par une famille finie d'éléments de A.*
— principal *s'il est engendré par un seul élément (on peut aussi dire* monogène*).*
— maximal *s'il est maximal pour l'inclusion parmi les idéaux* propres *de A (*i.e. *distincts de A).*
— premier *s'il est propre et si $\forall x, y \in A$, $xy \in I \Rightarrow (x \in I$ ou $y \in I)$.*
— radiciel *s'il est propre et si $\forall x \in A$, $(\exists k \in \mathbb{N}^*, x^k \in I) \Rightarrow x \in I$.*

Il est clair que "principal" implique "de type fini". On a aussi les implications suivantes.

LEMME. – *Pour un idéal I, on a I maximal $\Rightarrow$ I premier $\Rightarrow$ I radiciel.*

Démonstration. Supposons I maximal, soient $x, y \in A$ tels que $xy \in I$, et considérons l'idéal $(x) + I$. Si c'est idéal est *propre* il est égal à I par maximalité de I et on a alors $x \in I$. S'il n'est pas propre, on a $(x) + I = A$, donc on peut écrire $1 = ax + i$ avec $i \in I$ et $a \in A$, d'où l'égalité $y = axy + iy$ qui montre que $y \in I$. On a donc montré que I est premier. L'autre implication est immédiate. □

Exemple. – Dans $\mathbb{Z}$, tout idéal est principal, donc de la forme $n\mathbb{Z}$ pour un unique $n \geqslant 0$. Un tel idéal est propre si $n \neq 1$. Dans ce cas, il est premier si et seulement si n est premier, auquel cas il est aussi maximal. Par ailleurs, il est radiciel si et seulement si n est sans facteur carré (exercice).

Exemple. – Un anneau A est intègre si et seulement si son idéal nul $I = \{0\}$ est premier.

Exemple. – Dans l'anneau $A = \mathbb{C}[X, Y]$, l'idéal (X) est premier mais non maximal, puisque contenu dans (X, Y). Ce dernier est par contre maximal. En effet, pour tout polynôme $f = f(X, Y)$, on a $f \in f(0, 0) + (X, Y)$, et donc $f(0, 0) \in (f, X, Y)$. Donc si $f \notin (X, Y)$, le nombre $f(0, 0)$ (vu comme polynôme de degré 0) est non nul donc inversible dans $\mathbb{C}[X, Y]$ et l'idéal (f, X, Y) contient un inversible donc est égal à $\mathbb{C}[X, Y]$. Il s'ensuit que (X, Y) n'est contenu dans aucun idéal propre.

Remarque. – Dans l'anneau $\mathbb{C}[X_1, \cdots, X_n]$ on dispose d'une "chaîne" d'idéaux *premiers* emboités

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \cdots, X_n).$$

La longueur de cette chaîne est n et on peut montrer que toute autre chaîne maximale d'idéaux premiers est aussi de longueur n. On peut donc retrouver la dimension n de $\mathbb{C}^n$ à partir de considérations relevant exclusivement de la théorie des anneaux sur $\mathcal{O}(\mathbb{C}^n)$.

THÉORÈME. (utilise l'axiome du choix) – *Tout anneau possède un idéal maximal.*

Démonstration. Le *lemme de Zorn* est un résultat de théorie des ensembles équivalent à l'axiome du choix dénombrable qui affirme la chose suivante : *si dans un ensemble ordonné $(E, \leqslant)$, toute suite croissante possède un majorant, alors E possède un élément maximal.* Soit A un anneau et E l'ensemble de ses idéaux propres, ordonné par inclusion. Si $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ est une suite croissante d'idéaux, alors le sous-ensemble $\bigcup_{i \in \mathbb{N}} I_i$ de A est un idéal qui contient chaque I_i. C'est donc un majorant, dans E, de cette suite.

Le lemme de Zorn nous affirme donc l'existence d'un élément maximal dans E, comme voulu. □

2.1.9 *Opérations sur les idéaux.* Soient I, J deux idéaux d'un anneau A. On a déjà défini la somme $I+J$ et le produit $I \cdot J$ de ces idéaux. Rappelons simplement que $I+J$ est l'idéal engendré par $I \cup J$, tandis que $I \cdot J$ est l'idéal engendré par les éléments ij, $i \in I$, $J \in J$. Bien que cela puisse être ambigu, nous noterons souvent IJ au lieu de $I \cdot J$.

Remarque. – Si $I = (a_1, \cdots, a_r)$ et $J = (b_1, \cdots, b_s)$, alors $I+J = (a_1, \cdots, a_r, b_1, \cdots, b_s)$ et $IJ = (a_1b_1, \cdots, a_rb_1, a_1b_2, \cdots, a_rb_2, \cdots, a_rb_s)$

On a bien sûr les inclusions d'idéaux $I \subset I+J$, $J \subset I+J$ et $IJ \subset I \cap J$.

Remarque. – A propos d'inclusion d'idéaux, il est utile de remarquer que la relation de contenance des idéaux généralise la notion de divisibilité entre élements de A au sens où

$$\forall a, b \in A,\ a|b \Leftrightarrow (a) \supset (b).$$

Exercice. – Avec $A = \mathbb{Z}$, $I = n\mathbb{Z}$ et $J = m\mathbb{Z}$ supposés propres et non nuls, montrer que

$$IJ = nm\mathbb{Z}, \quad I \cap J = \mathrm{ppcm}(n, m) \cdot \mathbb{Z}, \quad I + J = \mathrm{pgcd}(n, m) \cdot \mathbb{Z}.$$

Remarque. – Dans un anneau A général, il n'est pas vrai que si deux éléments a, b n'ont pas de diviseur commun alors $(a)+(b) = A$. Par exemple dans $\mathbb{Z}[\sqrt{-5}]$, on a vu que l'idéal $\mathfrak{p} = (2) + (1+\sqrt{-5})$ est propre, puisque $\mathfrak{p}^2 = (2)$.

2.1.10 *Idéaux de $\mathcal{O}(\mathbb{C}^n)$ et sous-ensembles algébriques de $\mathbb{C}^n$.* Rappelons que $\mathcal{O}(\mathbb{C}^n)$ désigne la $\mathbb{C}$-algèbre des fonctions polynomiales sur $\mathbb{C}^n$. A tout idéal $I \subset \mathcal{O}(\mathbb{C}^n)$ on a associé le sous-ensemble algébrique $V_I := \{z \in \mathbb{C}^n, \forall f \in I, f(z) = 0\}$ de $\mathbb{C}^n$, qui est le lieu d'annulation commun des fonctions contenues dans I. Dans l'autre sens, étant donné un sous-ensemble V de $\mathbb{C}^n$, on note $I_V := \{f \in \mathcal{O}(\mathbb{C}^n), \forall z \in V, f(z) = 0\}$, qui est l'idéal des fonctions polynomiales qui s'annulent sur V. On a alors les propriétés suivantes

i) $I \subset J \Rightarrow V_J \subset V_I$ (évident)

ii) $V_I \cap V_J = V_{I+J}$. En effet, chaque côté est l'ensemble des $z \in \mathbb{C}^n$ qui annulent toutes les fonctions dans I et toutes les fonctions dans J.

iii) $V_I \cup V_J = V_{I \cap J} = V_{IJ}$. En effet, les inclusions $V_I \cup V_J \subseteq V_{I \cap J} \subseteq V_{IJ}$ découlent de i). Pour voir l'inclusion $V_{IJ} \subseteq V_I \cup V_J$, prenons $z \in V_{IJ}$ et supposons que $z \notin V_I$. Alors il existe $f \in I$ telle que $f(z) \neq 0$. Pour toute $g \in J$, on a $fg \in IJ$, donc $(fg)(z) = f(z)g(z) = 0$, donc $g(z) = 0$. On a donc $z \in V_J$.

iv) $V \subset W \Rightarrow I_W \subset I_V$ (évident)

v) $I_{V \cup W} = I_V \cap I_W$. En effet, chaque côté est l'ensemble des fonctions polynomiales dont les restrictions à V et à W sont nulles.

vi) $I_{V \cap W} \supseteq I_V + I_W$. En effet, v) implique $I_{V \cap W} \supseteq I_V$ et $I_{V \cap W} \supseteq I_W$, donc $I_{V \cap W} \supseteq (I_V \cup I_W)$, donc $I_{V \cap W}$ contient l'idéal engendré par $I_V \cup I_W$, qui est $I_V + I_W$.

vii) $\forall V \subset \mathbb{C}^n$, l'idéal I_V est radiciel. En effet, pour tout $z \in \mathbb{C}^n$, on a $(\exists k \in \mathbb{N},\ f^k(z) = 0) \Leftrightarrow f(z) = 0$.

viii) I_V maximal $\Leftrightarrow$ V singleton. En effet, si $V = \{z\}$, alors pour toute fonction $f \notin I_V$, on a $f(z) \neq 0$ et $f - f(z) \in I_V$, donc $1 = f(z)^{-1}f + (1 - f(z)^{-1}f) \in (f) + I_V$, et il s'ensuit que I_V est maximal. Réciproquement, si I_V est maximal, il est en particulier propre, donc $V \neq \emptyset$. Soit donc $z \in V$, on a une inclusion d'idéaux $I_V \subset I_{\{z\}}$ qui sont tous les deux maximaux, donc c'est une égalité. Si maintenant $z' \in V$, on a donc $I_{\{z'\}} = I_{\{z\}}$. En particulier, notant $z = (z_1, \cdots, z_n)$ et $z' = (z'_1, \cdots, z'_n)$, on a que pour tout i, la fonction $X_i - z_i$ s'annule sur z', donc $z'_i = z_i$, puis $z' = z$. On a donc montré que $V = \{z\}$ est un singleton.

2.1.11 *Anneaux quotients.* Voici une construction fondamentale qu'il est important de bien comprendre. Soit A un anneau et I un idéal de A. On munit l'ensemble A de la relation d'équivalence définie par

$$x \equiv y \,(\mathrm{mod}\, I) \text{ si et seulement si } x - y \in I.$$

Les classes d'équivalence pour cette relation sont donc de la forme $x + I = \{x + i, i \in I\}$ pour $x \in A$. On note A/I l'ensemble des classes d'équivalences, appelé *ensemble quotient* de A par cette relation d'équivalence, et $\pi_I : A \longrightarrow A/I$ la projection canonique qui envoie x sur sa classe d'équivalence. Nous noterons indifféremment selon l'humeur $\pi_I(x)$, $\overline{x}$, $x + I$, $x \,(\mathrm{mod}\, I)$, l'image de x dans A/I.

PROPOSITION. – *Il existe une unique structure d'anneau commutatif sur A/I telle que π_I soit un morphisme d'anneaux.*

Démonstration. L'unicité découle de la surjectivité de π_I. En effet, la contrainte que π_I soit un morphisme d'anneaux force les identités

$$\overline{x} + \overline{y} = \overline{x + y} \text{ et } \overline{x} \cdot \overline{y} = \overline{xy}.$$

Reste à voir que ceci est bien défini et satisfait les axiomes qui définissent un anneau. Pour voir que c'est bien défini, il faut vérifier que pour $x \equiv x' \,(\mathrm{mod}\, I)$ et $y \equiv y' \,(\mathrm{mod}\, I)$, on a $(x+y) \equiv (x'+y') \,(\mathrm{mod}\, I)$ et $xy \equiv x'y' \,(\mathrm{mod}\, I)$. Ceci est immédiat ; vérifions par exemple la deuxième relation : si on écrit $x' = x+i$ et $y' = y+i'$ avec $i, i' \in I$, on voit que $x'y' = xy+i''$ avec $i'' = (iy + i'x + ii') \in I$.

De même on vérifie sans difficulté que les deux lois ainsi construites font de A/I un anneau avec pour éléments neutres $\overline{0}$ et $\overline{1}$. □

L'anneau A/I est appelé *anneau quotient* de A par I.

Exemple. – l'anneau "bien connu" $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par l'idéal $(n) = n\mathbb{Z}$.

Exemple. – Si $I = A$, le quotient A/I est l'anneau nul.

On a la correspondance suivante entre propriétés de I et propriétés de A/I.

PROPOSITION. – *Soit A un anneau commutatif et I un idéal de A.*

i) I est maximal si et seulement si A/I est un corps.

ii) I est premier si et seulement si A/I est intègre.

iii) I est radiciel si et seulement si A/I est réduit.

Démonstration. i) Supposons I maximal. On veut montrer que tout élément non nul de A/I possède un inverse. Un tel élément est de la forme $\overline{x} = x + I$ avec $x \notin I$. Par maximalité de I, on a $I + (x) = A$ donc il existe $i \in I$ et $y \in A$ tels que $i + xy = 1$. Alors $xy \equiv 1 \,(\mathrm{mod}\, I)$ donc $\overline{yx} = \overline{1}$ et $\overline{x}$ possède bien un inverse dans A/I. Ce dernier est donc un corps. Réciproquement, supposons que A/I est un corps, et soit J un idéal contenant strictement I. On doit montrer que $J = A$. Choisissons un élément $j \in J/I$. Son image $\overline{j}$ dans A/I admet un inverse $\overline{a}$ pour $a \in A$ et on a donc $aj \in 1 + I$. Il s'ensuit que $1 \in (j) + I$ donc $(j) + I = A$ et a fortiori $J = A$.

ii) Pour deux éléments $x, y \in A$ on a les équivalences $\overline{x} = 0 \Leftrightarrow x \in I$, $\overline{y} = 0 \Leftrightarrow y \in I$ et $\overline{xy} = 0 \Leftrightarrow xy \in I$. Le point ii) découle donc immédiatement des définitions. De même pour iii). □

Exercice. – Montrer que l'application $J \mapsto \pi_I^{-1}(J)$ induit une bijection

$$\{\text{idéaux de } A/I\} \xrightarrow{\sim} \{\text{idéaux de } A \text{ contenant } I\}$$

dont la bijection réciproque est $I' \mapsto \pi_I(J)$. Montrer que $\pi_I^{-1}(\sqrt{0}) = \sqrt{I}$.

2.1.12 *Propriété universelle des quotients.*

PROPOSITION. – *Pour tout morphisme d'anneaux $\varphi : A \longrightarrow A'$ tel que $I \subset \mathrm{Ker}(\varphi)$, il existe une unique factorisation $\varphi = \overline{\varphi} \circ \pi_I$ comme dans le diagramme suivant.*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \,. \\ {\scriptstyle \pi_I}\downarrow & \nearrow_{\overline{\varphi}} & \\ A/I & & \end{array}$$

De plus, $\overline{\varphi}$ est injectif si et seulement si $I = \mathrm{Ker}(\varphi)$.

Démonstration. L'unicité découle de la surjectivité de π_I. En effet, si $\overline{x} \in A/I$, on doit avoir $\overline{\varphi}(\overline{x}) = \varphi(x)$. Pour l'existence, il faut d'abord vérifier que ceci définit sans ambiguïté $\overline{\varphi}$. Pour cela, il faut vérifier que si $x \equiv x' \,(\mathrm{mod}\, I)$, on a bien $\varphi(x) = \varphi(x')$. Ecrivons $x' = x + i$ avec $i \in I$. On a donc $\varphi(x') = \varphi(x) + \varphi(i) = \varphi(x)$ puisque $i \in \mathrm{Ker}(\varphi)$, comme voulu. On a donc bien une factorisation d'applications $\varphi = \overline{\varphi} \circ \pi_I$, et il reste à vérifier que $\overline{\varphi}$ est bien un morphisme d'anneaux. Mais ceci est clair vu la définition de la structure d'anneau sur A/I.

Montrons la dernière assertion. Supposons d'abord que $\overline{\varphi}$ est injective. Alors le fait général $\mathrm{Ker}(\varphi) = \pi_I^{-1}(\mathrm{Ker}(\overline{\varphi}))$ montre que $\mathrm{Ker}(\varphi) = \pi_I^{-1}(\{0\}) = I$. Réciproquement, supposons $\mathrm{Ker}(\varphi) = I$. Pour tout $\overline{x} \in \mathrm{Ker}(\overline{\varphi})$, le même fait général nous dit que $x \in \mathrm{Ker}(\varphi)$ donc $x \in I$ et $\overline{x} = \overline{0} = 0$. □

Remarque. (Qu'est-ce qu'une propriété *universelle* ?) – Dans le langage "méta-mathématique", une propriété d'un objet est dite *universelle* si elle *caractérise* cet objet parmi tous les objets de la même "catégorie". Autrement dit, un objet qui possède cette propriété universelle est déterminé de manière *unique à isomorphisme unique près* (la notion d'isomorphisme étant celle pertinente pour la catégorie d'objets considérée). Dans le cas qui nous intéresse ici, la paire $(A/I, \pi)$ vit dans la "catégorie" des A-algèbres (B, ψ) telles que $\psi(I) = 0$, et la proposition nous dit qu'elle possède la propriété suivante : *pour toute A-algèbre (A', φ) telle que $\varphi(I) = 0$, il existe un unique morphisme de A-algèbres $A/I \longrightarrow A'$.* Supposons qu'une autre A-algèbre (B, ψ) avec $\psi(I) = 0$ vérifie la même propriété. Alors en appliquant cette propriété à $(A', \varphi) = (A/I, \pi_I)$ on obtient un morphisme de A-algèbres $B \xrightarrow{\overline{\pi}} A/I$. D'un autre côté la proposition nous fournit un morphisme de A-algèbres $A/I \xrightarrow{\overline{\psi}} B$. La composition $\overline{\pi}\overline{\psi}$ est un endomorphisme de la A-algèbre A/I, mais la proposition nous dit qu'il existe un unique tel endomorphisme. Comme l'identité est clairement un endomorphisme de A-algèbres, on doit donc avoir $\overline{\pi} \circ \overline{\psi} = \mathrm{id}_{A/I}$. De même la propriété supposée de (B, ψ) nous assure que $\overline{\psi} \circ \overline{\pi} = \mathrm{id}_B$ et on obtient ainsi un isomorphisme de A-algèbres $A/I \xrightarrow{\sim} B$ qui est est de plus *unique* d'après la propriété ou la proposition.

Corollaire. – *Tout morphisme d'anneaux $\varphi : A \longrightarrow A'$ admet une unique factorisation*

$$\varphi : \ A \twoheadrightarrow A/\operatorname{Ker}(\varphi) \xrightarrow{\sim} \operatorname{Im}(\varphi) \hookrightarrow A'$$

où la première flèche est la projection canonique sur le quotient $A/\operatorname{Ker}(\varphi)$.

On rappelle que le symbole $\twoheadrightarrow$ désigne une surjection, le symbole $\hookrightarrow$ désigne une injection, et le symbole $\xrightarrow{\sim}$ désigne un isomorphisme.

Démonstration. En appliquant la proposition à $I = \operatorname{Ker}(\varphi)$, on obtient une factorisation $\varphi = \overline{\varphi} \circ \pi_I$. De plus, $\overline{\varphi}$ est injective, donc réalise un isomorphisme de sa source sur son image $\operatorname{Im}(\overline{\varphi}) = \operatorname{Im}(\varphi)$, qui est un sous-anneau de A'. □

Exemple. – Soit V un sous-ensemble algébrique de $\mathbb{C}^n$. Vu la définition de l'algèbre des fonctions polynômiales $\mathcal{O}(V)$, l'application de restriction des fonctions $\mathcal{O}(\mathbb{C}^n) \longrightarrow \mathcal{O}(V)$ est surjective. Soit $\mathcal{I}$ son idéal, elle induit donc un isomorphisme $\mathcal{O}(\mathbb{C}^n)/\mathcal{I} \xrightarrow{\sim} \mathcal{O}(V)$ qui présente $\mathcal{O}(V)$ comme un quotient de l'algèbre de polynôme $\mathbb{C}[X_1, \cdots, X_n]$.

2.1.13 *Morphismes entre quotients.* Soit maintenant $J \supset I$ un idéal de A contenant I. La proposition universelle du quotient A/I nous fournit une factorisation

$$\pi_J : \ A \xrightarrow{\pi_I} A/I \xrightarrow{\overline{\pi}_J} A/J.$$

Proposition. – *L'image $J/I := \pi_I(J)$ de J dans A/I est un idéal et le morphisme $\overline{\pi}_J$ induit un isomorphisme*

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

Démonstration. Puisque le morphisme π_J est surjectif, le morphisme $\overline{\pi}_J$ l'est aussi, et il nous suffit de voir que son noyau est donné par $\mathrm{Ker}(\overline{\pi}_J) = \pi_I(J)$ (ce qui démontrera au passage que $\pi_I(J)$ est bien un idéal). On a $\pi_I^{-1}(\mathrm{Ker}(\overline{\pi}_J)) = \mathrm{Ker}(\overline{\pi}_J \circ \pi_I) = \mathrm{Ker}(\pi_J) = J$. Mais puisque π_I est surjectif, on a $\mathrm{Ker}(\overline{\pi}_J) = \pi_I(\pi_I^{-1}(\mathrm{Ker}(\overline{\pi}_J)) = \pi_I(J)$. □

Exemple. – On retrouve le fait "bien connu" que pour $m|n$ l'application $a \mapsto a \,(\mathrm{mod}\, m)$ se factorise par un morphisme $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ via l'application $a \mapsto a \,(\mathrm{mod}\, n)$ et induit un isomorphisme $(\mathbb{Z}/n\mathbb{Z})/m(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}$.

Variante : au lieu de partir de $J \supset I$, partons de J quelconque et appliquons la proposition à l'idéal $I + J$, qui contient I. On obtient une factorisation $\pi_{I+J} = \overline{\pi}_{I+J} \circ \pi_I$ avec $\overline{\pi}_{I+J}$ qui induit un isomorphisme

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

2.1.14 *Théorème des restes chinois.* Soient I, J deux idéaux de A. Le noyau du morphisme $A \longrightarrow A/I \times A/J$, $a \mapsto (a \,(\mathrm{mod}\, I), a \,(\mathrm{mod}\, J))$ contient clairement $I \cap J$, donc (propriété universelle) ce morphisme se factorise via $\pi_{I\cap J}$ par un morphisme

$$A/(I \cap J) \xrightarrow{(\overline{\pi}_I, \overline{\pi}_J)} A/I \times A/J.$$

Proposition. – *Le morphisme $(\overline{\pi}_I, \overline{\pi}_J)$ ci-dessus est injectif. Il est surjectif si et seulement si $I + J = A$. Dans ce dernier cas on obtient donc un isomorphisme*

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

Démonstration. Pour l'injectivité, il suffit de vérifier que $I \cap J$ est exactement le noyau du morphisme (π_I, π_J), ce qui est clair.

Pour prouver la surjectivité de $(\overline{\pi}_I, \overline{\pi}_J)$ il faut montrer que pour tous $a, b \in A$, l'intersection $(a + I) \cap (b + J)$ est non vide. En effet, si c'est le cas, pour tout c dans cette intersection on a $(c \,(\mathrm{mod}\, I), c \,(\mathrm{mod}\, J)) = (a \,(\mathrm{mod}\, I), b \,(\mathrm{mod}\, J))$.

Supposons donc que $I + J = A$, et choisissons $i \in I$ et $j \in J$ tels que $i + j = 1$. Alors l'élément $c = aj + bi$ est dans $(a + I)$ puisque $c = a - ai + bi$ et dans $(b + J)$ puisque $c = b - bj + aj$. Il s'ensuit que $(\overline{\pi}_I, \overline{\pi}_J)$ est bien surjectif.

Réciproquement, supposons que $(\overline{\pi}_I, \overline{\pi}_J)$ est surjectif. Alors en particulier il existe $j \in A$ tel que $(\overline{1}, 0) = (\pi_I(j), \pi_J(j))$, ce qui est équivalent à $(j \in 1 + I$ et $j \in J)$. En posant $i = 1 - j$, on a $i \in I$ et $i + j = 1$ donc on obtient que $I + J = A$ comme voulu. □

Exemple. – Avec $A = \mathbb{Z}$, $I = n\mathbb{Z}$ et $J = m\mathbb{Z}$ supposés propres et non nuls, on a $I \cap J = \mathrm{ppcm}(n, m) \cdot \mathbb{Z}$ et $I + J = \mathrm{pgcd}(n, m) \cdot \mathbb{Z}$. En particulier la condition $I + J = A$ équivaut à $\mathrm{pgcd}(n, m) = 1$ et dans ce cas on retrouve le lemme des restes chinois usuel : $\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

2.2 Généralités sur les modules

Les modules sont aux anneaux (commutatifs) ce que les espaces vectoriels sont aux corps. Néanmoins, ils ne possèdent pas nécessairement de base, ce qui rend leur étude bien plus délicate.

2.2.1 Définition.– *Soit A un anneau. Un A-module M est un groupe abélien muni d'une "action" de A*

$$\begin{array}{rcl} A \times M & \to & M \\ (a, m) & \mapsto & a \cdot m \end{array}$$

satisfaisant les axiomes suivants pour tous $a, a' \in A$ et $m, m' \in M$:

i) $a \cdot (m + m') = a \cdot m + a \cdot m'$ *(linéarité de l'action).*

ii) $(a + a') \cdot m = a \cdot m + a' \cdot m$ *et* $(aa') \cdot m = a \cdot (a \cdot m)$.

iii) $1 \cdot m = m$.

On dit aussi que M est un "module sur A".

Remarque. – L'axiome i) nous dit que l'application $m \mapsto a \cdot m$ est un endomorphisme du groupe abélien M, et les axiomes ii) et iii) nous disent que l'application $A \longrightarrow \mathrm{End}(M)$ qui en résulte est un morphisme d'anneaux (noter que le produit de $\mathrm{End}(M)$ est donné par la composition des endomorphismes donc est non-commutatif mais cela n'affecte pas la notion de morphisme). Réciproquement tout morphisme d'anneaux $\psi : A \longrightarrow \mathrm{End}\,(M)$ (endomorphismes du groupe abélien M) définit une structure d'anneau en posant $a \cdot m := \psi(a)(m)$.

Nous simplifierons souvent la notation en écrivant am plutôt que $a \cdot m$. La définition suivante est sans surprise :

Définition. – *Un morphisme $\varphi : M \longrightarrow M'$ de A-modules est un morphisme de groupes abéliens qui est A-linéaire au sens où $\forall a \in A$, $\forall m \in M$ on a $\varphi(am) = a\varphi(m)$.*

Nous noterons $\mathrm{Hom}_A(M, M')$ l'ensemble des morphismes de A-modules et $\mathrm{End}_A(M)$ l'ensemble des endomorphismes du A-module M. Notons qu'ils sont eux-même munis d'une structure naturelle de A-module par les formules

$$a \cdot \varphi : m \mapsto a\varphi(m), \quad \text{et} \quad \varphi + \varphi' : m \mapsto \varphi(m) + \varphi'(m).$$

Comme d'habitude, un *isomorphisme de A-modules* est un morphisme inversible à gauche et à droite. On vérifie sans peine qu'un morphisme est un isomorphisme si et seulement si il est bijectif (en tant qu'application).

Exemple. ($A = \mathbb{Z}$) – Tout groupe abélien possède une unique structure de $\mathbb{Z}$-module, donnée par l'unique morphisme d'anneaux $\mathbb{Z} \longrightarrow \mathrm{End}(M)$. Ainsi un $\mathbb{Z}$-module n'est rien d'autre qu'un groupe abélien et tout morphisme de groupes abéliens est aussi un morphisme de $\mathbb{Z}$-modules.

Exemple. (A un corps) – Un module sur un corps K est un K-espace vectoriel et un morphisme de K-modules est une application K-linéaire.

Exemple. (Lien avec les A-algèbres) – Si (B, ψ) est une A-algèbre, *i.e.* un morphisme d'anneaux $\psi : A \longrightarrow B$, alors B est naturellement un A-module pour l'action $a \cdot b := \psi(a)b$. Réciproquement, si un A-module B est muni d'un produit qui en fait un anneau d'unité 1_B, et si ce produit est A-bilinéaire au sens où $a \cdot (bc) = (a \cdot b)c = b(a \cdot c)$, alors l'application $\psi : a \mapsto a \cdot 1_B$ est un morphisme d'anneau qui fait donc de B une A-algèbre. Cela fait le lien avec la notion peut-être vue précédemment de K-algèbre lorsque K est un corps (K-ev muni d'un produit K-bilinéaire et d'une unité). De plus, un morphisme de A-algèbres $(B, \psi) \longrightarrow (B', \psi')$ tel qu'on l'a défini plus haut n'est autre qu'un morphisme d'anneaux A-linéaire.

2.2.2 *Restriction des scalaires.* Soit $\varphi : B \longrightarrow A$ un morphisme d'anneaux, et soit M un A-module. La composée

$$B \xrightarrow{\varphi} A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$$

munit M d'une structure de B-module, donnée par $b \cdot m := \varphi(b)m$. On dit que ce B-module M est la "restriction des scalaires via φ" du A-module M. Si on veut lever l'ambiguité de la notation M sur la structure considérée on pourra noter $\varphi^* M$ ou $M_{|B}$ ou encore $\mathrm{Res}_A^B(M)$ ce B-module.

Exemple. – La restriction des scalaires d'un A-module M via le morphisme canonique $\mathbb{Z} \longrightarrow A$ est le groupe abélien sous-jacent à M.

Remarquons qu'un morphisme de A-modules $M \longrightarrow N$ est aussi un morphisme de B-modules $\varphi^* M \longrightarrow \varphi^* N$, la réciproque n'étant en général pas vraie. On a donc une inclusion

$$\mathrm{Hom}_A(M, N) \subset \mathrm{Hom}_B(M, N).$$

Exercice. – Vérifier que c'est une égalité si φ est surjectif.

2.2.3 *Retour sur les A-algèbres.* Nous avons défini une A-algèbre comme un anneau B muni d'un morphisme $\psi : A \longrightarrow B$. On a alors les propriétés suivantes :

- *B est un A-module.* En effet, B est un module sur lui même donc, par restriction des scalaires à A, devient un A-module. Explicitement l'action de A est donnée par $a \cdot b = \psi(a)b$.
- Pour tout $b \in B$ les applications $b' \mapsto bb'$ et $b' \mapsto b'b$ sont A-linéaires.
- Le morphisme ψ est donné par $\psi(a) = a \cdot 1_B$.

Réciproquement, partons d'un A-module B muni d'une structure d'anneau d'unité 1_B telle que pour tout $b \in B$ les applications $b' \mapsto bb'$ et $b' \mapsto b'b$ sont A-linéaires. Alors l'application $a \mapsto a \cdot 1_B$ est un morphisme d'anneaux qui fait de B une A-algèbre.

2.2.4 *Sous-modules, modules quotients.* Sans surprise, un *sous-A-module* de M est un sous-groupe de M stable par l'action de A sur M.

Remarque. – A est un A-module via la multiplication. Un sous-A-module de A n'est rien d'autre qu'un idéal de A.

Exemple. – L'image $\mathrm{Im}(\varphi)$ d'un morphisme $\varphi : M \longrightarrow M'$ est un sous-A-module de M' et son noyau $\mathrm{Ker}(\varphi) = \varphi^{-1}(0)$ est un sous-A-module de M. Plus généralement, si N est un sous-module de M, son image $\varphi(N)$ est un sous-module de M', et si N' est un sous-module de M', son image inverse $\varphi^{-1}(N')$ est un sous-module de A.

Soit M un A-module et N un sous-A-module de M. Considérons l'ensemble quotient M/N de M par la relation d'équivalence

$$m \sim m' \Leftrightarrow m - m' \in N$$

et notons $\pi : M \longrightarrow M/N$ la projection canonique. Comme précédemment, on notera selon l'humeur $\pi(m)$, $\overline{m}$, $m + N$ ou encore $m \,(\mathrm{mod}\, N)$ la classe d'équivalence de m.

Proposition. – *Il existe une unique structure de A-module sur M/N qui fait de π un morphisme de A-module.*

Démonstration. C'est le même argument que pour la construction du quotient A/I. L'unicité découle de la surjectivité de π qui nous impose les formules suivantes : $a\overline{m} = \overline{am}$ et $\overline{m} + \overline{m}' = \overline{m + m'}$. Pour l'existence, il faut vérifier que ces formules font sens, c'est-à-dire que

$$m \sim m' \Rightarrow am \sim am' \text{ et } m \sim m_1, m' \sim m'_1 \Rightarrow (m + m') \sim (m_1 + m'_1)$$

ce qui découle immédiatement du fait que N est un sous-A-module. □

Exercice. – Montrer que π^{-1} induit une bijection

$$\{\text{sous-modules de } M/N\} \xrightarrow{\sim} \{\text{sous-modules de } M \text{ contenant } N\}$$

dont la bijection réciproque est $P \mapsto \pi(P) = P/N$.

Comme pour toute notion de quotient, on peut aussi caractériser M/N par une propriété universelle.

Proposition. – *Soit $\psi : M \longrightarrow M'$ un morphisme de A-module tel que $\psi(N) = \{0\}$. Il existe un unique morphisme de A-module $\overline{\psi} : M/N \longrightarrow M'$ tel que $\psi = \overline{\psi} \circ \pi$.*

Corollaire. – *Tout morphisme $M \xrightarrow{\psi} M'$ admet une factorisation unique*

$$M \twoheadrightarrow M/\mathrm{Ker}(\psi) \xrightarrow{\sim} \mathrm{Im}(\psi) \hookrightarrow M'.$$

Soit maintenant P un sous-module de M contenant N. Le noyau de la projection canonique $\pi_P : M \longrightarrow M/P$ contient donc N et la proposition ci-dessus nous donne donc une factorisation de π_P

$$M \xrightarrow{\pi_N} M/N \xrightarrow{\overline{\pi}_P} M/P.$$

COROLLAIRE. (1er théorème d'isomorphisme) – *$\overline{\pi}_P$ induit un isomorphisme*

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

Démonstration. Puisque π_N est surjective, on a $\mathrm{Ker}(\overline{\pi}_P) = \pi_N(\mathrm{Ker}(\pi_P)) = \pi_N(P) = P/N$, donc $\overline{\pi}_P$ se factorise via un morphisme injectif $(M/N)/(P/N) \hookrightarrow M/N$. Ce dernier est aussi surjectif, puisque π_P, et donc $\overline{\pi}_P$ l'est. □

Considérons maintenant la situation suivante : soit M un A-module et soient N, P deux sous-modules de M. On définit leur somme

$$N + P := \{m \in M, \exists\, n \in N, \exists p \in P, m = n + p\}$$

qui est visiblement un sous-A-module de M (le vérifier !) contenant N et P. De même, l'intersection $N \cap P$ est un sous-A-module de M. Alors le noyau du morphisme composé

$$\rho :\ N \hookrightarrow N + P \twoheadrightarrow (N + P)/P$$

contient visiblement $N \cap P$ et ce morphisme se factorise donc par un morphisme

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

PROPOSITION. (2ème théorème d'isomorphisme) – *Ce morphisme est un isomorphisme*

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

Démonstration. Pour l'injectivité, il faut prouver que $\mathrm{Ker}(\rho) = N \cap P$, ce qui est clair. Pour la surjectivité, il faut voir que tout élément de $(N + P)/P$ se relève en un élément de N via la projection $N + P \twoheadrightarrow (N + P)/P$ ce qui est aussi immédiat, vu la définition d'un quotient. □

2.2.5 *Sommes directes et produits.* Soit I un ensemble et soit $(M_i)_{i\in I}$ une famille de A-modules indexée par I (on pourra penser à $I = \mathbb{N}$ ou $I = \{1, \cdots, r\}$). On rappelle que le produit cartésien $\prod_{i\in I} M_i$ est l'ensemble des familles $(m_i)_{i\in I}$ indexées par I où $m_i \in M_i$ pour tout i. On munit ce produit cartésien d'une structure de A-module en posant :

— $(m_i)_{i\in I} + (m'_i)_{i\in I} := (m_i + m'_i)_{i\in I}$

— $a \cdot (m_i)_{i\in I} := (am_i)_{i\in I}$.

(On laisse au lecteur le soin de vérifier que c'est bien un A-module dont l'élément 0 est la famille $(0)_{i\in I}$). Ce module sera appelé *produit des M_i* et noté

$$\prod_{i\in I} M_i\ , \quad \text{ou plus simplement } M_1 \times \cdots \times M_r \text{ lorsque } I = \{1, \cdots, r\}.$$

Pour chaque $j \in I$, la projection $(m_i)_{i\in I} \mapsto m_j$ est un morphisme de A-modules

$$\prod_{i\in I} M_i \xrightarrow{\pi_j} M_j.$$

On définit maintenant

$$\bigoplus_{i\in I} M_i := \left\{ (m_i)_{i\in I} \in \prod_{i\in I} M_i, m_i = 0 \text{ pour presque tout } i \right\},$$

le sous-ensemble des familles à support fini (i.e. tel que $m_i = 0$ hors d'un sous-ensemble fini de I). On voit que c'est un sous-A-module de $\prod_{i\in I} M_i$ et on l'appelle *somme directe* ou *coproduit* des M_i.

Remarque. – Si I est *fini* on a $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$. Lorsque $I = \{1, \cdots, r\}$ on le note aussi $\bigoplus_{i=1}^{r} M_i$ ou simplement $M_1 \oplus \cdots \oplus M_r$.

Pour chaque $j \in I$, on a une application

$$\iota_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$$

qui envoie m sur la famille $(m_i)_{i\in I}$ telle que $m_i = 0$ pour $i \neq j$ et $m_j = m$. Cette application est visiblement un morphisme de A-modules.

Ces modules, munis de leurs familles de morphismes, satisfont chacun une propriété universelle, et ces propriétés sont en quelque sorte "duales" l'une de l'autre.

PROPOSITION. – *i) Soit N un A-module muni d'une famille de morphismes $\psi_i : N \longrightarrow M_i$ pour chaque $i \in I$. Alors il existe un unique morphisme $\Psi : N \longrightarrow \prod_{i\in I} M_i$ tel que $\psi_i = \pi_i \circ \Psi$ pour tout i. Autrement dit, l'application $\Psi \mapsto (\pi_i \circ \Psi)_{i\in I}$ induit une bijection*

$$\mathrm{Hom}_A\left(N, \prod_{i\in I} M_i\right) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A(N, M_i).$$

ii) Soit N un A-module muni d'une famille de morphismes $\psi_i : M_i \longrightarrow N$ pour chaque $i \in I$. Alors il existe un unique morphisme $\Psi : \bigoplus_{i\in I} M_i \longrightarrow N$ tel que $\psi_i = \Psi \circ \iota_i$ pour tout i. Autrement dit, l'application $\Psi \mapsto (\Psi \circ \iota_i)_{i\in I}$ induit une bijection

$$\mathrm{Hom}_A\left(\bigoplus_{i\in I} M_i, N\right) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A(M_i, N).$$

Démonstration. Tout cela est très formel. i) Pour l'existence, il suffit de poser $\Psi(n) := (\psi_i(n))_{i\in I}$. Pour l'unicité, si Ψ' est un autre morphisme, on voit que pour tout n, $\Psi(n) - \Psi'(n)$ est annulé par toutes les projections π_i, donc est nul.

ii) Pour l'existence il suffit de poser $\Psi((m_i)_{i\in I}) := \sum_{i\in I} \psi_i(m_i)$, ce qui a un sens puisque la famille $\psi_i(m_i)$ est presque nulle (seulement un nombre fini de termes non nuls dans cette somme). Pour l'unicité, si Ψ' est une autre solution, on voit que $\Psi - \Psi'$ s'annule sur l'image $\iota_i(M_i)$ de chaque ι_i. Or tout élément de $\bigoplus_{i\in I} M_i$ est somme d'éléments de cette forme (ce n'est pas vrai pour les éléments de $\prod_{i\in I} M_i$ si I est infini). □

2.2.6 *Somme de sous-modules, modules engendrés.* Soit M un A-module. Comme l'intersection de deux sous-modules est encore un sous-module, on peut parler du "plus petit sous-module" $M(E)$ contenant un sous-ensemble donné $E \subset M$. C'est aussi l'intersection de tous les sous-modules contenant E, et on l'appelle le *sous-module engendré par* E. Explicitement, c'est l'ensemble

$$M(E) = \{m = a_1 e_1 + \cdots + a_r e_r,\ r \in \mathbb{N}, e_i \in E, a_i \in A\}.$$

Supposons maintenant donnée une famille $(M_i)_{i\in I}$ de sous-modules indexée par un ensemble I. On note

$$\sum_{i\in I} M_i, \text{ ou plus simplement } M_1 + \cdots + M_r \text{ si } I = \{1, \cdots, r\}$$

le sous-module de M engendré par la réunion $\bigcup_{i\in I} M_i$. Explicitement, il est donné par

$$\sum_{i\in I} M_i = \{\sum_{i\in J} m_i,\ J \subset I \text{ fini }, m_i \in M_i\}.$$

De manière plus formelle, considérons le morphisme $\Psi : \bigoplus_{i\in I} M_i \longrightarrow M$ associé aux inclusions $\psi_i : M_i \hookrightarrow M$ fourni par la propriété universelle du coproduit. Alors

$$\sum_{i\in I} M_i = \mathrm{Im}(\Psi).$$

Définition. – *On dit que les M_i sont "en somme directe" si le morphisme Ψ ci-dessus est injectif. Il induit alors un isomorphisme $\bigoplus_{i\in I} M_i \xrightarrow{\sim} \sum_{i\in I} M_i$.*

On peut traduire l'injectivité de Ψ comme ceci : pour toute famille finie d'élements $m_i \in M_i$, on a $\sum_{i\in I} m_i = 0 \Rightarrow \forall i \in I, m_i = 0$.

Exercice. – Montrer que les sous-modules $M_1, \cdots M_r$ sont en somme directe si et seulement si pour chaque $i = 1, \cdots, r$ on a $M_i \cap \sum_{j\neq i} M_j = \{0\}$.

Remarque. – Lorsque $A = k$ est un corps, on sait que tout sous-espace vectoriel W d'un espace vectoriel V admet un supplémentaire, c'est-à-dire un sous-espace W' de V tel que $V = W \oplus W'$. Ceci n'est plus vrai en général. Par exemple pour $A = \mathbb{Z}$, le sous-module $2\mathbb{Z}$ de $M = \mathbb{Z}$ n'admet pas de supplémentaire, puisque tout sous-module non nul de $\mathbb{Z}$ a une intersection non nulle avec $2\mathbb{Z}$.

Un sous-module N d'un module M qui admet un supplémentaire est appelé *facteur direct* de M.

2.2.7 *Modules libres.* Un cas particulier important de somme directe est celui où $M_i = A$ pour tout $i \in I$. On note alors

$$A^I := \prod_{i\in I} A \quad \text{et} \quad A^{(I)} := \bigoplus_{i\in I} A.$$

Lorsque I est fini, on a bien-sûr $A^{(I)} = A^I$ et on utilise plutôt la seconde notation, qui est plus simple. Lorsque $I = \{1, \cdots, r\}$ on note aussi simplement A^r ou $A^{\oplus r}$ plutôt que $A^{\{1,\cdots,r\}}$. Pour $i \in I$, notons e_i l'élément de $A^{(I)}$ dont toutes les composantes sont nulles sauf celle en i qui vaut 1. Par exemple, si $I = \{1, \cdots, r\}$, on a $e_i = (0, \cdots, 1, \cdots, 0)$ où le 1 est placé à la i-ème position.

PROPOSITION. – *i) Tout élément de $A^{(I)}$ s'écrit de manière unique sous la forme $\sum_{i\in I} a_i e_i$ pour une famille presque nulle $(a_i)_{i\in I}$ d'éléments de A.*

ii) Le A-module $A^{(I)}$ possède la propriété universelle suivante : pour tout A-module M et toute famille $(m_i)_{i\in I}$ d'éléments de M, il existe un unique morphisme de A-modules $\Psi : A^{(I)} \longrightarrow M$ qui envoie e_i sur m_i. En d'autres termes, l'application $\Psi \mapsto (\Psi(e_i))_{i\in I}$ est une bijection

$$\mathrm{Hom}_A(A^{(I)}, M) \xrightarrow{\sim} M^I.$$

Démonstration. i) découle de la construction

ii) Remarquons d'abord que pour tout élément m d'un module M, il existe un *unique* morphisme de A-module $A \xrightarrow{\psi_m} M$ qui envoie 1 sur m. Il est défini par $\varphi_m(a) := am$. Ainsi pour tout i on a un morphisme $\psi_{m_i} : A \longrightarrow M$, et il ne reste plus qu'à invoquer la propriété universelle des sommes directes. Explicitement, on a tout simplement $\Psi(\sum_{i\in I} a_i e_i) = \sum_{i\in I} a_i m_i$. □

DÉFINITION. – *Soit $(m_i)_{\in I}$ une famille d'éléments de M et $\Psi : A^{(I)} \longrightarrow M$ le morphisme associé. On dit que la famille est*

- libre *si Ψ est injectif, ce qui équivaut à la condition $\sum_i a_i m_i = 0 \Rightarrow \forall i, a_i = 0$*
- génératrice *si Ψ est surjectif, ce qui équivaut à ce que tout $m \in M$ puisse s'écrire sous la forme $\sum_{i\in I} a_i m_i$ avec $a_i \in A$ pour tout i.*
- une base de M *si Ψ est un isomorphisme, ce qui équivaut à ce que tout $m \in M$ s'écrive de manière unique sous la forme $\sum_{i\in I} a_i m_i$ avec $a_i \in A$ pour tout i.*

Lorque M admet une famille génératrice finie, on dit qu'il est *de type fini.*

Exemple. – Soit $A = \mathbb{Z}$ et $M = \mathbb{Z}$.

- La famille $\{2, 3\}$ est génératrice de M, puisque tout $n \in \mathbb{Z}$ est de la forme $2a + 3b$ par Bézout. Mais ce n'est pas une base, puisque $0 = 2 \cdot 3 - 3 \cdot 2$.
- La famille $\{2\}$ est libre, mais pas génératrice, donc pas une base.
- Les seules bases de M sont $\{1\}$ et $\{-1\}$.

Exemple. – Plus généralement, pour $M = A$, toute famille contenant deux éléments distincts a, a' n'est pas libre à cause de la relation $a.a' - a'.a = 0$. Il s'ensuit qu'une famille libre est un singleton $\{a\}$ avec a élément régulier de A. De plus un tel singleton est une base si et seulement si a est inversible.

DÉFINITION. – *Un A-module M est dit libre s'il possède une base. Tout choix de base induit alors un isomorphisme $A^{(I)} \xrightarrow{\sim} M$ pour un ensemble I convenable.*